Федеральное государственное бюджетное образовательное учреждение высшего образования «Томский государственный университет систем управления и радиоэлектроники»

На правах рукописи
УДК 004.056.5

ЖИЛЯЕВ АНДРЕЙ ЕВГЕНЬЕВИЧ

МЕТОДИКА ПОСТРОЕНИЯ СЕТЕЙ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ СМЕШАННОЙ ТОПОЛОГИИ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель
д. т. н., доцент А.Г. Сабанов

Томск – 2022

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования и степень ее разработанности.

Тема исследования посвящена решению задач применения перспективной технологии квантового распределения ключей, а именно задачам по формированию и использованию новых секретных ключей, основываясь на системах выработки квантовых ключей и распределении этих ключей в сетях сложных топологий.

В системах защищенной связи данные передаются по сетям связи общего пользования, а следовательно, доступны потенциальному нарушителю для проведения различных атак. Нарушитель способен сохранять закодированные данные, передаваемые в канале, а попытку декодирования производить в будущем, когда новые технические возможности и способы атаки на алгоритмы защиты информации позволят провести раскодирование за приемлемое время. В этом заключается принцип «Store now, decrypt later», указываемый одной из основных проблем систем защиты информации в работах [1], [2].

В то же время для известных блочных шифров существует параметр, называемый нагрузкой на ключ, ограничивающий объемы данных, которые можно обработать на одном ключе с применением конкретного алгоритма защиты. Так, рекомендации NIST [3] дают временные рамки использования ключей, исчисляемые годами.

Уполномоченный федеральный орган в сфере информационной безопасности вносит гораздо более существенные ограничения нагрузки на ключ в документе [4], связанные с числом блоков, которые можно обработать на одном ключе, обусловленные известными атаками на блочные шифры, в том числе по побочным каналам, и возможностями потенциального нарушителя в зависимости от класса средства защиты информации (СЗИ), в котором применяется рассматриваемый алгоритм защиты. При таких ограничениях возникает потребность регулярной смены используемого ключа, а следовательно, и поиск вариантов доставки и/или генерации таких ключей между двумя устройствами,

организующими защищенный канал. Смена ключа на новый, независимый от предыдущего, позволяет добиться защиты передачи будущей информации при компрометации текущего ключа.

Отдельно стоит отметить обеспокоенность научного сообщества угрозой создания квантового компьютера. Данная технология позволяет эффективно атаковать известные схемы генерации ключей, основанные на сложности вычисления дискретного логарифма или факторизации больших чисел. Квантовый алгоритм Шора, описанный в работах [5], [6], позволяет решать данные задачи за полиномиальное время, поэтому необходимо уже сейчас искать альтернативные варианты решения задачи регулярной смены секретного ключа в паре устройств.

Важно учитывать необходимость обеспечения свойства *Perfect forward secrecy*, т.е. при компрометации мастер-ключа все последующие ключи должны оставаться не скомпрометированными. Одним из способов достижения такого свойства алгоритмов кодирования является периодическое обновление мастер-ключей на новые, независимые от ранее использованных.

Для предотвращения накопления материала для атак потенциальным нарушителем и удовлетворения требования нагрузки на ключ необходимо решить задачу регулярной смены этого ключа, а соответственно, регулярной доставки и/или генерации этих ключей в сопряженной паре устройств.

Известны следующие способы доставки/генерации секретного ключа.

1) Доставка с помощью доверенного курьера.
2) Доставка с помощью алгоритмов с секретным ключом.
3) Генерация ключа с помощью схем выработки ключа на основе вычислительно сложных задач.

Первый способ доставки подразумевает привлечение значительных человеческих ресурсов. Более того, доставка ключевого материала на дальние расстояния требует значительного времени и, возможно, существенных финансовых ресурсов. Поэтому такой способ не решает задачу регулярной смены секретных ключей.

Доставка ключей с помощью алгоритмов с секретным ключом требует наличие предварительно распределенного секрета. В то же время существует та же самая проблема выработки нагрузки на ключ и смены ключа защиты канала передачи секретных ключей. Поэтому необходимо искать альтернативные варианты доставки ключей.

Использование классических ассиметричных алгоритмов, основанных на решении сложных математических задач, также оказывается небезопасным из-за описанных выше возможностей квантового компьютера (в том числе для применения алгоритма Шора) и нарушителя сохранять данные для получения доступа к ним в будущем, когда развитие уровня техники и технологии позволит преодолевать используемые в прошлом меры защиты.

Среди новых технологий доставки и генерации секретных ключей можно выделить два перспективных способа.

1) Распределение ключей с помощью технологии квантового распределения ключей (КРК).
2) Генерация ключей между двумя участниками с помощью постквантовых алгоритмов.

Второй вариант основывается на математических задачах, сложных для вычисления даже на квантовом компьютере. Текущий уровень проработки таких алгоритмов не достаточен для их внедрения в существующие системы. Скорость работы и необходимые длины ключей таких алгоритмов не позволяют создавать эксплуатационно-оправданные образцы. Более того, существует опасность, что после создания эффективного квантового компьютера появятся новые квантовые алгоритмы, позволяющие эффективно решать задачи, положенные в основу постквантовых алгоритмов. Такие алгоритмы создадут новые вектора атак на постквантовые алгоритмы и потребуют пересмотра проблемы регулярной доставки секретных ключей.

Таким образом, проблема распределения ключей между парами пользовательских устройств является актуальной научной проблемой, требующей решения в условиях появления новых угроз, связанных с созданием квантового

компьютера. Существующие решения разрабатывались задолго до развития квантовых коммуникаций и квантовых вычислений и не учитывают появляющиеся новые вектора атак с применением квантовых устройств.

Вариант распределения ключей с применением технологии квантового распределения ключей выглядит наиболее перспективным для решения поставленной научной проблемы. Распределение, а точнее генерация идентичных ключей на двух концах квантового канала основывается на совершенно иных физических принципах, что предотвращает возможность проведения эффективных атак с применением квантового компьютера и не позволяет проводить классические атаки с накоплением защищенных данных, как в случае с доставкой ключей с применением алгоритмов с секретным ключом. В то же время у технологии КРК есть ряд существенных ограничений, которые необходимо учитывать при проектировании систем доставки ключей на базе КРК.

Технология КРК позволяет распределять ключи на ограниченном расстоянии, которое определяется используемым протоколом КРК и качеством квантового канала. Для известных протоколов КРК на InGaAs/InP лавинных фотодиодах предельным считается расстояние порядка 100 км, о чем можно судить по представленным эксплуатационным характеристикам квантовой аппаратуры [7], [8], [9].

В текущей работе решается научная проблема безопасного распределения общего секрета для пар узлов, находящихся на расстоянии, превышающем допустимую длину квантового канала. Для этого усовершенствован известный подход построения сетей квантового распределения ключей с доверенными промежуточными узлами.

Простейшим случаем применения КРК является использование только двух экземпляров квантовой аппаратуры, соединенных квантовым каналом. То есть применение технологии в топологии «точка-точка». Это базовый конструктив, из которого в дальнейшем могут строиться распределённые сети с применением КРК. Протоколы КРК для такой топологии «точка-точка» активно разрабатываются и изучаются учеными-физиками. Неоспоримый вклад в развитие технологии КРК

внесли Ch. Bennett и G. Brassard, предложив первый протокол КРК BB84 [10]. Развитием протоколов КРК занимаются A. Poppe [11], [12], A. Shields [13], [14], С.Н. Молотков [15], [16], [17], [18]. В изучение применения технологии КРК в сетях смешанных топологий существенный вклад вносят N. Lütkenhaus [19], M. Mosca [20], [21], Группа В. Макарова вносит значимый вклад в анализ безопасности систем КРК, проводя исследования уязвимости реализаций систем КРК [22], [23], [24]. Устройства, реализующие протоколы КРК, разрабатываются в Китае [25], [26], США [27], Европе [28], [29] и России. В России сложилось три крупных центра разработки в области квантовых коммуникаций: МГУ имени М. В.Ломоносова совместно с АО «ИнфоТеКС» [30], Российский квантовый центр совместно с ООО «КуРейт» [31] и Национальный исследовательский университет ИТМО совместно с ООО «СМАРТС-Кванттелеком» [32], [33]. К сожалению, большинство работ, касающихся протоколов КРК и квантовой аппаратуры, посвящены физике процесса и не рассматривают реализацию неотъемлемой части квантовой аппаратуры, а именно классического аутентифицированного канала.

Любой квантовой аппаратуре требуется классический аутентифицированный канал. Способы построения такого канала с учетом требований, накладываемых разработчиками протокола КРК, рассматриваются в главе 2. Также существующие научные публикации не уделяют подробно внимание вопросам сопряжения квантовой аппаратуры и пользовательских устройств, СЗИ, для которых формируются общие секреты. По сути, квантовая аппаратура генерирует некоторую случайную последовательность, идентичную с двух концов квантового канала и неизвестную нарушителю. Однако существует задача формирования непосредственно общего секрета из такой последовательности, а также синхронизации переданных секретов в двух удаленных друг от друга СЗИ.

Для преодоления ограничения длины квантового канала аппаратура КРК объединяется в так называемые сети КРК. Однако получение истинно квантового ключа между двумя объектами сети, не связанными напрямую квантовым каналом, требует технологии квантовых повторителей, которая в настоящее время далека от практической реализации. Вопросы, касающиеся создания и применения

квантовых повторителей активно обсуждаются на международных конференциях [34], [35]. Подход, реализуемый в настоящее время, заключается в построении сетей КРК на базе доверенных промежуточных узлов. При данном подходе квантовые ключи вырабатываются только между узлами сети, соединенными напрямую квантовым каналом. На прочие узлы квантовой сети (УКС) одни квантовые ключи передаются под защитой других выработанных квантовых ключей.

В сетях КРК необходимо не только передавать ключевую информацию с применением квантовых ключей по цепочке УКС, но и осуществлять эти процессы в сетях смешанной топологии. Под смешанной топологией понимаются как топология связей УКС квантовыми каналами, так и топология классических связей между узлами, например, через сеть связи общего пользования, в том числе защищенные каналы взаимодействия между УКС. При этом граф, отображающий связи квантовыми каналами, должен быть связным. Работы в этом направлении осуществляются ведущими организациями по всему миру. В Китае создана и успешно функционирует сеть КРК, протяженностью более 2000 км [36]. Также ведутся работы по стандартизации сетей КРК, в том числе в ETSI [37] и в ITU-T [38]. Международная организация ISO занимается вопросами разработки требований по безопасности к квантовой аппаратуре и сетям КРК [39]. Создан европейский проект OpenQKD [40], предполагающий развертывание испытательных полигонов для тестирования наработок по созданию крупных сетей КРК и создания практически применимых промышленных образцов. В России, в рамках национальной программы «Цифровая экономика», принятой в соответствии с Указом Президента Российской Федерации от 7 мая 2018 года № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», утверждена дорожная карта развития «сквозной» цифровой технологии «квантовые технологии» [41]. Дорожная карта «разработана с целью получения в среднесрочной и долгосрочной перспективе практически значимых научно–технических и практических результатов мирового уровня по следующим субтехнологиям: квантовые вычисления, квантовые

коммуникации и квантовые сенсоры». В исполнение дорожной карты развития «сквозной» цифровой технологии утверждена дорожная карта ОАО «РЖД» развития высокотехнологичной области «Квантовые коммуникации» на период до 2024 года [42]. Целью дорожной карты ОАО «РЖД» является «ускорение технологического развития и достижение РФ позиций одного из лидеров на глобальных технологических рынках в высокотехнологичной области «Квантовые коммуникации».

Не решенным является вопрос как осуществлять распределение общих секретов на требуемые узлы сети КРК, в том числе есть ли способы избежать появления передаваемого по сети секрета в открытом виде на промежуточных УКС. Для решения этого вопроса в главе 3 разрабатывается методика распределения общего секрета в сети магистральной топологии.

В главе 4 формируются требования к многоуровневой структуре и функциям сети КРК, на основе которых формулируется методика построения сетей КРК смешанной топологии, включая методику распределения общего секрета на произвольные пары узлов сети.

Цели и задачи исследования

Целью работы является развитие методического обеспечения квантовых коммуникаций для повышения защищенности сетей квантового распределения ключей смешанной топологии.

Для этого решаются следующие задачи.

1) Разработка способа построения классического аутентифицированного канала квантовой аппаратуры.
2) Создание способа взаимодействия квантовой аппаратуры с пользовательскими СЗИ, уточняющего процессы синхронизации и обеспечения целостности общих секретов при их передаче в СЗИ.
3) Разработка методики распределения общего секрета для пары узлов сети КРК магистральной топологии.

4) Выработка методики построения сетей КРК смешанной топологии, включающей требований к структуре сети КРК смешанной топологии и способу функционирования такой сети.

Объектом исследования являются сети квантового распределения ключей смешанной топологии.

Предметом исследования является методика построения сетей квантового распределения ключей смешанной топологии с учетом требований безопасности.

Научная новизна

1. Разработана структура комплекса защищенной передачи данных, интегрированного с аппаратурой квантового распределения ключей, в том числе порядок функционирования такого комплекса для синхронизированной передачи ключевой информации в СЗИ, отличающийся от известных учетом целостности и конфиденциальности общих секретов в процессе передачи в СЗИ и контролем идентичности сформированных секретов, объединением классического канала аппаратуры КРК с транспортным каналом СЗИ для повышения защищенности классического канала аппаратуры КРК. Новизна предлагаемого решения подтверждается полученным патентом на изобретение [43].

2. Разработана методика распределения общих секретов в сети КРК магистральной топологии, отличающаяся сохранением стойкости распределенных общих секретов при компрометации квантовых ключей, а также возможностью сохранения конфиденциальности распределяемых секретов на промежуточных узлах сети КРК.

3. Предложена методика построения сети КРК смешанной топологии, включающая требования к структуре сети КРК, способу ее функционирования, методику распределения квантовозащищенных ключей (п. 2 новизны), отличающаяся от известных полностью децентрализованным управлением при создании квантовозащищенных ключей, учетом требований их целостности и конфиденциальности, а также имеющая по сравнению с зарубежными аналогами большую гибкость при масштабировании сети. Новизна предлагаемого решения подтверждается полученным патентом на изобретение [44].

Теоретическая и практическая значимость работы.

Результаты данной работы представляют развитие теории защиты информации в части применения технологии КРК для регулярной доставки общих секретов, в том числе в устройства, расположенные на расстояниях, существенно превышающих предельные длины квантовых каналов.

Введенное автором понятие квантовозащищенных ключей позволяет различать общий секрет, распределяемый в сети КРК, и квантовые ключи, создаваемые непосредственно в результате выполнения протокола КРК, в связи с чем уменьшается путаница при описании квантовой аппаратуры, сетей КРК, а также анализе их стойкости.

В то же время основные положения работы представляют практическую ценность для создания промышленных образцов квантовых сетей, что соответствуют, например, основным направлениям дорожной карты ОАО РЖД по развитию сквозной цифровой технологии квантовых коммуникаций [42]. Предложенная структура базового сегмента сети КРК топологии «точка-точка» позволяет минимизировать число каналов между географически разнесенными узлами, что приводит к упрощению развертывания таких пар узлов.

Полученные результаты успешно применены при создании комплексов ViPNet Quandor и ViPNet QSS, а также положены в основу комплексного проекта «Разработка технологии и аппаратуры сетей квантового распределения криптографических ключей с использованием доверенных узлов», выполняемого по соглашению с Министерством промышленности и торговли РФ № 020-11-2019-933 от 19.11.2019.

Методы исследования

При проведении исследования использованы методы системного анализа, теории защиты информации, теории кодирования, теории квантового распределения ключей. В работе использованы такие общенаучные методы, как восхождение от абстрактного к конкретному, декомпозиция задачи и объекта исследования на подзадачи, анализ аналогов исследуемых объектов при различной степени детализации разбиения и синтез решений на базе проведенного анализа.

Положения, выносимые на защиту.

1) Структура комплекса защищенной передачи данных, состоящего из пары СЗИ и пары квантовой аппаратуры, и способ доставки общих секретов в таком комплексе, позволяющий контролировать идентичность формируемых в квантовой аппаратуре секретов с секретами, полученными парой СЗИ.

   Соответствует пункту 6 паспорта специальности 05.13.19: модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования.

2) Методика распределения общего секрета в оконечные узлы магистральной сети квантового распределения ключей, позволяющая повысить защищенность распределяемых секретов за счет сохранения конфиденциальности распределяемых секретов на промежуточных узлах сети, контроля целостности секретов при их передаче между узлами сети, а также сохранении общего секрета нескомпрометированным даже при компрометации квантовых ключей.

   Соответствует пункту 8 паспорта специальности: модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем.

3) Методика построения сетей КРК смешанной топологии, включая требования к структуре и функциям такой сети, позволяющая конструировать децентрализованные сети КРК.

   Соответствует пункту 13 паспорта специальности: принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Степень достоверности и апробация результатов

Достоверность и обоснованность результатов и выводов работы подтверждается анализом современного состояния исследований в предметной области, обоснованием предложенных методик, не противоречащих известным положениям других авторов, апробацией полученных результатов в научных публикациях и докладах на международных и российских научных и научно-практических конференциях, положительным эффектом внедрения результатов в экспериментальные макеты сетей КРК (Университетская квантовая сеть, ViPNet QTS), промышленные комплексы систем КРК (ViPNet Quandor, ViPNet QSS, Квазар-СКР), а также использованием результатов работы в проектах документов национальной системы стандартизации.

Основные положения диссертации представлены в рецензируемых журналах ВАК [30], [45], [46], [47] и Scopus, [48] [49]. Основные результаты диссертационной работы апробированы на международных конференциях по соответствующей тематике в виде докладов [50], [51], [52]. Получены патенты РФ на изобретения № 2708511 Жиляев А.Е. Способ формирования ключа между узлами вычислительной сети с использованием системы квантового распределения ключей [53]; № 2736870 Втюрина А.Г., Жиляев А.Е. Комплекс для защищенной передачи данных в цифровой сети передачи данных с использованием однопроходной системы квантового распределения ключей и способ согласования ключей при работе комплекса [43]; № 2752844 Жиляев А.Е. Система выработки и распределения ключей и способ распределенной выработки ключей с использованием квантового распределения ключей (варианты) [44].

Внедрение

Результаты данной диссертационной работы применены при разработках комплексов ViPNet Quandor, ViPNet QSS [54], [55], положены в основу комплексного проекта «Разработка технологии и аппаратуры сетей квантового распределения криптографических ключей с использованием доверенных узлов», а также в основу проекта методических рекомендаций, разрабатываемых рабочей группой ТК26. Имеется 4 акта внедрения (приложение Б).

1 АНАЛИЗ ТЕКУЩЕГО СОСТОЯНИЯ

В этой главе проводится анализ технологии квантового распределения ключей и особенности квантовой аппаратуры, реализующей данную технологию. В п. 1.1 рассматривается структура протоколов КРК и формулируются проблемы, препятствующие массовому и эффективному применению данной технологии. В п. 1.2 анализируются известные способы построения сетей, использующих технологию КРК. В п. 1.3 формируются цели и задачи настоящего исследования исходя из проблем, сформулированных в п. 1.1 и п. 1.2.

1.1 Описание технологии и типовой архитектуры системы квантового распределения ключей

Технология КРК – технология получения идентичных случайных последовательностей двумя абонентами, сформированных с использованием передачи некоторой информации между этими абонентами с применением квантовых частиц. Два абонента используют специальную квантовую аппаратуру (аппаратуру КРК), которая реализует некоторый протокол КРК.

Протокол КРК – протокол кодирования, который включает:

– способ приготовления и преобразования информационных квантовых состояний в одном устройстве. Такое устройство должно иметь в своем составе источник квантовых состояний;
– способ передачи информационных квантовых состояний по квантовому каналу;
– способ преобразования, регистрации и интерпретации результатов измерений на сопряженном устройстве;
– способ обработки последовательности, полученной по результатам измерений, с применением открытого классического аутентифицированного канала связи. Обычно обработка включает этапы коррекции ошибок и усиления секретности.

Целью протокола КРК является получение квантового ключа, идентичного на обеих сторонах квантового канала.

Квантовая аппаратура, реализующая протокол КРК, представляет собой комплекс из двух устройств, соединенных квантовым каналом. Упрощенная архитектура комплекса приведена на рисунке 1.

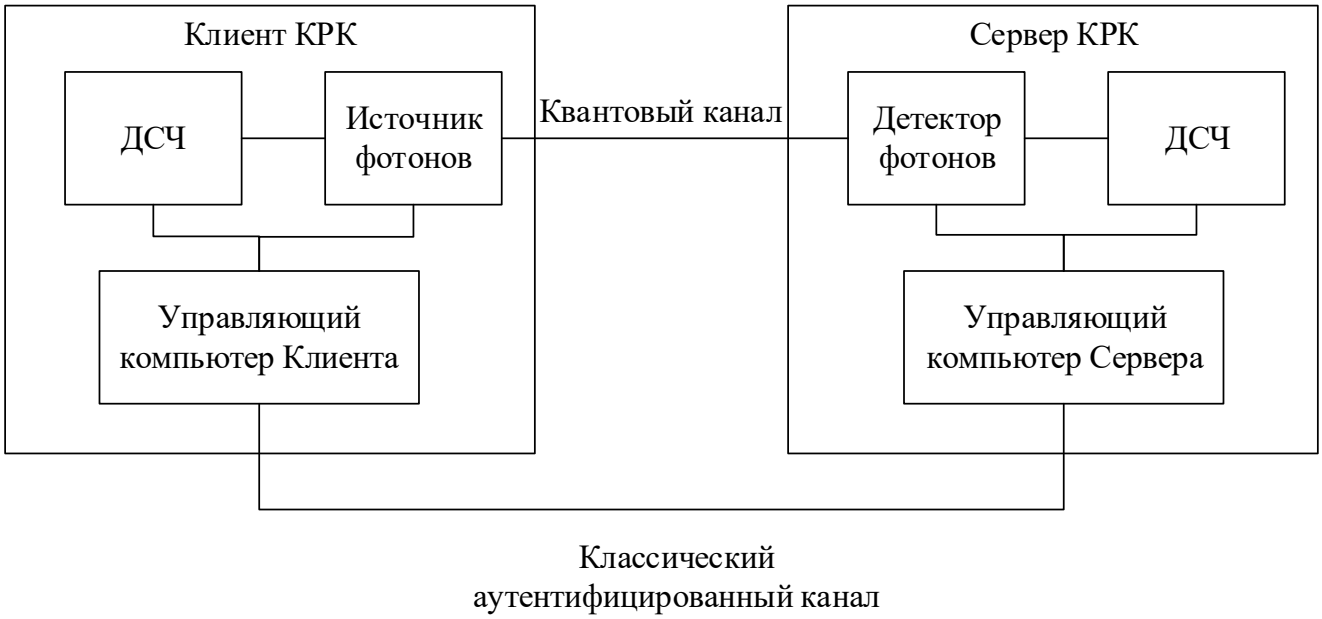


Рисунок 1 – Схема комплекса квантовой аппаратуры

Одно из устройств комплекса, содержащее генератор (источник) одиночных фотонов, принято называть Клиентом КРК. Сопряженное устройство, содержащее детектор (приемник) одиночных фотонов, называют Сервер КРК. Каждое из устройств содержит датчик случайных чисел (ДСЧ). Причем рекомендуется использовать датчики, в основе случайных процессов которых лежат квантовые эффекты, что показано в работе [56]. Таким образом можно получить истинно случайную последовательность, из которой в дальнейшем будет формироваться квантовый ключ.

Сервер КРК и Клиент КРК соединены двумя логическими каналами: квантовым и классическим. Квантовый канал предназначен для передачи квантовых информационных состояний, фотонов, обычно реализуется оптоволокном. Существуют системы КРК, в которых в качестве квантового канала используется воздушная среда передачи, однако они находятся пока в стадии лабораторных установок [57], [58], [59]. Важной особенностью технологии КРК

является полная доступность квантового канала для нарушителя, т.е. данный канал не контролируется и не защищается от внедрения нарушителя в канал. Помимо квантового канала Сервер КРК и Клиент КРК должны быть соединены классической линией связи, в которой реализуется логический классический канал, именуемый далее классическим аутентифицированным каналом. К данному каналу предъявляются требования по обеспечению целостности передаваемых данных и аутентификации отправителя данных.

Реальная система КРК дополнительно имеет логический служебный канал данных, соединяющий Клиент КРК и Сервер КРК, в котором передаются команды и данные управления и мониторинга аппаратуры, не связанные непосредственно с протоколом КРК. Отметим, что в зависимости от конкретной реализации системы КРК состав этих команд и данных может потребовать обеспечения не только их целостности, но и конфиденциальности. Для функционирования системы КРК в квантовую аппаратуру необходимо загрузить предварительно распределенные ключи, которые требуются как минимум при построении классического аутентифицированного канала до первой успешной выработки достаточного количества квантовых ключей. Одну итерацию реализации протокола КРК будем именовать сеансом КРК.

Обычно каждый сеанс КРК состоит из следующих неотъемлемых этапов

1) Подготовка квантового канала.
2) Передача одиночных фотонов по квантовому каналу.
3) Постобработка переданной последовательности.

Первые два этапа непосредственно задействуют квантовый канал. В результате передачи по квантовому каналу у обоих устройств появляется так называемый сырой ключ. Последний этап протокола КРК выполняется без использования квантового канала, а только через классический аутентифицированный канал.

Этап постобработки включает в себя три подэтапа.

1) Согласование базисов измерения на стороне приемника с базисами кодирования квантовых состояний на стороне источника. В результате согласования позиций сырого ключа, в которых базисы не совпали, отбрасываются, а сырой ключ преобразует в просеянный ключ.
2) Исправление ошибок в полученных просеянных ключах с целью получить идентичные последовательности в Сервере и Клиенте КРК. Результат исправления ошибок называется очищенным ключом.
3) Усиление секретности, представляющее собой сжатие полученных идентичных последовательностей с целью уменьшения информации о генерируемом квантовом ключе, доступной нарушителю. В результате усиления секретности очищенный ключ преобразуется в секретный квантовый ключ.

На рисунке 2 представлена обобщенная последовательность выполнения протокола КРК.

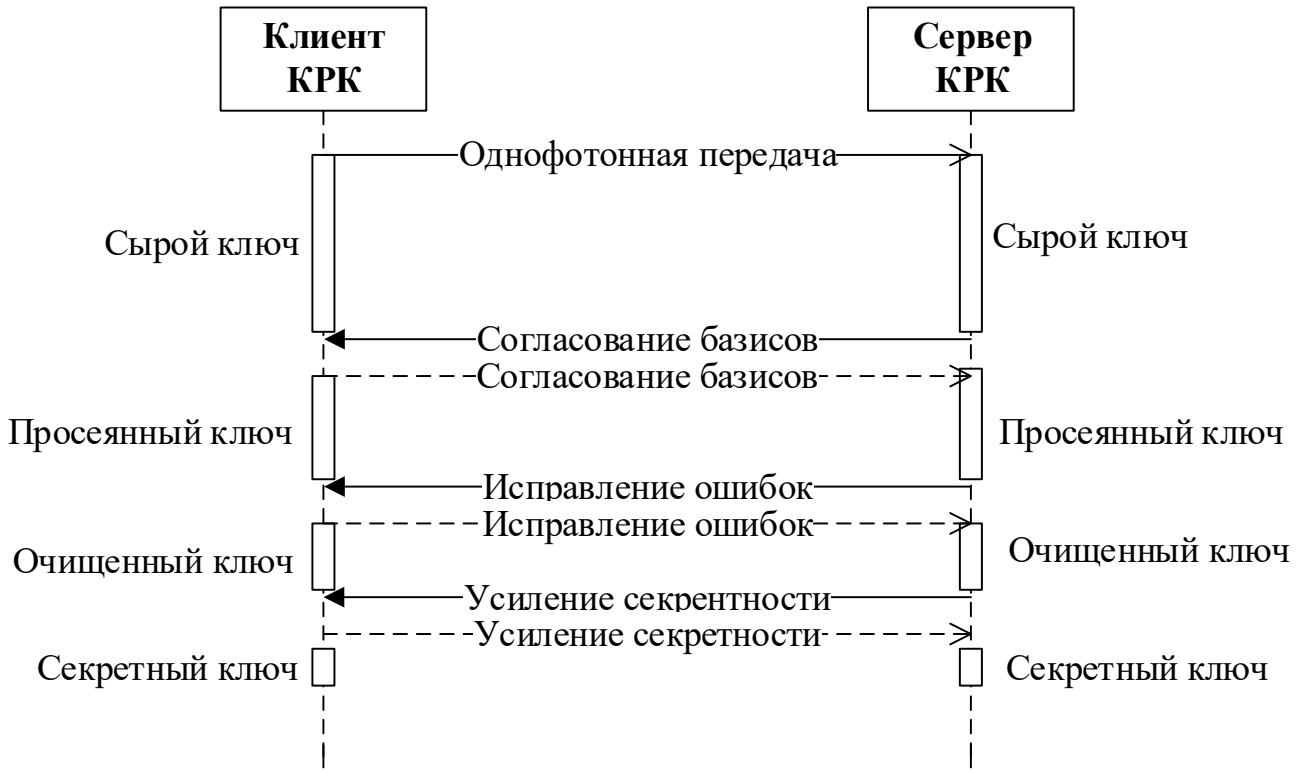


Рисунок 2 – Последовательность выполнения протокола КРК

Требуется отметить, что результат работы квантового протокола не совсем корректно называть квантовым ключом. Корректнее говорить, что результатом сеанса КРК является случайная квантовая гамма, идентичная у двух абонентов, так как этот результат имеет переменную длину, не всегда совпадающую с длиной ключей, использующихся в алгоритмах кодирования. Более того, результат выполнения одного и того же протокола КРК существенно отличается для квантовых каналов с низкими и высокими потерями, которые напрямую влияют на величину ошибок при передаче в квантовом канале (QBER), что в свою очередь влияет на величину информации о квантовой гамме, доступной нарушителю и уменьшаемой на этапе усиления секретности. Для краткости далее под квантовым ключом будем понимать именно случайную квантовую гамму.

Согласно экспериментальным данным, приведенным в работе [60], при длине линии в 50 км (что соответствует потерям 10 дБ при типовых потерях в ВОЛС 0,2 дБ/км [61]) эффективность выработки квантовых ключей, т.е. отношение числа зарегистрированных импульсов на сервере КРК к полному числу импульсов, отправленных клиентом КРК, составляет 2×10^{-5}. Так, для получения 256-битного квантового ключа при длине линии связи в 50 км за один сеанс КРК требуется последовательность импульсов 2×10^{7}. Потери при длине квантового канала 100 км составляют 20 дБ, т. е. в 10 раз больше, чем при длине 50 км. Поэтому для выработки 256-битного квантового ключа за один сеанс КРК длина последовательности импульсов, передаваемая в квантовый канал, должна быть в 10 раз больше, т. е. составлять не менее 2×10^{8} импульсов.

Оценим объем случайных чисел, необходимый для одного сеанса КРК, в результате которого должен получиться квантовый ключ длиной не менее 256 бит. Длина ключа 256 бит взята как типовая для стандартизованных алгоритмов с секретным ключом (например, Магма, Кузнечик [62]). Для кодирования информационного состояния протокола КРК необходимо минимум 2 бита информации. Один бит определяет базис кодирования или базис измерения, второй непосредственно значение передаваемого информационного бита 0 или 1. Более сложные протоколы КРК, например, протокол ГОКС на геометрически

однородных когерентных состояниях [15], могут иметь 3 и более бит для кодирования информации в однофотонном состоянии. Исходя из экспериментальных данных для одного сеанса КРК необходима случайная последовательность длиной не менее 4×10^8 бит. Оценим снизу необходимую скорость генерации для получения 256 бит ключа в секунду. Пусть имеется идеальный протокол КРК, который за секунду переводит все импульсы в квантовый ключ. Тогда скорость ДСЧ должна быть не менее 4×10^8 бит/с или 400 Мбит/с. Если учитывать, что часть квантового ключа используется для аутентификации следующего сеанса КРК, то фактическая скорость генерации квантовых ключей должна учитывать требуемый размер ключа аутентификации, что увеличит нижнюю оценку на скорость ДСЧ.

К датчикам случайных чисел в системах КРК предъявляют строгие требования, касающиеся природы случайности и, соответственно, качества формируемой последовательности [56], [63]. В то же время скорость физических датчиков, в основе которых лежат квантовые процессы, ограничена [64], что ведет к ограничению предельных скоростей выработки квантовых ключей скоростями доступных датчиков случайных чисел.

Таким образом, для корректного построения протокола КРК и получения необходимого качества квантовых ключей требуется осуществление передачи информации по квантовому каналу, построение классического аутентифицированного канала и наличие датчика случайных чисел соответствующего качества как источника энтропии для создаваемых квантовых ключей.

Множество теоретических работ, описывающих физическую сторону технологии КРК, не уделяют должного внимания построению классического аутентифицированного канала. Для создания такого канала необходимо определить способ обеспечения целостности данных и аутентификации источника данных. Типовым решением является вычисление имитовставки от передаваемых сообщений для обеспечения целостности данных. Аутентификация отправителя данных при этом осуществляется за счет использования секретного ключа,

известного только паре легитимных абонентов. Широко распространенным способом вычисления имитовставки является применение вычислительно стойких функций хэширования, таких как ГОСТ 34.11-2018 [65]. Ряд работ [66], [67] рекомендуют применение функций универсального хэширования в качестве функций вычисления имитовставки для классического аутентифицированного канала систем КРК. При этом функции универсального хэширования требуют значительно больше ключевого материала для формирования одной имитовставки. Полагается, что квантового ключа, создаваемого в результате одного сеанса КРК, должно хватать и для аутентификации следующего сеанса, и для формирования полезного секрета, который будет передан абонентам.

Стоит учитывать, что квантовая аппаратура не используется сама по себе, а является источником общих секретов для пользовательских устройств, СЗИ. Классический аутентифицированный канал в силу разных причин, например, для экономии числа физических каналов, соединяющих устройства, может быть реализован через пользовательские СЗИ. Открытым научным вопросом является способ обеспечения аутентификации канала.

Более того, в работе квантовой аппаратуры необходимо учитывать, что возможны однократные и множественные прерывания сеанса КРК из-за нарушения целостности данных в классическом аутентифицированном канале в связи с действиями нарушителя или случайными сбоями. Каждый повторный запуск сеанса КРК ведет к дополнительному расходу ключей аутентификации.

Другой важной научной проблемой, не рассмотренной в научной литературе, является собственно передача созданного квантового ключа от квантовой аппаратуры абонентам, а точнее пользовательским устройствам, которые будут использовать этот квантовый ключ. В отличие от классических систем, взаимодействие квантовой аппаратуры с СЗИ происходит одновременно в двух парах устройств: Сервер КРК – СЗИ и Клиент КРК – СЗИ. Квантовый ключ создается в одной паре устройств (квантовой аппаратуре), а должен попасть в пару других устройств, СЗИ. При этом, в отличие от классических систем, небезопасно применение алгоритмов, не стойких к атакам с применением квантового

компьютера, а возможности безопасного взаимодействия географически удаленных устройств ограничены. Такие устройства могут иметь только предварительно распределенный ключ для организации безопасного взаимодействия или, что хуже, не иметь никакого первичного общего ключа. Формирование общих секретов пользовательских устройств ассиметричными методами небезопасно из-за атак с применением квантового компьютера.

Научной проблемой является достижение синхронизации передаваемой в СЗИ гаммы в описанных условиях, так, чтобы пара сопряженных СЗИ использовала гарантированно идентичные общие секреты, а также могла их однозначно идентифицировать.

Таким образом, можно перечислить ряд нерешенных научных проблем в распределении общих секретов с применением КРК в топологии точка-точка:

– способ организации классического аутентифицированного канала аппаратуры КРК, включающий способ формирования имитовставки для обеспечения целостности и источник ключей для формирования имитовставки.
– организация защищенной передачи общих секретов в СЗИ, стойкой к атакам квантовым компьютером;
– необходимость синхронизации передаваемой в пару СЗИ ключевой гаммы в условиях отсутствия возможности взаимодействия этих СЗИ до получения первичных ключей.

Решение обозначенных научных проблем позволит применять технологию КРК для систем в топологии «точка-точка» для регулярного распределения общих секретов в пользовательские устройства.

1.2 Анализ известных способов преодоления максимальной дальности создания квантовых ключей

Все протоколы КРК имеют предельную длину квантового канала, на которой возможно создание квантовых ключей. В среднем максимальная длина

квантового канала для волоконных систем КРК составляет 100 км [10], [15]. Однако, пользовательские устройства, на которые необходимо распределять общие секреты, располагаются произвольно. В связи с этим встает задача преодоления максимальной удаленности устройств квантовой аппаратуры с целью создания общих секретов для пар устройств с неограниченным расстоянием между ними.

Первыми шагами в решении данной проблемы можно считать создание специальных протоколов КРК, использующих один недоверенный промежуточный узел, либо Сервер КРК, либо Клиент КРК. К таким протоколам относятся протоколы MDI-QKD [68], [69] и Twin-Field QKD [13]. Основная идея этих протоколов заключается в том, что абоненты используют два экземпляра квантовой аппаратуры одного типа (два Сервера КРК или два Клиента КРК), каждый из которых является доверенным узлом и соединен с промежуточным недоверенным узлом другого типа. Специальная структура протокола КРК позволяет без кодирования квантовых информационных состояний на промежуточном недоверенном узле сообщить каждому абоненту достаточную информацию для формирования сырого ключа. В результате применения подобных протоколов в среднем удваивается максимальное расстояние между абонентами, получающими секретный ключ, так как фактически имеется два квантовых канала, каждый из которых не должен превышать максимальной длины, определенной протоколом КРК [70].

К сожалению, данные типы протоколов КРК не решают задачи создания общего секрета для двух произвольно расположенных абонентов, а дают только удвоение максимальной дальности.

Следующим шагом в решении проблемы максимальной удаленности абонентов является использование одного из двух подходов: применение сетей КРК на основе доверенных промежуточных узлов и применение сетей КРК на основе недоверенных промежуточных узлов. В каждом случае речь идет о сетях смешанной топологии, в которых необходимо иметь возможность распределять общий секрет на произвольные пары узлов сети.

В основе сетей КРК с множеством недоверенных промежуточных узлов лежит применение спутанных фотонов и ячеек квантовой памяти, расположенных на промежуточных узлах. Описание подобных сетей приводится в работах [71], [72]. В настоящее время квантовая память является абстрактным объектом, не имеющим физического воплощения, поэтому сети КРК с недоверенными промежуточными узлами являются перспективным, но не реализуемым подходом в ближайшее время.

В основу сетей КРК с доверенными промежуточными узлами заложена идея последовательной передачи некоторого квантового ключа, полученного на некотором сегменте сети КРК, через промежуточные узлы на требуемые узлы, на которые необходимо распределить общий секрет [73], [74], [75]. Далее все узлы такой сети КРК будем именовать узлами квантовой сети (УКС). Система, описанная в п. 1.1, с учетом решения обозначенных ранее проблем, является базовым блоком при построении сетей КРК с доверенными промежуточными узлами и минимальным сегментом такой сети.

Известный подход, предложенный в работе [76], конкретизирует один из способов распределения общего секрета путем использования одного из квантовых ключей, полученного на некотором сегменте сети КРК. Этот квантовый ключ назначается общим секретом для оконечных УКС. В теоретической модели для передачи общего секрета на оконечные УКС используется последовательная передача по цепочке УКС с защитой на квантовых ключах соответствующего сегмента. При этом на каждом УКС происходит перекодирование общего секрета, и он появляется в открытом виде на промежуточных УКС. Отсюда следует требование, при котором УКС сети КРК должны быть доверенными и должен быть невозможен доступ нарушителя к общим секретам, появляющимся в УКС в открытом виде. В качестве алгоритма кодирования в публикациях, касающихся применения технологии квантового распределения ключей, обычно выбирают одноразовый шифроблокнот (One-Time Pad Encryption) [27], [76], [77], [78].

Описанный способ формирования общего секрета для магистральной сети из четырех УКС представлен на рисунке 3.

Пусть есть сеть КРК из узлов УКС1, УКС2, УКС3, УКС4. Узлы УКС1 и УКС4 целевые, между ними необходимо сформировать общий секрет. Сначала между парами УКС вырабатываются квантовые ключи КК12, КК23, КК34. Затем общим секретом пары целевых УКС назначается один из выработанных квантовых ключей, например, ключ КК12. Он уже есть на УКС1, теперь необходимо доставить его на УКС4. Для этого на УКС2 получают закодированный текст путем кодирования ключа КК12 на ключе КК23. Закодированный текст передается на УКС3, раскодируется на ключе КК23. Теперь на УКС3 тоже есть КК12.

Аналогичным образом КК12 передается с УКС3 на УКС4 в закодированном виде. В качестве ключа кодирования используется КК34. Раскодировав полученный закодированный текст на УКС4 с помощью ключа КК34 получают КК12. Таким образом на обоих оконечных УКС имеется общий ключ КК12, который используется в качестве общего секрета для передачи из сети КРК внешним устройствам.

Существенным недостатком предлагаемого подхода при передаче ключа является решение только задачи обеспечения конфиденциальности передачи, но не целостности ключа. Кроме того, предлагается использовать квантовый ключ некоторого сегмента, т.е. ключ, о котором у нарушителя есть некоторая, пусть малая информация. Также передаваемый ключ в явном виде появляется на каждом промежуточном узле. Использование одноразового шифроблокнота предполагает однократное применение квантовых ключей, что влечет существенный расход квантовых ключей каждого сегмента. Таким образом, известный базовый подход может рассматриваться как начальный шаг при синтезе способов распределения общего секрета для произвольных УКС, но требует дальнейшей проработки и устранения описанных недостатков.

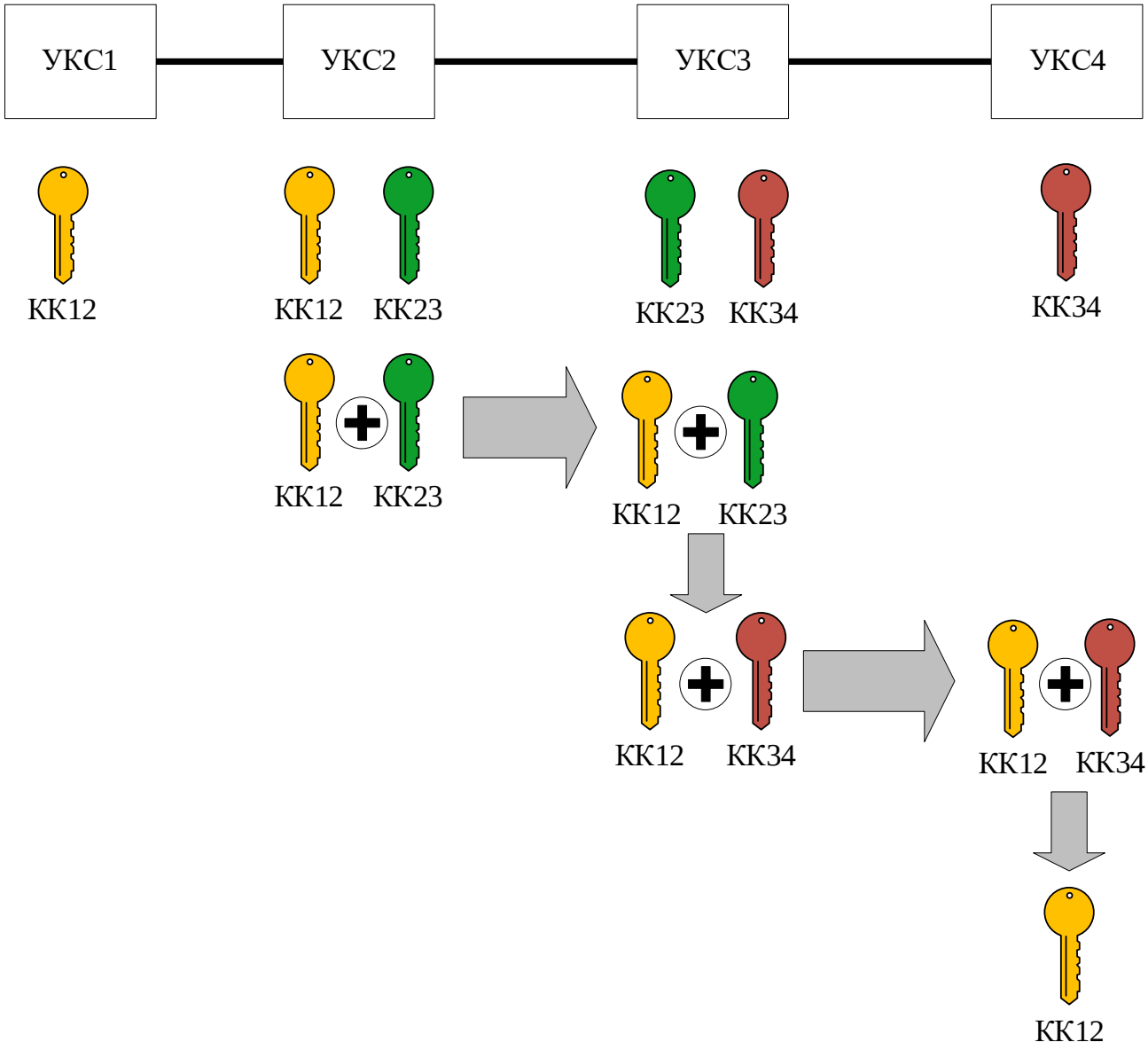


Рисунок 3 – Базовый способ формирования секретного ключа через цепочку УКС

Одним из известных вариантов решения проблемы появления ключевой информации в открытом виде на промежуточных УКС является способ, описанный А.М. Поздняковым в патенте РФ № 2697696 [79]. Данный способ показывает применение строго стандартизованных классических методов для защищенного представления ключевой информации на промежуточных УКС. Для понимания указанного способа рассмотрим схему магистральной сети КРК, представленной на рисунке 4.

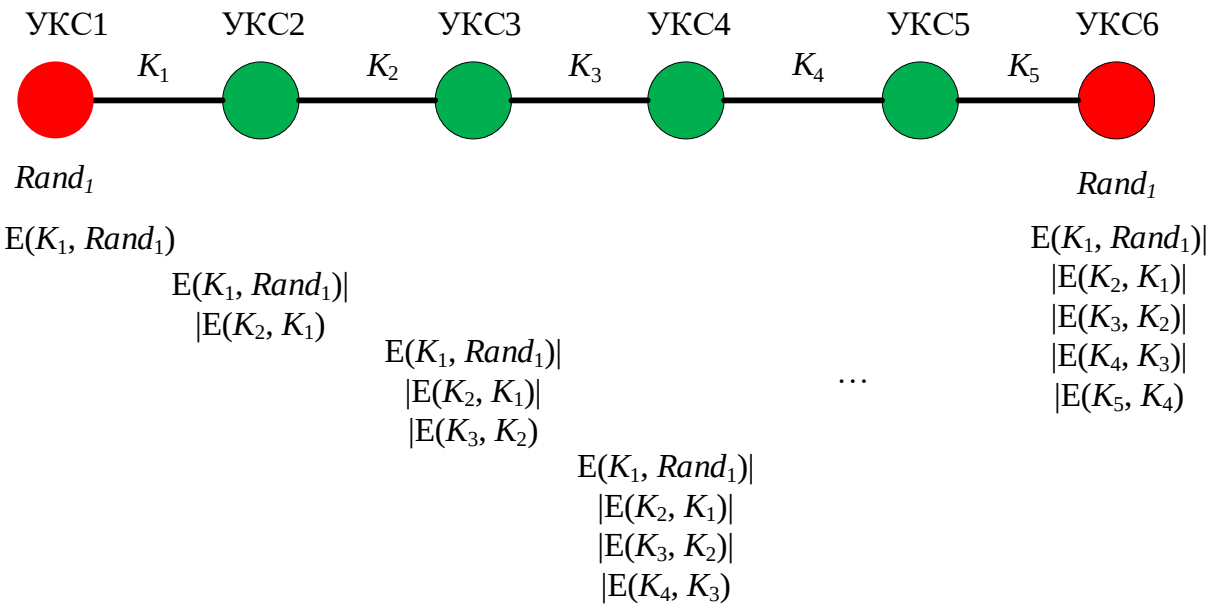


Рисунок 4 – Способ передачи секретного ключа «матрешкой»

Для защиты непосредственно ключевой информации $Rand_1$, назначаемой общим секретом целевых УКС, используется квантовый ключ первого сегмента K_1сети КРК. Формируется закодированный текст $C_1 = \mathrm{E}(K_1, Rand_1)$. Данный закодированный текст передается по цепочке узлов до второго целевого УКС, т.е. УКС6. Для раскодирования на УКС6 необходим квантовый ключ K_1. Он передается от УКС2 сети КРК, с защитой на квантовом ключе K_2, т.е. $C_2 = \mathrm{E}(K_2, K_1)$. Формирование и передача C_i продолжается до тех пор, пока не будет передан предпоследний квантовый ключ K_4, закодированный на квантовом ключе последнего сегмента K_5.

Теперь целевой УКС6 может в обратном порядке раскодировать все полученные закодированные тексты, получив в итоге переданную ключевую информацию $Rand_1$.

Заметим, что несмотря на отсутствие требований к функции кодирования в описании патента, необходимо применять независимый набор квантовых ключей для каждой магистральной подсети КРК выделенной в некоторой сети КРК смешанной топологии даже при пересечении на некоторых сегментах нескольких магистральных подсетей. Иначе передаваемые общие секреты разных подсетей

КРК будут иметь связь по ключам защиты, использованных при кодировании на пересекающихся сегментах.

В то же время, если достаточно обеспечивать вычислительную стойкость при распределении общего секрета целевых УКС, то для выделенной магистральной подсети КРК передачу ключей защиты общего секрета по сегментам необходимо осуществить только один раз, а затем можно сформировать несколько закодированных текстов C_1 от нескольких сообщений X для формирования нескольких общих секретов. Допустимое количество различных закодированных текстов на одном ключе первого сегмента зависит от допустимой нагрузки на ключ кодирования для конкретного выбранного алгоритма кодирования.

Как видно из приведенного описания, добавление новых УКС в цепочке между целевыми УКС существенно увеличивает объем передаваемой защищенной информации при попытке не допустить появления передаваемых КЗК на промежуточных УКС в открытом виде классическими методами.

Достоинствами данного способа являются:

– отсутствие перекодирования передаваемых общих секретов на промежуточных УКС, что решает проблему появления общих секретов на промежуточных УКС в открытом виде;
– теоретико-информационная стойкость защиты при передаче ключей при применении соответствующих алгоритмов кодирования и строго однократном применении квантовых ключей;
– возможность сокращения числа передаваемых закодированных текстов при формировании вычислительно стойких общих секретов для фиксированной магистральной подсети КРК с целью повышения скорости распределения общих секретов.

В то же время существенным недостатком способа является пропорциональное увеличение объема передаваемых закодированных сообщений от числа сегментов в сети КРК.

Существует другой способ, основанный на схемах разделения секрета. Итоговый общий секрет разделяется на доли некоторой схемой разделения секрета, после чего доставляется на целевые УКС по разным цепочкам УКС [80], [81]. В результате нарушителю необходимо получить доступ к множеству УКС из разных цепочек для того, чтобы получить доступ к общему секрету.

Таким образом, определена основа способа распределения общего секрета и наблюдаются попытки устранения основных недостатков способа. Однако, совершенствование способа распределения общего секрета на данный момент является нерешенной научной задачей.

1.2.1 Анализ структуры сети КРК по версии ETSI

В настоящее время ведутся работы в области стандартизации сетей КРК в части архитектуры таких сетей и способов их функционирования.

Группа стандартизации ETSI в области квантового распределения ключей (ISG QKD) [37] с 2010 года начала разрабатывать стандарты, касающиеся технологии КРК, базируясь на результатах хорошо известного проекта SECOQC (Secure Communication based on Quantum Cryptography) [82]. Эти стандарты касаются разных областей применения КРК: секретности протоколов и реализаций КРК, интерфейсов взаимодействия, методов измерений и др. Многие стандарты и спецификации, разработанные в 2010 году, пересматриваются и дополняются в настоящее время.

Первый вариант сети КРК был представлен в описании интерфейса взаимодействия квантовой аппаратуры и СЗИ в документе [83]. Сеть КРК построена из доверенных узлов, как показано на рисунке 5.

В сценарии взаимодействия согласно ETSI GS QKD 004 участвуют:

– Аппаратура КРК – QKD.

– Сервер управления квантовыми ключами – KML.

– Сервер управления ключами – KMS.

– Клиенты сети, пользовательские приложения – App.

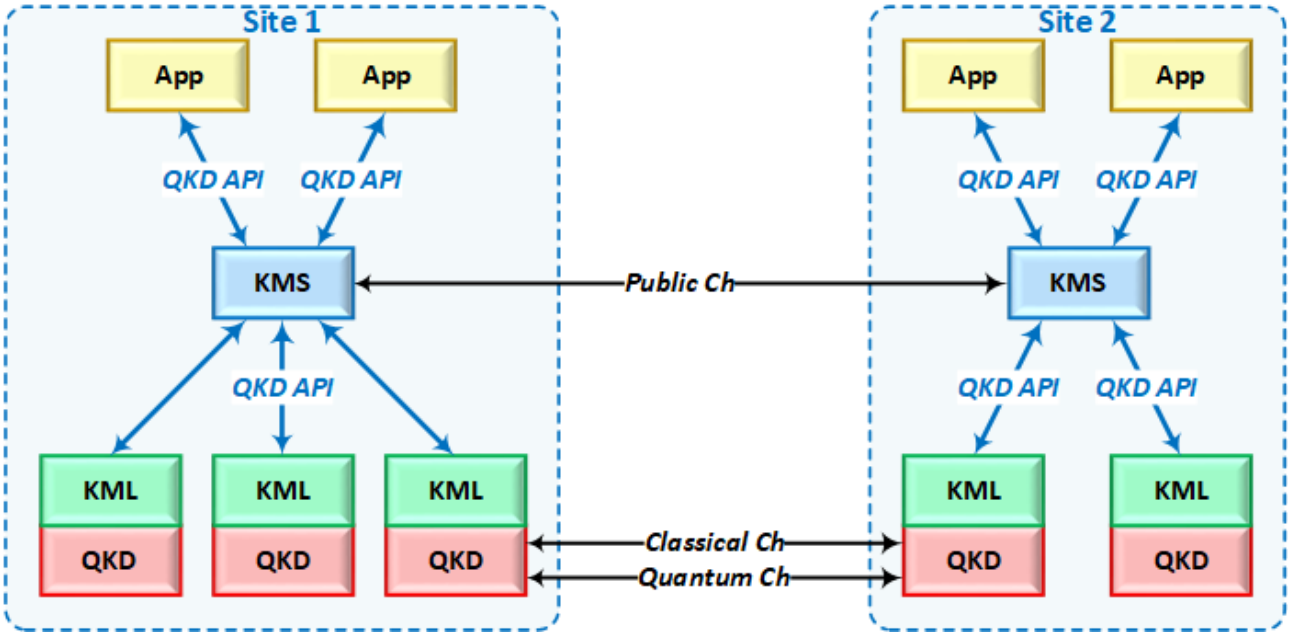


Рисунок 5 – Структура сети КРК по версии документ ETSI GS QKD 004

Система построена из независимых частей. Доверенный узел содержит несколько экземпляров квантовой аппаратуры, серверы управления квантовыми ключами, сервер управления ключами. При этом в доверенный узел включается также пользовательское приложение, для которого вырабатываются секретные ключи.

Далее проводится анализ каждого из объектов доверенного узла и его функции.

По опыту проекта европейской сети SECOQC базовым элементом сети КРК является квантовая аппаратура. Причем сопряженные пары комплектов квантовой аппаратуры, связанные как квантовым каналом, так и классическим аутентифицированным каналом, являются самодостаточным элементом. Выработка квантовых ключей происходит полностью независимо от остальных процессов в сети КРК.

Как указано в разделе 1.1, квантовая аппаратура генерирует не ключ, а случайную последовательность нефиксированной длины. Для формирования квантовых ключей из совокупности случайных последовательностей применяются сервера управления квантовыми ключами (KML). На каждый блок квантовой аппаратуры в каждом УКС приходится по одному серверу управления квантовыми ключами. Эта часть УКС формирует квантовые ключи из последовательностей,

получаемых от квантовой аппаратуры, в том числе присваивая идентификаторы квантовых ключей и иную метаинформацию. Сервер управления квантовыми ключами содержит хранилище квантовых ключей, в которое помещаются сформированные квантовые ключи со всей необходимой метаинформацией. При этом идентичность квантовых ключей, вырабатываемых в двух соседних узлах, основывается только на доверии к протоколу КРК, теоретически гарантирующему идентичность вырабатываемых последовательностей.

Для передачи общих секретов в СЗИ-потребители, закрепленные за УКС, не соединенными напрямую квантовым каналом, применяется сервер управления ключами (KMS). Данный элемент УКС в ранних документах ETSI описан поверхностно, без указания способа распределения общего секрета между несоседними узлами. По опыту проекта SECOQC можно предположить, что используется подход, описанный ранее (см. рис. 3), заключающийся в передаче квантового ключа с некоторого сегмента сети на целевые УКС. В качестве защиты передачи квантового ключа используется кодирование одноразовым блокнотом. Как показано на рисунке 5, каналы связи для формирования общего секрета отделены от классического канала аппаратуры КРК. Вопрос обеспечения целостности при передаче квантового ключа не рассматривается.

Сеть КРК допускает подключение множества СЗИ к одному узлу. При этом впервые вводится требование на размещение СЗИ и прочих элементов УКС в одной контролируемой зоне.

Таким образом, первый вариант сети КРК по версии ETSI представляет собой четырехуровневую структуру. Причем два уровня сети оперируют квантовыми ключами, третий уровень предназначен для передачи квантовых ключей, сгенерированных на одном сегменте сети КРК, на другие сегменты сети КРК. Четвертый уровень сети – уровень пользовательских приложений. Второй уровень сети довольно многочисленный по числу элементов, каждый из которых выполняет только небольшую долю функций, реализованных на УКС, и может быть оптимизирован. Третий уровень, наоборот, является самым высоконагруженным элементом УКС. Включение четвертого уровня в состав УКС

выглядит не совсем корректным решением. Без потребителя ключей сеть КРК и ее УКС могут функционировать. Пользовательские устройства необходимы именно как внешние по отношению к сети КРК устройства.

В настоящее время стандарт ETSI GS QKD 004 V1.1.1 [83] пересматривается и готовится новая версия.

Позже был выпущен стандарт ETSI GS QKD 014 V1.1.1 [84], в котором были внесены существенные изменения в описании структуры сети КРК. Схематичное изображение сети КРК представлено на рисунке 6.

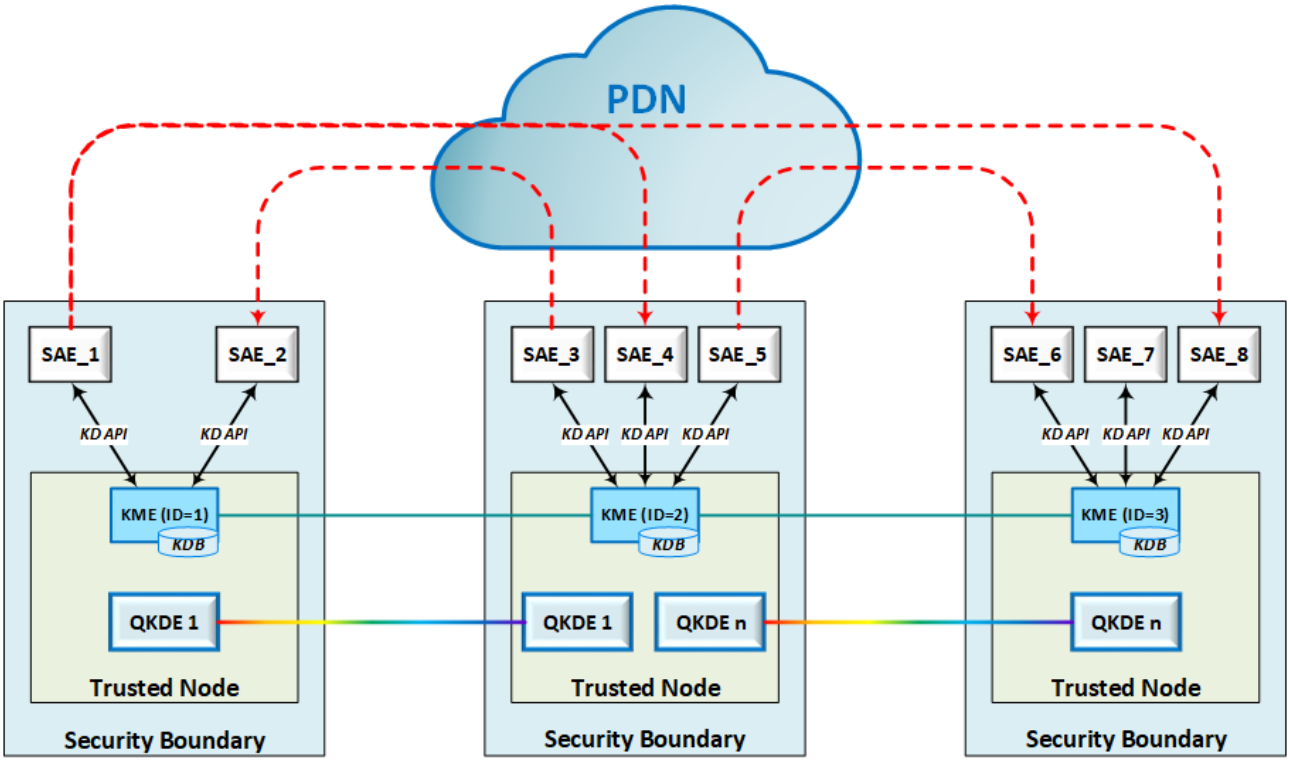


Рисунок 6 – Структура сети КРК согласно ETSI GS QKD 014

В сценарии работы сети КРК участвуют:

– Аппаратура КРК – QKDE.

– Сущность управления ключами – KME.

– Клиенты сети- SAE.

Как видно из рисунка 6, произошло существенное упрощение структуры сети путем объединения сервера управления квантовыми ключами и сервера управления ключами в единый объект. При этом СЗИ вынесены за пределы УКС,

но в то же время должны располагаться в пределах контролируемой зоны для обеспечения безопасности передачи секретных ключей в СЗИ.

Доверенным узлом называется узел, содержащий в себе и устройство управления ключами KME, и клиент сети SAE. При этом интерфейс взаимодействия описывается из следующих предположений.

1) Узел работает и управляется безопасно.
2) KME и SAE находятся в пределах границ одного узла.
3) Интерфейс взаимодействия не выходит за границы контролируемой зоны доверенного узла.
4) KME безопасен.
5) SAE безопасен.
6) KME должен иметь уникальный идентификатор в пределах сети КРК.
7) SAE должен иметь уникальный идентификатор в пределах сети КРК.

Таким образом, первоначальная структура сети содержала четыре уровня, разделяя управление квантовыми ключами и формирование общих секретов согласно запросам пользовательских приложений. При этом пользовательские приложения включались в состав доверенных узлов сети, что не совсем корректно. В следующей версии структуры сети этот недостаток был исправлен, пользовательские приложения были вынесены за границы сети, т.е. они пользуются сетью КРК как сервисом получения общих секретов. В то же время упрощение структуры узла путем объединения блоков по управлению квантовыми ключами и взаимодействию с пользовательскими приложениями усложняет узел сети, так как почти все функции узла концентрируются в единственном блоке, который ранее и так был самым нагруженным в УКС.

В обеих версиях сети КРК не рассматриваются способы распределения общего секрета для пользовательских приложений, вопросы защиты каналов взаимодействия узлов и управление узлами сети. Для второй версии сети КРК добавлены абстрактные требования по безопасности узлов сети, не способствующие упрощению построения сети ККР в целом и доверенных узлов в частности.

1.2.2 Анализ структуры сети КРК по версии ITU-T

Вслед за ETSI в ITU-T с 2018 года инициированы работы по созданию рекомендаций в области КРК, в первую очередь сконцентрированные на архитектуре сетей КРК. С 2019 года ведутся активные работы по созданию рекомендаций в части управления квантовыми ключами в сетях КРК, включая следующие вопросы.

– Хранение сгенерированных в сети КРК ключей.

– Распределение ключей между узлами в сети КРК.

– Передача ключей от аппаратуры КРК потребителям.

В настоящее время выпущен документ [85], содержащий краткое описание основных положений, содержащихся в разработанных рекомендациях, а также ряд документов, конкретизирующий частные аспекты, такие как управление ключами в сети КРК, а именно процессы распределения общих секретов через УКС, функциональные требования к сетям КРК и их элементам и др. Причем вопросы обеспечения безопасности взаимодействия УКС зачастую вынесены за рамки документов. На рисунке 7 представлена общая структура сети КРК, предлагаемая в рекомендациях ITU-T.

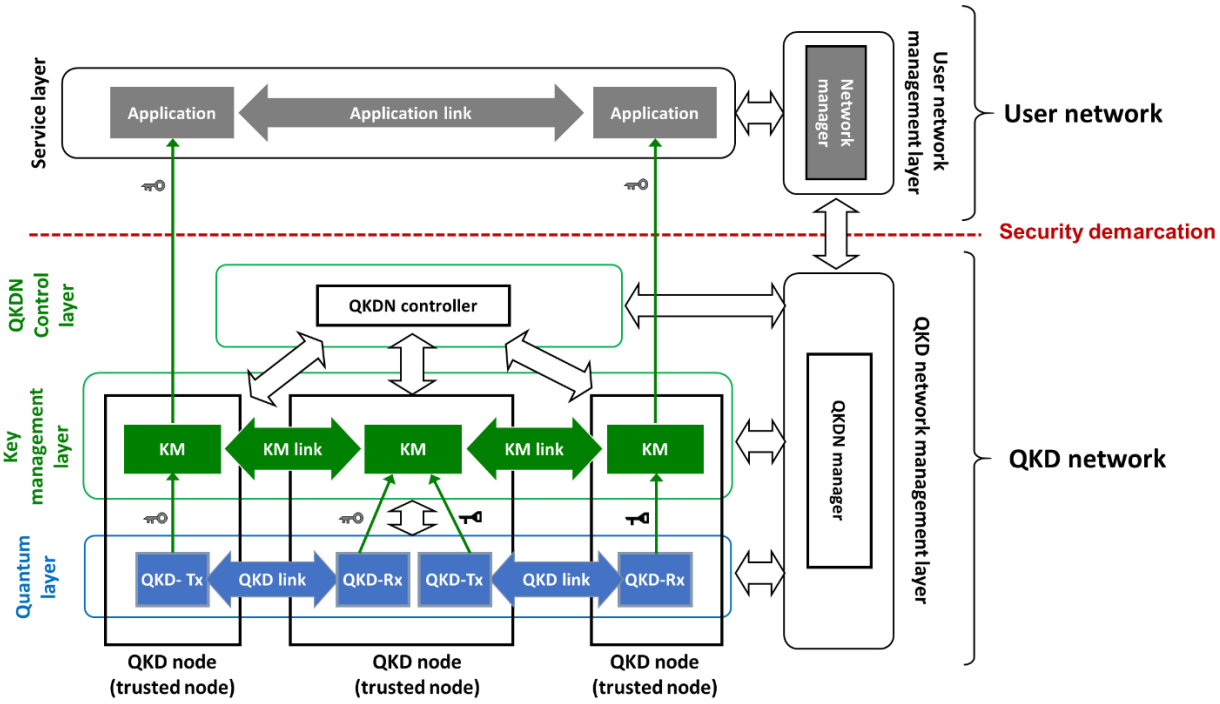


Рисунок 7 – Общая структура сети КРК ITU-T

Из рисунка 7 видно, что узлы сети КРК (доверенные узлы) состоят из двух логических уровней.

– Уровень квантовых сигналов (Quantum layer) отвечает:

а) за выработку квантовых ключей по каналу квантовой связи между соседними узлами;

б) за передачу выработанного квантового ключа уровню управления ключами.

– Уровень управления ключами (Key management layer) отвечает:

а) за распределение общих секретов в сети между несоседними узлами;

б) за выдачу общих секретов потребителю.

Распределение общих секретов между несоседними узлами названо сложным процессом, включающим:

– управление размером общего секрета;
– изменение формата распределяемого секрета и метаданных (идентификатор общего секрета, дата формирования, длина и т. д.) для управления секретами;
– хранение общих секретов;
– получение характеристик квантового канала (QBER, скорость генерации квантовых ключей, статус квантового канала связи (ККС) и др.);
– безопасную (т.е. стойкую в теоретико-информационном смысле) передачу общих секретов между узлами на уровне управления ключами;
– синхронизацию полученных общих секретов на узлах;
– формирование ключевого контейнера и выдачу общих секретов потребителю.

Существенное изменение относительно предыдущих предложений структуры сети КРК в описании архитектуры ITU-T заключается в выделении специализированного уровня управления сетью КРК (QKD network management layer), реализуемое центром управления сетью, и уровня контроля за сетью КРК (QKD control layer). Централизованное управлению сетью КРК использовано для решения проблемы расчета пути передачи квантового ключа при распределении общего секрета для двух УКС.

Работы авторов стандартов ITU-T, касающиеся управления сетями КРК через концепцию SDN сетей [86], позволяют предположить, что выделение уровня управления, связанного со всеми прочими уровнями сети КРК, сделано для дальнейшего упрощения интеграции сетей КРК в существующие сети связи общего пользования с единым управлением, т.е. объединения классических и квантовых SDN сетей. В качестве данных, передаваемых на уровне данных SDN сети, предполагаются однофотонные импульсы в квантовом канале вместе со служебным трафиком протокола КРК, а также ключевая информация при формировании общего секрета. Обратим внимание, что внешние СЗИ объединены в свою сеть, у которой тоже выделена централизованная сущность, отвечающая за управление сетью СЗИ.

Заметим, что существующие документы, описывающие структуру и сценарии работы сетей КРК, не разделяют квантовые ключи, сгенерированные непосредственно аппаратурой КРК, и общие секреты, передаваемые в СЗИ, подключенные к сети. Это не совсем корректный подход, так как квантовые ключи возможны только между УКС, соединенными напрямую квантовым каналом. Частично такой подход обоснован основным предлагаемым способом распределения общего секрета для пары СЗИ, заключающемся в передаче квантового ключа некоторого сегмента сети до целевых УКС.

Архитектура сети, предлагаемая ITU-T, рассматривает вопросы, ранее не освещенные в открытых научных публикациях. Предложены решения для синхронизации общих секретов на несоседних УКС, а также набор метаданных, которыми необходимо сопровождать квантовые ключи.

Далее приводятся существенные особенности функционирования сети КРК, описанные в документе [85].

Квантовая аппаратура вырабатывает ключи нефиксированной длины. Выработанная квантовая гамма передается на уровень управления ключами, где из переданной гаммы формируются квантовые ключи заданной, единой для всей сети КРК длины. К сформированным квантовым ключам добавляются метаданные, позволяющие контролировать жизненный цикл ключей в сети, включая время

создания ключа, длину, идентификаторы узлов, на которых сгенерирован ключ, время перемещения ключей между сущностями (от квантовой аппаратуры на уровень управления ключами, между устройствами управления ключами и т.д.).

Контроль за состоянием квантовой аппаратуры, в том числе за событиями в квантовом канале и величиной ошибки QBER, производится в едином центре управления (относящемся к уровню управления сетью КРК). Сбор данных для контроля производится уровнем управления ключами с последующей передачей в центр управления. Отметим, что предлагаемый в документах ITU-T подход требует передачи данных, позволяющих нарушителю оценить эффективность своих воздействий на сеть КРК, между узлами сети. Требуется подробный анализ такого трафика для определения необходимых мер защиты, т.е. достаточно ли обеспечивать только целостность данных или необходимо обеспечение и конфиденциальности.

Перенос функций контроля за состоянием квантовой аппаратуры с самой аппаратуры в удаленный центр управления с одной стороны позволяет оптимизировать процессы формирования квантовых ключей, так как параметры выработки квантовых ключей прямо или косвенно (в зависимости от способа формирования и передачи квантового ключа) влияют на его выработку. С другой стороны, анализ состояния квантовой аппаратуры на предмет наличия тех или иных атак нарушителя в удаленном центре увеличивает время реакции всей системы на действия нарушителя, что может негативно сказываться на стойкости системы в целом.

Единый центр контроля обладает функцией контроля жизненного цикла ключей, генерируемых в сети КРК. Для этого в центр контроля передаются метаданные, прикрепляемые к ключам при передаче из квантовой аппаратуры, в случае любого изменения этих метаданных.

Процесс распределения общих секретов для произвольной пары УКС согласно [85] заключается в следующем.

– Сервис управления сетью СЗИ формирует перечень пар СЗИ, для которых необходимы общие секреты от сети КРК. Этот перечень передается в центр

управления сетью КРК. Причем в документах ITU-T эти общие секреты именуются квантовыми ключами наравне с истинно квантовыми ключами, формируемыми на одном сегменте сети КРК.

– Центр управления сетью КРК определяет цепочки УКС, по которым можно передать квантовые ключи на УКС, сопряженные с парами СЗИ для которых сеть СЗИ запросила ключи.

  На определение цепочек УКС влияет количество готовых квантовых ключей на сегментах сети, скорость выработки новых квантовых ключей (по результатам анализа состояния квантовой аппаратуры), а также топология сети в целом.

– Набор определенных цепочек передается в контроллер сети КРК, который формирует инструкции для каждого УКС, включающие маршрут передачи ключей и указание, какие именно ключи использовать для передачи, а какие для обеспечения конфиденциальности передачи.

Вводятся три вида маршрутизации, определяющие пути передачи квантовых ключей на целевые УКС.

1) Ручная маршрутизация подразумевает статично заданные цепочки для пар УКС, к которым осуществляется подключение СЗИ.

   Данный способ целесообразно применять только к небольшим сетям КРК или к сетям с небольшим числом ветвлений, где такие цепочки легко рассчитываются и не имеют альтернативных вариантов.

2) Маршрутизация по фиксированной скорости. Данный вид маршрутизации, согласно описанию [85], нацелен на оптимальную загрузку сети исходя из производительности квантовой аппаратуры. Центр управления сетью анализирует текущую скорость работы каждой пары квантовой аппаратуры, а также определяет целевые пары УКС, на которые необходимо доставить ключи для передачи в СЗИ. Цепочки узлов подбираются так, чтобы скорость формирования квантовых ключей по всем цепочкам в совокупности оказалась минимальна. Затем

рассчитанные цепочки передаются в контроллер сети, где формируются конкретные инструкции для УКС.

3) Адаптивная маршрутизация. Данный вид маршрутизации описан как дополнительный к предыдущим. Каждый УКС запоминает рассчитанные маршруты. При получении сетью КРК запроса общего секрета, повторяющего один из ранее полученных, маршрут не пересчитывается, а УКС выдается команда повторить формирование общего секрета на основе ранее полученных инструкций. Этот вид маршрутизации может быть целесообразен при стабильной работе сети КРК и регулярных запросах ключей от постоянных пар СЗИ.

Ни один из предложенных способов маршрутизации не учитывает стойкость применяемых методов защиты при передаче ключевой информации по цепочкам УКС и, соответственно, итоговую стойкость распределенного общего секрета.

Особенности распределения общего секрета проиллюстрированы на рисунке 8, показывающем процедуру передачи квантовых ключей между УКС (key relay).

Как указано выше, общим секретом для пары СЗИ назначается квантовый ключ КМ1А, хранящийся на одном из двух целевых УКС, к которым подключены СЗИ, полученный с того экземпляра квантовой аппаратуры, который входит в рассчитанный маршрут между этими целевыми УКС.

На другой целевой УКС доставляется тот же квантовый ключ, но полученный с экземпляра квантовой аппаратуры, подключенной к второму УКС в маршруте. На рисунке обозначен КМ3В на УКС 2 (QKD node 2). Данный ключ передается закодированным одноразовым шифроблокнотом по цепочке УКС в маршруте до целевого УКС.

Стоит заметить, что при использовании одноразового шифроблокнота расходуется больше квантовых ключей, чем передается, так как помимо ключа передаются прикрепленные к нему метаданные.

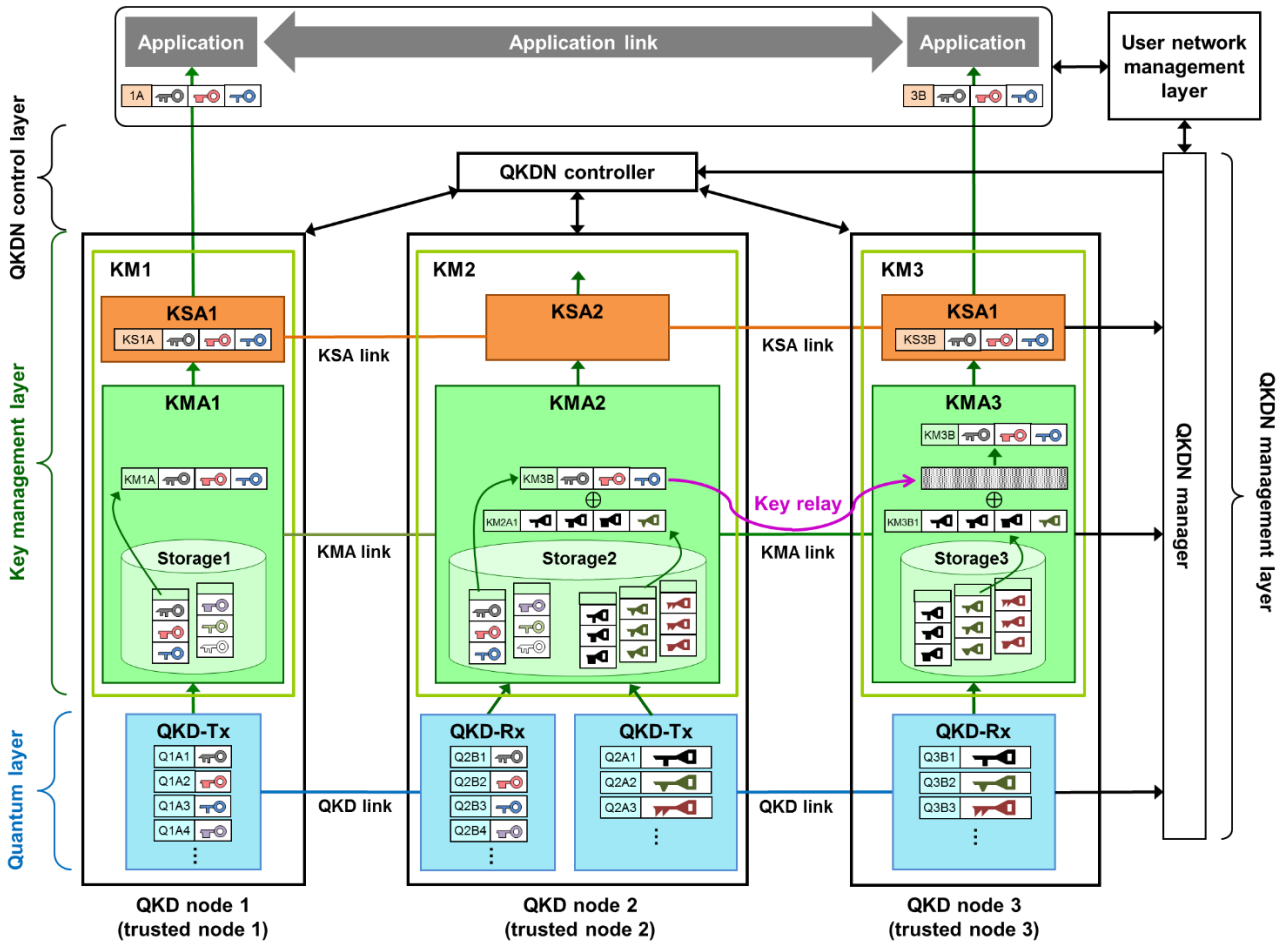


Рисунок 8 – Сценарий передачи ключей в сети КРК по версии ITU-T

При этом вопрос контроля целостности при передаче ключевой информации не рассматривается. Поэтому стоит учитывать, что потребуется еще дополнительный ключ для обеспечения целостности передаваемых данных.

Для мониторинга работы сети КРК в целом помимо обозначенных выше функций центр управления дополнительно оснащается следующим функционалом.

– Модуль управления, отвечающий, помимо расчетов маршрутов передачи квантовых ключей, за обеспечение качества предоставляемых сетью услуг (Quality of Service).
– Модуль аутентификации, отвечающий за аутентификацию и идентификацию узлов сети.
– Модуль политик, отвечающий за управление политиками безопасности сети КРК. Отмечается, что в этот модуль может подключаться оператор для мониторинга работы сети.

Для построения сети КРК необходимо выработать решение сопутствующих задач, касающихся взаимной идентификации устройств, составляющих сеть КРК; единой настройки и мониторинга параметров сети КРК, отвечающих за безопасное функционирование, а также за обеспечение требуемых эксплуатационных свойств.

В рассмотренных источниках встречается разное деление УКС. Документы ITU-T вводят следующую классификацию:

1) Пользовательские УКС. Эти УКС должны иметь возможность подключения СЗИ. Обычно пользовательские УКС содержат один экземпляр квантовой аппаратуры. Исходя из экономической целесообразности обычно это Клиент КРК.
2) Промежуточные УКС. Данные УКС, по мнению авторов документа, должны составлять основу сети КРК, решая основной вопрос: увеличение дальности распределения общего секрета для СЗИ. Промежуточные УКС содержат как минимум пару экземпляров квантовой аппаратуры, Сервер КРК и Клиент КРК, каждый из которых соединен с квантовой аппаратурой других УКС, промежуточных или доступа. Фактически промежуточные УКС составляют основные магистральные ветви сети КРК.
3) УКС доступа. Такие УКС необходимы для соединения промежуточных УКС с оконечными, т.е. пользовательскими УКС. Содержит Сервер КРК для связи с пользовательским УКС и один или более соответствующих экземпляров квантовой аппаратуры для связи с промежуточными УКС.

Отдельно отмечается, что потребителем общих секретов (имеются в виду распределяемые по сети общие секреты) могут выступать как независимые внешние устройства, так и встроенные непосредственно в УКС.

Таким образом, сети КРК, описываемые в европейских рекомендациях, имеют многоуровневую структуру с централизованным управлением. При этом взаимодействие с СЗИ, внешними по отношению к сети КРК, и распределение общего секрета для пары УКС относятся к одному уровню сети КРК. Все ключи, появляющиеся в сети КРК именуются квантовыми ключами, что вводит дополнительную путаницу и неотличимость квантовых ключей, создаваемых в

результате протокола КРК, от общих секретов, полученных в результате дальнейшего функционирования сети КРК. Централизованное управление сетью КРК ведет к возникновению точки отказа из-за повышения нагрузки на единый центр управления.

Таким образом, имеется научная проблема исследования возможности построения децентрализованной сети КРК, а также необходимость решения проблемы распределения общего секрета на произвольные пары узлов сети с обеспечением не только конфиденциальности, но и целостности передаваемой ключевой информации, а также уточнения понятия доверия к промежуточным узлам.

1.3 Формулирование целей и задач исследования

В результате проведенного в п. 1.1. и п. 1.2 анализа выявлены следующие научные проблемы, связанные с недостатками технологии КРК.

1) Системы КРК имеют предельную допустимую длину квантового канала, определяемую используемым протоколом КРК. Пользовательские устройства, для которых необходимо вырабатывать общие секреты, могут располагаться произвольно, в том числе на расстояниях, превышающих предельно допустимую длину квантового канала. Необходимо рассмотреть проблему распределения общего секрета для произвольных пар устройств, расположенных дальше предельной длины квантового канала.
2) Системы КРК должны иметь классический аутентифицированный канал, при этом способ обеспечения целостности данных в таком канале в опубликованных ранее работах упоминается поверхностно.
3) Не решены вопросы синхронизации квантовых ключей, передаваемых в пользовательские устройства. Известные методы, применяемые в классических системах, не учитывают квантовой специфики аппаратуры.

4) В качестве метода увеличения предельного расстояния распределения общих секретов рассматривается построение сетей КРК с доверенными промежуточными узлами. При этом способ распределения общего секрета исследован поверхностно, с указанием только рекомендуемого способа обеспечения конфиденциальности при передаче ключевой информации по каналам связи. Следовательно, необходимо рассмотреть проблему обеспечения целостности ключевой информации, а также обеспечения конфиденциальности ключевой информации на доверенных промежуточных узлах.
5) Все ключи, которыми оперирует сеть КРК, именуются квантовыми ключами, независимо от того, были они получены в результате протокола КРК или иных процессов в сети КРК, что создает дополнительную путаницу при описании и исследовании систем КРК.
6) Структура сети КРК и способ ее функционирования содержат не решенные вопросы, препятствующие эффективному создания и распространению ключей на произвольные пары УКС.

С учетом обозначенных проблем в рамках настоящего исследования в целях развитие методического обеспечения квантовых коммуникаций для повышения защищенности сетей квантового распределения ключей смешанной топологии. необходимо решить следующие **задачи**.

1) Разработать способ построения классического аутентифицированного канала квантовой аппаратуры.
2) Создать способ взаимодействия квантовой аппаратуры с пользовательскими СЗИ, уточняющий процессы синхронизации и обеспечения целостности общих секретов при их передаче в СЗИ.
3) Разработать методику распределения общего секрета для пары узлов сети КРК магистральной топологии.
4) Выработать методику построения сетей КРК смешанной топологии, в том числе требований к структуре сети КРК смешанной топологии и способу функционирования такой сети.

2 ОСОБЕННОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ДЛЯ СЕГМЕНТА СЕТИ В ТОПОЛОГИИ ТОЧКА-ТОЧКА

2.1 Способ построения классического аутентифицированного канала квантовой аппаратуры

Можно выделить два основных подхода к обеспечению аутентификации данных в классическом канале. Квантовые ключи, вырабатываемые в результате протокола КРК, обладают стойкостью в теоретико-информационном смысле [87]. Первым подходом является использование аутентификации того же класса стойкости, так как стойкость всей системы будет определяться по стойкости ее наименее защищенного элемента [4]. Альтернативным подходом является использование аутентификации, стойкой в вычислительном смысле (например, с применением функции хэширования ГОСТ 34.11-2018 [65], на которую не существует эффективных реализуемых атак на сегодняшний день [88]). В этом случае достигается вычислительная стойкость аутентификации классического канала, при этом возможна экономия ключа аутентификации с сохранением вычислительной стойкости используемого протокола, но происходит понижение класса стойкости квантовых ключей до вычислительно стойких.

2.1.1 Универсальное хэширование как способ вычисления имитовставки

В качестве аутентификации, стойкой в теоретико-информационном смысле, для систем КРК рассматриваются функции универсального хэширования [66], [89], [90]. Класс функций универсального хэширования H определяется следующими требованиями [91].

1) Число хэш-функций из H, таких что произвольное сообщение $m_1 \in M$ переводится в произвольную метку $t_1 \in T$, в точности равно $\frac{|H|}{|T|}$.

2) Число функций из H, которые переводят произвольное сообщение $m_1 \in M$ в произвольную метку $t_1 \in T$, при этом переводят произвольное сообщение

$m_2 \neq m_1 \in M$ в некоторую метку $t_2 \in T$ (возможно равную t_1), не превышает $\varepsilon \frac{|H|}{|T|}, \varepsilon > \frac{1}{|T|}$.

Такой класс хэш-функций называется классом $\varepsilon - ASU_2$-функций (Almost Strong Universal Hashing). Параметр ε является параметром стойкости класса хэш-функций.

Варианты использования хэш-функций для аутентификации.

Для построения аутентифицированного канала в целях обеспечения целостности передаваемых данных необходимо вырабатывать метку аутентификации (имитовставку) с использованием универсальных хэш-функций. Метка аутентификации сообщения *t* может быть получена несколькими способами [66], [89], [92].

1) $t = h_{k^j}(m^j)$, где m^j – j-ое аутентифицируемое сообщение, h_{k^j} – функция хэширования, соответствующая ключу аутентификации k^j. Каждый ключ k^j используется для аутентификации только одного сообщения.

2) $t = \begin{cases} h_{k^j}(m_0^j), \ j = 0, 1, 2, \dots \\ h_{k^j}(m_i^j) + k_{otp_i}^j, \ j = 0, 1, 2, \dots; i = 1, 2, 3, \dots \end{cases}$

В данном случае каждая функция хэширования используется более одного раза, при этом после первого применения функции хэширования h_{k^j} последующие метки аутентификации от последующих сообщений m_i кодируются одноразовым шифроблокнотом на ключах $k_{otp_i}^j$. j – порядковый номер используемой функции хэширования, соответствующей ключу k^j. $\{m_i^j\}, i = 0, 1, 2, \dots$ – набор сообщений, для аутентификации которых используется одна функция хэширования.

3) $t = h_{k^j}(m_i^j) + k_{otp_i}^j, \ j = 0, 1, 2, \dots; i = 0, 1, 2, \dots$

В данном варианте все результаты применения функции хэширования h_{k^j} к аутентифицируемому сообщению m_i^j кодируются одноразовым

шифроблокнотом на ключе $k_{otp_i}^{j}$. $j-$ порядковый номер используемой функции хэширования, соответствующей ключу k^j.

Варианты аутентификации 2 и 3 позволяют экономить ключ аутентификации, как показано в работах [90], [91], [93], так как длина кодируемой метки аутентификации, а следовательно, и ключа одноразового шифроблокнота, меньше, чем длина ключа функции универсального хэширования. Однако в работе [93] показана эффективная атака на вариант аутентификации 1 и 2, а также необходимость кодировать одноразовым шифроблокнотом все метки аутентификации, включая первую.

Таким образом, наиболее предпочтительным вариантом вычисления метки аутентификации с использованием универсальных хэш-функций является вариант 3.

Далее приводится способ построение некоторых функций универсального хэширования и сравнение их характеристик.

Используемые обозначения, общие для всех функций:

M – пространство сообщений,

$l_m = \log_2|M|$ – длина сообщения,

$m \in M$ – сообщение,

T – пространство меток аутентификации,

$l_t = \log_2|T|$ – длина метки аутентификации,

$t \in T$ – метка аутентификации.

Функции универсального хэширования для формирования меток аутентификации

1) Семейство функций Wegman-Carter [89]

Параметры хэш-функции представлены в формуле (1):

$$|M| = 2^i, |T| = 2^j, j < i, p - \text{наименьшее простое}, p > 2^i. \quad (1)$$

Хэш-функция вычисляется согласно формуле (2):

$$\mathrm{f}_{(q,r)}(m) = \big((mq + r) \bmod p\big) \bmod |T|, \quad (2)$$

где q, r – секретные параметры (ключ хэш-функции), однозначно определяющие хэш-функцию из семейства хэш-функций. $H_1 = \{f_{(q,r)}: q \in Z_p \backslash \{0\}, r \in Z_p\}$ – семейство SU_2 хэш-функций. Согласно [89] для данного семейства хэш-функций оптимальными с точки зрения расхода ключа являются длина сообщений $2L$ и длина выхода хэш-функции L определяемые по формуле (3):

$$L = l_t + \log_2 \log_2 l_m \qquad (3)$$

Вычисление меток аутентификации от произвольных сообщений с помощью семейства функций Wegman-Carter производится следующим образом.

Формируется H_1 – семейство хэш-функций, с максимальной длиной обрабатываемых сообщений $l_m{}' = 2L$ и длиной выхода хэш-функций L. Параметр L определяется по формуле (3).

Аутентифицируемое сообщение m делится на блоки длины $2L$, которые хэшируются в блоки длины L с применением $f_{(q_1,r_1)}$. Имеем $\left\lceil \frac{\log_2 |M|}{2L} \right\rceil$ блоков. Блоки, полученные в результате применения хэш-функции, конкатенируются в промежуточную строку m_1.

Промежуточная строка m_1 делится на блоки длины $2L$, которые хэшируются в блоки длины L с применением $f_{(q_2,r_2)}$.

Процесс повторяется на различных хэш-функциях из H (т.е. с использованием разных ключей для каждого раунда хэширования) до тех пор, пока не останется последний блок длины L. Ключом для выбора хэш-функции является пара (q_i, r_i).

Младшие $\boldsymbol{t}$ бит этого последнего блока – искомая метка аутентификации t.

Совокупная длина ключей, необходимых для идентификации всех используемых хэш-функций составляет $4L \log_2 l_m$. Под ключом понимается конкатенация ключей для всех использованных хэш-функций

Стойкость хэш-функции $\frac{2}{T} - ASU_2$.

2) Семейство функций Stinson [94]

Параметры функции хэширования представлены в формуле (4):

$$q = 2, s = l_t + \lceil \log_2 \log_2 l_m \rceil, i = \left\lceil \log \frac{l_m}{s} \right\rceil, p = q^s,$$
$$M = M_1^{2i}, T = T_2, |M| = 2^{l_m}, |T| = 2^{l_t}. \quad (4)$$

Семейство функций хэширования строится на основе двух вспомогательных функций.

Первая вспомогательная функция хэширования описывается формулой (5):

$$\mathrm{g}_x : M_1 \to T_1,$$
$$\mathrm{g}_x(y, z) = xy + z, \quad (5)$$

где $M_1 = F_p \times F_p$ – пространство хэшируемых сообщений,

$T_1 = F_p$ – пространство выходов хэш-функции,

$x, y, z \in F_p$.

Семейство универсальных хэш-функций G_1, построенное на вспомогательной хэш-функции (5) имеет вид:

$$G_1 = \{\mathrm{g}_x : x \in F_p\}. \quad (6)$$

Данное семейство может быть расширено до семейства $M_1^{2^j}$ для всех $j = 1, \dots, i$. В этом случае имеем хэш-функцию, представленную в формуле (7):

$$\mathrm{h}^{2j} : M^{2j} \to T^{2j}$$
$$\mathrm{h}^{2j}(m_1, \dots m_{2j}) = \left(\mathrm{h}(m_1), \dots, \mathrm{h}(m_{2j})\right), \mathrm{h} \in G_1. \quad (7)$$

И соответственно семейство хэш-функций, представленное в формуле (8):

$$G_1^{2^j} = \{\mathrm{h}^{2j} : \mathrm{h} \in G_1\}. \quad (8)$$

Последовательно применяя функции из семейств $G_1^{2^j}$ для всех $j = i, \dots, 1$ получаем метку аутентификации длины p из сообщения длиной p^{2i}. Таким образом, получаем класс функций $G_1^{2^i}$, состоящий из p^i хэш-функций, хэширующих сообщения из $M_1^{2^i}$ в метки аутентификации из T_1.

Вторая вспомогательная функция хэширования представлена в формуле (9):

$$\mathrm{g}_{xy} : M_2 \to T_2 \quad (9)$$

$$z \to \varphi(xz) + y,$$

где $M_2 = F_{q^s}, T_2 = F_{q^t}$ параметры функции хэширования,

$\varphi(x) = \varphi\big((x_1, \dots, x_s)\big) = \left(x_{i_1}, \dots, x_{i_{l_t}}\right)$ – некоторое отображение наборов длины s в наборы длины l_t.

Класс SU хэш-функций имеет вид, представленный в формуле (10):

$$G_2 = \left\{\mathrm{g}_{xy} : (x, y) \in F_{q^s} \times F_{q^t}\right\}. \quad (10)$$

Итоговое семейство хэш-функция получается путем комбинирования семейств $G_1^{2^i}$ и G_2

Вычисление меток аутентификации от произвольных сообщений с помощью семейства функций Stinson производится следующим образом.

Метка аутентификации получается за $i + 1$ раундов.

На первых i раундах хэшируемое значение дополняется нулями до длины, кратной $2s$. Значение сообщения хэшируется функцией из $G_1^{2^j}$, где j – номер раунда, применяется функция g_{k_j}, где k_j – ключ для j раунда.

На последнем раунде применяется функция g_{k_a,k_b} из G_2, где k_a, k_b – ключи для хэш-функции.

Длина ключа для идентификации всех необходимых хэш-функций равна $(\log_2 l_m - \log_2 l_t + 2)l_t$.

Стойкость хэш-функции $\frac{2}{|T|} - ASU_2$.

3) Семейство функций den Boer [95]

Полагаем $|M| = n \cdot l_m$, т.е. сообщение $m \in M$ разбивается на n сообщений m_i из $GF(2^t)$.

Хэш-функция имеет вид (11):

$$\mathrm{h}_{k_1,k_2}(m) = k_1 + \sum_{i=1}^{n} m_i k_2^i. \quad (11)$$

Тогда семейство хэш-функций представляется в виде (12):

$$H = \{\mathrm{h}_{k_1,k_2} : k_1, k_2 \in GF(2^{l_t})\}. \quad (12)$$

Длина ключа для идентификации всех необходимых хэш-функций $2l_t$.

Стойкость хэш-функции $\frac{|M|}{|T|\log_2|T|} - ASU_2$.

Примечание – Стойкость функции хэширования существенно зависит от выбора максимальной длины обрабатываемых сообщений.

4) Семейство функций Bierbrauer (на базе кодов Рида-Соломона) [96]

Для формирования функции аутентификации строится $[n, k, d]_q$ код.

Параметры кода $[n, k, d]_q$ удовлетворяют соотношению (13):

$$n = 2^{l_t+s}, k = 1 + 2^s, d = n - k + 1 = 2^{l_t+s} - 2^s, q = 2^{l_t+s}, \quad (13)$$

Где s – минимальное целое, такое что $l_m < (l_t + s)(1 + 2^s)$, тогда $s \approx \lceil \log_2 l_m - \log_2 l_t \rceil$.

Мощность пространства обрабатываемых сообщений для хэш-функции, построенной на таком коде составит $|M| = 2^{(l_t+s)(1+2^s)}$.

Аутентификация с помощью семейства функции Bierbrauer производится следующим образом**.**

Выбирается $k_1 \in \{0,1\}^{n+s}$ – ключ универсальной хэш-функции.

Выбираются $k_a \in \{0,1\}^{n+s}, k_b \in \{0,1\}^n$ – ключи для хэш-функции из G_2 (см. формулу (10)).

Сообщение дополняется нулями до длины кратной $l_t + s$ и разбивается на блоки длины $l_t + s$. Каждый j-ый блок умножается на $k_1^{(j-1)}$ для всех $j = 1, \dots, i$, после чего все результаты умножений складываются. Умножение и возведение в степень производится в поле $F_{2^{r+s}}$.

На последнем раунде применяется функция g_{k_a,k_b} из G_2.

Длина ключа для идентификации всех необходимых хэш-функций $3l_t + 2s$.

Стойкость хэш-функции $\frac{2}{|T|} - ASU_2$.

5) Матрицы Тёплица [97]

Пусть A – матрица Тёплица с a строками и b столбцами. Пусть $y \in T$.

Тогда функция хэширования сообщения m имеет вид (14):

$$\mathrm{h}_{(A,y)}: M \to T$$
$$t = \mathrm{h}_{(A,y)}(m) = Am + y. \quad (14)$$

Длина ключа для идентификации всех необходимых хэш-функций $l_m + 2l_t - 1$.

Стойкость такой хэш-функции $\frac{1}{|T|} - ASU_2$.

Заметим, что для хэширования каждого нового сообщения необходимо построение новой матрицы Тёплица. Следовательно, ключ функции хэширования может превышать длину хэшируемого сообщения, так как для построения матрицы требуется объем случайных данных, превышающий размер аутентифицируемого сообщения.

В Таблице 1 приведены ключевые параметры и особенности рассмотренных функций хэширования. Рассматриваются ключевые параметры, определяющие эксплуатационные свойства, а именно: параметр стойкости ε и общую длину ключа, необходимую для аутентификации сообщения m длины l_m.

Таблица 1 – Сравнительная таблица параметров функций хэширования

	ε	Длина ключа	Примечание
Wegman-Carter	$\frac{2}{\|T\|}$	$4(t + \log_2 \log_2 l_m) \log_2 l_m$	Фиксированное значение ε
Stinson	$(\log_2 l_m - \log_2 l_t + 1) / \|T\|$	$(\log_2 l_m - \log_2 t + 2\ )l_t$	Малый размер ключа
der Boer	$\frac{\|M\|}{\|T\| \log_2 \|T\|}$	$2l_t$	Наименьший размер ключа
Bierbrauer	$\frac{2}{\|T\|}$	$3l_t + 2(\log_2 l_m - \log_2 l_t) \approx 3l_t + 2\log_2 l_m$	Фиксированное значение ε. Малый размер ключа.
Матрицы Тёплица	$\frac{1}{\|T\|}$	$2l_t + l_m - 1$	Матрицы Тёплица не применимы при условии смены ключа для каждого аутентифицируемого сообщения.

Типичным источником ключа для функции аутентификации классического аутентифицированного канала в системах КРК для некоторого (не первого) сеанса КРК является часть квантового ключа, выработанного на предыдущем сеансе КРК. Если применять функции аутентификации с минимальной требуемой длиной ключа, то бóльшая часть квантового ключа одного сеанса КРК может быть использована для передачи абонентам.

Как видно из приведенной Таблицы 1, наименьшими размерами ключей обладают функции семейств Stinson, der Boer, Bierbrauer. Однако, использование семейства функций Bierbrauer сопряжено с построением кода Рида-Соломона большой размерности [48], а стойкость семейства функций der Boer существенно зависит от длины обрабатываемых сообщений. Наиболее целесообразным является применение функций семейства Stinson. При малом расходе ключа они обладают простотой конструкции и параметром стойкости, зависящим всего от логарифма длины обрабатываемых сообщений.

Фундаментальной проблемой теоретико-информационно стойкой аутентификации является необходимость использования новых различных независимых ключей аутентификации для каждого аутентифицируемого сообщения [37]. Напомним, что в качестве ключа для аутентификации последующей сессии выработки квантовых ключей принято использовать часть от общего квантового ключа, выработанного в результате текущего протокола КРК. Таким образом, в зависимости от объемов передаваемых данных, которые необходимо аутентифицировать на этапах протокола КРК, возможна ситуация, при которой бóльшая часть выработанного квантового ключа будет потрачена на аутентификацию канала для последующей серии.

Как показано в работе [98] нижняя оценка для длины ключа аутентификации таких функций – двоичный логарифм от длины сообщения.

Покажем необходимый объем ключа аутентификации для одного сеанса КРК. Можно выделить несколько подходов для аутентификации сообщений, появляющихся на этапе постобработки протокола КРК.

1) Метка аутентификации вычисляется от каждого сообщения при первичной передаче его в классическом аутентифицируемом канале. Данный метод наиболее затратный по необходимому размеру ключа аутентификации, так как длина ключа аутентификации пропорциональна логарифму длины аутентифицируемых сообщений. Проводить расчеты для данного метода нецелесообразно.

2) Метка аутентификации вычисляется от всех сообщений, переданных в течение одного этапа сеанса КРК в одну сторону (только в сторону Клиента КРК и только в сторону Сервера КРК раздельно) в конце каждого этапа. Т. е. необходимо выделить шесть ключей аутентификации некоторой длины.

3) Метка аутентификации вычисляется от всех сообщений в обе стороны (в сторону Клиента КРК и в сторону Сервера КРК вместе), переданных в течение одного этапа сеанса КРК.

4) Метка аутентификации вычисляется один раз от всех сообщений, переданных в течение всех трех этапов протокола КРК по окончании сеанса КРК.

Рассчитаем нижнюю оценку необходимых размеров ключей аутентификации для предложенных подходов. Расчет произведен на основе объемов данных, передаваемых в классическом аутентифицированном канале, для комплекса ViPNet Quandor в процессе выполнения работ по комплексному проекту, реализуемому по Соглашению № 03.G25.31.0254 от 27.04.2017 с Министерством образования и науки Российской Федерации. Длине квантового канала составляет 100 км и длина квантового ключа, получаемого в результате одного сеанса КРК, равна 256 бит. На этапе согласования базисов объем данных от Сервера КРК в сторону Клиента КРК и обратно составил, соответственно, $m_1 = m_2 = 1920$ бит. На этапе исправления ошибок – $m_3 = 1056000$ бит и $m_4 = 256000$ бит. На этапе усиления секретности – $m_5 = 2256000$ бит и $m_6 = 12000$ бит.

В общем случае длина необходимого ключа аутентификации вычисляется по формуле (15):

$$k_j = \sum_i \log_2 m_i, \qquad (15)$$

где i – номер аутентифицируемого сообщения;

m_i – длина аутентифицируемого сообщения;

j – номер подхода аутентификации.

Для подхода аутентификации 4 имеем:

Общий объем данных в обе стороны равен:

$$m = \sum_m m_i = 3583840 \text{ бит.}$$

Тогда длина ключа аутентификации принимает значение согласно (15):

$$k_4 = \log_2 m \approx 22 \text{ бита.}$$

Для подхода аутентификации 3 имеем:

Объемы аутентифицируемых данных соответственно:

$$m_1' = m_1 + m_2 = 3840 \text{ бит;}$$
$$m_2' = m_3 + m_4 = 1312000 \text{ бит;}$$
$$m_3' = m_5 + m_6 = 2268000 \text{ бит.}$$

Тогда длина ключа аутентификации согласно (15) равна:

$$k_3 = \log_2 m_1' + \log_2 m_2' + \log_2 m_3' \approx 55 \text{ бит.}$$

Для подхода аутентификации 2 имеем длину ключа аутентификации согласно (15):

$$k_2 = \sum_i \log_2 m_i \approx 97 \text{ бит.}$$

Уточним полученные оценки длин ключа аутентификации. Согласно приведенным в работе [98] оценкам длины ключа аутентификации наименьшей длиной обладает хэш-функция на базе кода Рида-Соломона. Для такой хэш-функции длина ключа вычисляется по формуле (16):

$$k' = 2\log_2 m + 3t, \qquad (16)$$

где t – длина метки аутентификации, m – длина аутентифицируемого сообщения. Согласно рекомендациям SECOQC длина метки аутентификации должна быть не менее 64 бит [82].

Таким образом, имеем следующие оценки длин ключа аутентификации согласно (16) соответственно:

$$k_2' = 1346 \text{ бит}, k_3' = 686 \text{ бит} ,k_4' = 236 \text{ бит}.$$

Расчеты для подхода аутентификации 1 не производились в силу того, что данный подхода еще более затратный, чем подход аутентификации 2. Согласно произведенным расчетам объемов данных и результирующей длины квантового ключа из [99] следует, что для квантового канала длиной 100 км ожидается выработка 400 бит квантового ключа в результате выполнения одного сеанса КРК. Таким образом, только подход аутентификации 4 потенциально возможен: число бит, необходимых на ключ аутентификации, меньше, чем число бит получаемого квантового ключа. Однако при таком подходе аутентификации останется всего 164 бита квантового ключа, который можно использовать для организации защищенного канала взаимодействия. Если при расчете длины ключа аутентификации принимать, что за один сеанс КРК выработается 256 бит квантового ключа, то ни один из предложенных подходов не позволит выделять часть квантового ключа в качестве ключа аутентификации, и необходимо применять альтернативный метод доставки ключей аутентификации в квантовую аппаратура для удовлетворения потребности в ключах аутентификации множества сеансов КРК.

Таким образом, при рассматриваемых скоростях выработки квантовых ключей 256 бит за сеанс КРК невозможно применение аутентификации, имеющей теоретико-информационную стойкость [45].

Недостаточный размер квантового ключа, т.е. необходимость тратить весь или бóльшую часть квантового ключа на аутентификацию следующего сеанса, обусловлен степенью сжатия очищенного ключа на этапе усиления секретности. Степень сжатия этапа усиления секретности зависит от величины ошибки в

квантовом канале и, соответственно, размера данных, передаваемых на этапе исправления ошибок и раскрывающих нарушителю информацию о вырабатываемом квантовом ключе. Для конкретной системы, использованной для расчета, возможно уменьшение фактической длины квантового канала, что приведет к уменьшению ошибки в квантовом канале и, соответственно, уменьшению степени сжатия на этапе усиления секретности.

В общем случае, для систем КРК, обладающих недостаточной скоростью генерации квантовых ключей из-за высокого уровня стойкости вырабатываемых квантовых ключей (высокой степени сжатия на этапе усиления секретности), применение теоретико-информационно стойкой аутентификации оказывается невозможным. Для таких систем необходимо применение **вычислительно** стойкой аутентификации. При этом, в отличие от первого подхода, на одном ключе аутентификации допустимо аутентифицировать несколько сообщений до исчерпания допустимой нагрузки на ключ соответствующей функции аутентификации.

В этом случае для аутентификации классического канала используется имитовставка, вычисляемая согласно ГОСТ 34.13-2018 [100]. Длина ключа аутентификации составляет 256 бит. При этом, в отличии от теоретико-информационно стойкого подхода, на одном ключе аутентификации вычисляются метки аутентификации от множества сообщений в пределах допустимой нагрузки на ключ аутентификации. В любом из этих подходов каждый вырабатываемый квантовый ключ диверсифицируется на ключ аутентификации и ключ кодирования, который будет использован для передачи внешним устройствам. В случае систем КРК функция диверсификации тривиальна и состоит в разбиении выработанного квантового ключа $КК$ на ключи для пользователей $К_{\text{Полз}}$ и ключи аутентификации $К_{\text{Аут}}$ следующего сеанса КРК соответствующего размера согласно выбранной функции аутентификации (см. рис. 9).

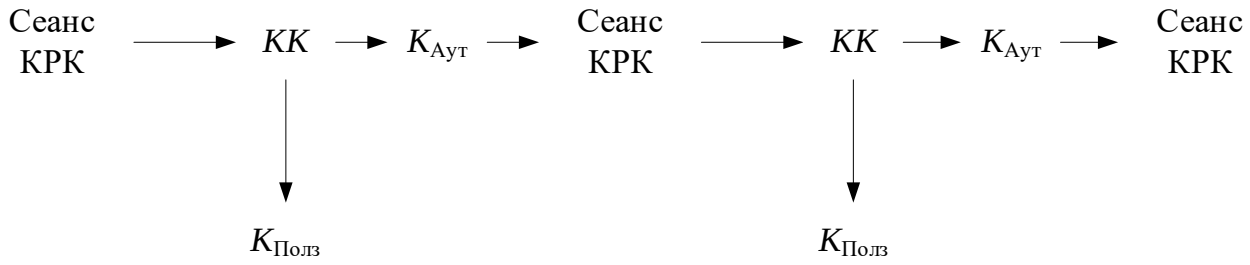


Рисунок 9 – Схема диверсификации квантовых ключей протокола КРК

Таким образом, в системах КРК с высокой степенью сжатия на этапе усиления секретности невозможно применение теоретико-информационно стойкой аутентификации с учетом требуемого объема ключей аутентификации универсальных хэш-функций. При этом сохраняется возможность применения вычислительно стойких способов аутентификации при построении классического аутентифицированного канала для таких систем из-за фиксированного размера ключа аутентификации независимо от объема аутентифицируемых данных.

В то же время, если степень сжатия на этапе усиления секретности позволяет получить необходимый объем ключа для формирования ключа аутентификации, рекомендуется применение универсальных функций хэширования для сохранения теоретико-информационной стойкости вырабатываемых квантовых ключей. Функции универсального хэширования, построенные по принципу Stinson обладают минимальным требуемым размером ключа среди функций универсального хэширования с фиксированным показателем стойкости.

2.2 Способ взаимодействия квантовой аппаратуры с пользовательскими СЗИ

Данный раздел посвящен особенностям сопряжения квантовой аппаратуры и пары пользовательских СЗИ. В частности, решается научная задача формирования общих секретов из квантовой последовательности, полученной в результате выполнения протокола КРК, последующей согласованной передачи идентичных секретов в пару СЗИ и контроля успешной передачи.

Как указано в п. 1.1, в результате выполнения протокола КРК на двух концах квантового канала получается идентичная случайная последовательность некоторой длины. Вариативность длины последовательности обусловлена неидеальностью квантового канала и этапами исправления ошибок и усиления секретности протокола КРК. Для различной длины квантового канала длина значения получаемой случайной последовательности может отличаться, так как бóльшая длина квантового канала означает бóльшие значения потерь в канале, а следовательно, и бóльшую итоговую ошибку в сформированном сыром ключе.

Для сопряжения квантовой аппаратуры и СЗИ в последние необходимо передавать общие секреты соответствующего фиксированного размера. С целью однозначной идентификации общего секрета парой СЗИ каждый секрет должен сопровождаться уникальным набором метаданных. Минимально необходимый набор метаданных – уникальный идентификатор общего секрета. Далее в данном разделе под общим секретом пары СЗИ будем понимать ключевой материал фиксированной длины, полученный путем форматирования квантового ключа, и сопоставленные ему метаданные.

Можно допустить передачу квантовой гаммы произвольного размера, кратного длине ключа кодирования в СЗИ, однако такой способ потребует двойного процесса форматирования ключевой гаммы и присвоения идентификаторов общих секретов. Первый раз в квантовой аппаратуре для синхронизации ключевой гаммы для передачи. Второй раз в СЗИ при получении ключевой гаммы каждым СЗИ независимо и дальнейшей синхронизации полученных последовательностей. Дублирование процесса форматирования и синхронизации приводит к повышенной вероятности сбоя хотя бы в одной из пар устройств.

Также существенной проблемой является контроль идентичности секретов, полученных между двумя географически разнесенными СЗИ. Принято считать, что идентичность квантовых ключей гарантируется протоколом КРК. Рассмотрим несколько последовательных успешных сеансов КРК. В результате каждого сеанса созданы квантовые ключи, то есть случайные последовательности. Длины данных

последовательностей в каждом сеансе различны (как указано в п. 1.1 из-за неидеальности квантового канала). Также часть каждой последовательности используется для защиты классического аутентифицированного канала и не может быть использована для формирования общего секрета пары СЗИ. Оставшиеся части необходимо конкатенировать в одну последовательность и разбить на блоки длины, соответствующей размеру требуемых общих секретов СЗИ. Уже на этапе данного форматирования могут возникать случайные сбои, приводящие к расхождению последовательностей, составляющих блоки. При передаче сформированных блоков в СЗИ также необходимо обеспечивать целостность передаваемой ключевой информации.

Ниже приводится анализ некоторых комплексов, состоящих из квантовой аппаратуры и пары СЗИ.

Известен способ и устройство для передачи информации с использованием технологии КРК (заявка США № 20180054304, приоритет от 19.08.2016 г. [101]), в котором коммуникационное устройство состоит из модуля загрузки, модуля контроля потока и модуля обработки, а способ предусматривает передачу и использование ключей в устройстве. Модуль загрузки предоставляет ключи, полученные с помощью технологии КРК. В случае, если при получении данных коммуникационным устройством отсутствует ключ, модуль контроля потока выполняет одно из трех действий: отбрасывает данные, сохраняет данные в буфер или добавляет к данным метку, что ключ не был предоставлен, с последующей передачей данных в модуль обработки. При получении данных от модуля контроля потока модуль обработки производит обработку (закодирование) данных с использованием ключа.

С помощью данного устройства реализуется система передачи информации, состоящая из устройств генерации, производящих ключи с помощью технологии КРК, и коммуникационных устройств, описанных выше.

Данное устройство и способ имеют следующие недостатки.

Если в течение продолжительного промежутка времени отсутствует ключ от устройства генерации, то защищенная передача данных прерывается. При этом

отбрасывание данных может быть недопустимым в силу характера передаваемых данных, а размер буфера для данных, ожидающих ключа – ограниченным, то есть выполнение первого действия модулем контроля потока может быть запрещено, а выполнение второго невозможно из-за заполненного буфера данных. Другими словами, данное устройство тесно интегрировало СЗИ в квантовую аппаратуру, причем приоритет работы отдается квантовой аппаратуре. Квантовая аппаратура ради квантовой аппаратуры не целесообразна. Применение технологии КРК должно осуществляться с целью повышения безопасности передачи полезных пользовательских данных за счет регулярной доставки и смены ключей в СЗИ. В приведенном устройстве наблюдается ориентация на создание квантовых ключей, а защита пользовательских данных выглядит побочной функцией.

Ключи, передаваемые в два коммуникационных устройства системы, в общем случае могут быть различны из-за непредвиденных ошибок. Однако проверка на идентичность загружаемых ключей не производится, как и контроль использования одного и того же ключа для зашифрования и расшифрования данных, что может привести к невозможности расшифрования в одном коммуникационном устройстве данных, зашифрованных на другом ключе в другом коммуникационном устройстве. Таким образом, становится невозможно выполнение устройством своего функционального предназначения по передаче информации за счет нарушения ее доступности.

Известен способ аутентификации и устройство для его осуществления для системы квантовой криптографии (заявка США № 20190238326, приоритет от 29.01.2018 г. [102]); способ заключается в сравнении последовательностей, переданных по квантовому каналу передачи в позициях совпадающих базисов.

Этот способ имеет следующий недостаток: аутентифицируются непосредственно устройства квантовой криптографии, но не данные, передаваемые в процессе выработки квантового ключа, а именно: служебные сообщения по согласованию базисов измерений, исправлению ошибок и сообщения этапа усиления секретности. Таким образом, не гарантируется целостность и аутентичность этих служебных данных, и нарушитель может осуществить атаку

«человек посередине», встроившись в квантовый и классический канал системы КРК ради навязывания служебного трафика.

Также известен способ и устройство для шифрования с использованием технологии КРК (заявка США № 20050063547, приоритет от 03.05.2004 г. [103]), в котором устройство состоит:

– из первого и второго получающего/передающего узла, соединенных соответственно с первым и вторым зашифровывающим/расшифровывающим процессором;
– первой и второй станции КРК, соединенных соответственно с первым и вторым зашифровывающим/расшифровывающим процессором и адаптированных для обмена квантовыми ключами и передачи их в первый и второй зашифровывающий/расшифровывающий процессоры;
– первым и вторым узлами классического распределения ключей, соединенных соответственно с первым и вторым зашифровывающим/расшифровывающим процессором и адаптированных к обмену классическими ключами и передаче классических ключей в первый и второй зашифровывающий/расшифровывающий процессор.

Зашифровывающий/расшифровывающий процессоры адаптированы для получения сигналов от одной получающей/передающей станции; зашифрования сигналов с использованием сессионного ключа, полученного в зашифровывающем/расшифровывающем процессоре путем сложения операцией XOR квантового и классического ключа; передачи зашифрованного сигнала на другую получающую/передающую станцию.

В устройстве реализуется способ передачи зашифрованных сигналов между первой и второй приемной/передающей станциями, включающий:

– передачу первого открытого сигнала с первой приемной/передающей станции на первый зашифровывающий/зашифровывающий процессор классической системы шифрования, содержащей также второй зашифровывающий/расшифровывающий процессор,

– обмен квантовыми ключами между первым и вторым узлом КРК системы КРК и предоставление квантовых ключей первому и второму зашифровывающему/расшифровывающему процессору,
– обмен классическими ключами между первой и второй классическими станциями и предоставление классических ключей первому и второму зашифровывающему/расшифровывающему процессору,
– формирование сессионного ключа путем сложения операцией XOR полученных классического и квантового ключа,
– формирование зашифрованного сигнала из первого открытого сигнала на первом зашифровывающем/расшифровывающем процессоре с использованием сессионного ключа, сформированного на первом процессоре,
– формирование расшифрованного сигнала из зашифрованного сигнала, полученного от первого зашифровывающего/расшифровывающего процессора на втором зашифровывающем/расшифровывающем процессоре с использованием сессионного ключа, сформированного на втором процессоре,
– передачу второго открытого сигнала на вторую приемную/передающую станцию.

Данное техническое решение имеет ряд недостатков.

Контроль идентичности используемых ключей (квантовых и классических) в зашифровывающем/расшифровывающем процессорах производится передачей идентификаторов ключей в открытом виде по линии связи между процессорами, что может вызвать навязывание использования различных сессионных ключей для зашифрования и расшифрования сигнала в процессоре.

Применение в изобретении внешнего источника классических ключей в целях регулярного распределения ключей требует использования технологий, основанных на ассиметричных алгоритмах, что приводит к появлению рисков компрометации распределяемых ключей в условиях нарушителя, обладающего квантовым компьютером.

Недостатком изобретения является также наличие отдельных физических каналов взаимодействия для системы КРК и системы обмена классическими ключами, что повышает затраты на создание и развертывание устройства.

В результате анализа выявленных недостатков предлагаются следующие решения для комплекса, представленного на рисунке 10.

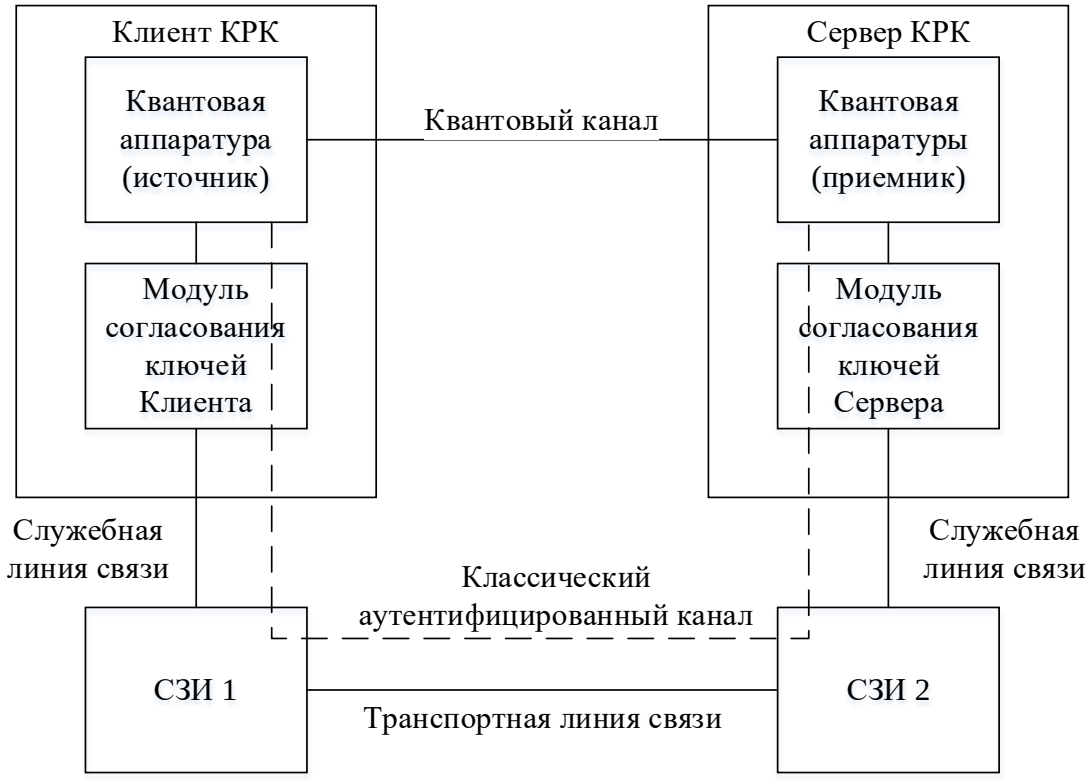


Рисунок 10 – Схема комплекса квантовой аппаратуры защиты информации

В предлагаемом комплексе используется только одна классическая линия связи (транспортная линия связи), соединяющая как два СЗИ, так и два узла системы КРК.

Логический канал передачи служебных сообщений системы КРК состоит из перечисленных ниже каналов передачи информации:

– аутентифицированный с использованием квантовых ключей канал передачи служебной информации и квантовых ключей из приемного узла системы КРК в сопряженное СЗИ и обратно,

– аутентифицированный с использованием квантовых ключей канал передачи пользовательских данных между СЗИ,

– аутентифицированный с использованием квантовых ключей канал передачи служебной информации и квантовых ключей из передающего узла системы КРК в сопряженное СЗИ и обратно.

Таким образом, по сравнению с рассмотренными ранее решениями, в предлагаемом техническом решении не требуется отдельный канал для обмена служебными данными узлов системы КРК при выработке квантовых ключей, вместо этого используется единый канал для передачи служебных сообщений системы КРК и передачи закодированных пользовательских данных, что позволяет снизить затраты на создание, развертывание и эксплуатацию комплекса.

Транспортная линия связи может быть доступной для атак возможного нарушителя. При использовании предлагаемого устройства и способа критически важная информация, содержащая сведения о данных в транспортной линии связи, включая служебные данные классического канала системы КРК о квантовом ключе, передается в закодированном виде на текущем ключе кодирования. Данное решение повышает защищенность передаваемых пользовательских данных.

Для аутентификации служебных данных протокола КРК выбрана функция вычисления имитовставки ГОСТ Р 34.13-2018 [100], обладающая вычислительной стойкостью (см. обоснование выбора вычислительно стойких способов аутентификации в разделе 2.1). При этом необходимо производить аутентификацию каждого передаваемого сообщения целиком, что гарантирует его целостность на принимающей стороне. Обычно при аутентификации сообщений, передаваемых по классическим линиям связи, сообщение перед передачей разбивается на части (например, кадры для линии связи, выполненной в виде Ethernet, или IP-пакеты для линии связи, выполненной в виде WAN, LAN) с последующим добавлением имитовставки к каждой части. Такой способ гарантирует целостность каждой части в отдельности (т.е. целостность данных на транспортном уровне), но не гарантирует целостность полного сообщения, собранного из отдельных частей, так как, например, может быть нарушен порядок частей сообщения.

В квантовой аппаратуре предлагается реализация дополнительных модулей согласования ключей, выполняющих функции накопления случайной последовательности и формирования квантовых ключей. При этом после накопления достаточного количества квантовых ключей из них формируются общие секреты для СЗИ и ключи аутентификации для аутентификации служебных данных системы КРК, передающихся между Клиентом и Сервером КРК в процессе выполнения квантового протокола. Под достаточным количеством накопленных квантовых ключей понимается число квантовых ключей, суммарная длина которых не меньше суммарной длины хотя бы одного общего секрета и одного ключа аутентификации. Необходимые длины общего секрета и ключей аутентификации определяются применяемыми способом кодирования в СЗИ и способом аутентификации.

За счет накопления квантовых ключей перед дальнейшим формированием ключей кодирования и ключей аутентификации достигается повышение надежности комплекса в случае непредвиденных кратковременных сбоев системы КРК, выражающихся во временном прекращении генерации квантовых ключей или вызванных, например, атаками нарушителя на квантовый канал связи. В таком случае уже выработанные квантовые ключи сохраняются, и после восстановления работоспособности системы КРК продолжается накопление квантовых ключей к уже имеющимся накопленным ранее квантовым ключам. Также работоспособность комплекса сохраняется в случае выработки системой КРК квантовых ключей, длина которых недостаточна для формирования новых ключей кодирования и ключей аутентификации. В этом случае происходит накопление ключей для формирования требуемых общих секретов и ключей аутентификации уже из совокупности накопленных квантовых ключей.

Предлагается два варианта контроля идентичности ключей на двух концах квантового канала в зависимости от рассматриваемых возможных сбоев при работе аппаратуры.

В первом случае полагается, что случайная последовательность, полученная в результате протокола КРК идентична, а формирование ключей из

последовательности происходит без сбоев. Контроль целостности передачи данных от квантовой аппаратуры в СЗИ производится непосредственно средствами организации канала, через который проходит служебная линия связи, и передача данных защищена от случайных искажений.

В таком способе возможно согласование ключей по их идентификаторам путем сравнения идентификаторов ключей. Если идентификаторы не совпадают, то соответствующие им ключи отбрасываются (удаляются), чтобы не нарушать работоспособность комплекса из-за расхождения ключей, которые должны быть идентичными. За счет дополнительного сравнения идентификаторов переданных общих секретов в СЗИ (помимо их сравнения в модулях согласования ключей перед передачей в СЗИ) достигается повышение надежности комплекса в случае искажений (случайных или преднамеренных), вносимых служебной линией связи, связывающей узел системы КРК с СЗИ.

Если рассматривается модель, в которой возможны случайные сбои как внутри устройства, так и при передаче данных от квантовой аппаратуры в СЗИ, дополнительно производится сравнение хэш-значений от сформированного общего секрета в паре устройств. Напомним, что классический аутентифицированный канал квантовой аппаратуры проходит через транспортный канал данных, защищенный на текущем ключе кодирования. Сервер КРК перед помещением сформированного общего секрета вычисляет его хэш-значение от секрета и его идентификатора и передает полученное хэш-значение вместе с идентификатором ключа в Клиент КРК. Клиент КРК вычисляет хэш-значение от секрета и его идентификатора на своей стороне и сравнивает его значение с полученным от Сервера КРК. В случае успешного сравнения Клиент КРК посылает соответствующее уведомление на Сервер КРК, после чего Сервер КРК и Клиент КРК помещают проверенные общие секреты в свои ключевые хранилища. В противном случае секреты и оставшаяся часть квантовой гаммы отбрасываются. СЗИ, при получении общих секретов от квантовой аппаратуры аналогично могут вычислять и сравнивать хэш-значения от полученных секретов с их идентификаторами между собой перед помещением ключей в свои ключевые

хранилища. В качестве хэш-функции предлагается использовать стандартизированную хэш-функцию согласно ГОСТ 34.11-2018 [65].

В результате в рамках комплексного проекта, выполняемого по Соглашению № 03.G25.31.0254 от 27.04.2017 с Министерством образования и науки Российской Федерации, было разработано устройство комплекса квантовой аппаратуры защиты информации и способ его функционирования, реализованный в промышленном комплексе ViPNet Quandor. На устройство и способ получен патент РФ №2736870 [43].

Техническим результатом разработанного комплекса и способа являются:

1) повышение надежности комплекса, в том числе в случае искажений (случайных или преднамеренных), вносимых локальной линией связи; в случае непредвиденных или преднамеренных кратковременных сбоев системы КРК, выражающихся во временном прекращении генерации квантовых ключей; в случае низкой скорости генерации квантовых ключей и/или генерации квантовых ключей малой длины; а также в случае навязывания ложных идентификаторов ключей;
2) снижение затрат на создание, развертывание и эксплуатацию комплекса за счет уменьшения числа классических линий связи;
3) повышение стойкости квантовых ключей, вырабатываемых системой КРК, за счет аутентификации служебных данных системы КРК на ключах аутентификации, сформированных из квантовых ключей, и аутентификации служебных данных системы КРК целиком, до разбиения на блоки, используемые при передаче по цифровой линии связи, и последующего кодирования служебных данных системы КРК в транспортной линии связи между парой СЗИ.

2.3 Выводы по главе

В данной главе проведен анализ способов аутентификации классического аутентифицированного канала для систем КРК, обладающих теоретико-информационной стойкостью. Данные способы требуют объем ключа аутентификации пропорционально объему аутентифицируемых данных, передаваемых в классическом канале. В связи с этим их применение в системах КРК, обладающих недостаточной скоростью создания квантовых ключей, обусловленной высокой степенью сжатия этапа усиления секретности, может быть недоступно. При достаточном объеме ключевого материала рекомендовано вычисление имитовставки от сообщений классического аутентифицированного канала функциями универсального хэширования в конструкции Stinson.

Произведен расчет требуемых объемов ключей аутентификации, необходимых для проведения одного сеанса КРК. В качестве альтернативного подхода предлагается применение вычислительно стойких алгоритмов вычисления меток аутентификации. Способы аутентификации, обладающие вычислительной стойкостью, допускают многократное применение ключа аутентификации, что существенно снижает расход квантовых ключей на формирование ключей аутентификации для следующих сеансов КРК и позволяет сохранить работоспособность системы КРК в случае кратковременных сбоев выработки квантовых ключей.

Проведен анализ способов сопряжения квантовой аппаратуры с парой пользовательских СЗИ. В результате анализа выявлены научные проблемы, возникающие при согласовании квантовых последовательностей в процессе формирования общих секретов для СЗИ и в процессе передачи этих секретов в СЗИ. Разработан способ взаимодействия квантовой аппаратуры с пользовательскими СЗИ, уточняющий процессы синхронизации квантовых ключей и их передачи в СЗИ. На способ и устройство, реализующее разработанный способ получен патент РФ № 2736870 [43]. Данный способ успешно реализован в комплексе ViPNet Quandor.

3 МЕТОДИКА РАСПРЕДЕЛЕНИЯ ОБЩЕГО СЕКРЕТА МЕЖДУ УЗЛАМИ СЕТИ КРК МАГИСТРАЛЬНОЙ ТОПОЛОГИИ

В предыдущей главе рассматривалось решение научных проблем, возникающих при реализации технологии КРК в простейшей топологии «точка-точка». Как отмечалось в разделе 1.2, технология КРК, реализуемая через оптоволоконные квантовые каналы, имеет ограничения по максимальной длине квантового канала. Для распространенных систем [7], [8], [9], не использующих сверхпроводящие детекторы, предельная длина квантового канала составляет примерно 100 км, а рекомендуемая длина, на которой существенно возрастает скорость генерации квантовых ключей – 50 км. Возникает научная проблема, как распределять общий секрет на пары СЗИ, удаленные друг от друга на существенно большие расстояния, чем предельная длина квантового канала.

Выделяют два подхода к решению этой проблемы. Первый подход заключается в создании так называемых квантовых повторителей [71], [104], [105], т.е. устройств, которые смогли бы тем или иным образом получать передаваемые однофотонные состояния и пересылать их в следующий квантовый канал без изменений. Однако, теорема о запрете клонирования квантовых состояний [106] запрещает классическое измерение однофотонных сигналов без их искажений. Заметим, что этим объясняется устойчивость протоколов КРК к атаке прием-перепосыл [16], не позволяющая нарушителю встраиваться в квантовый канал и имитировать сопряженную сторону взаимодействия без вмешательства в классический аутентифицированный канал между легитимными участниками протокола КРК.

В настоящее время ведутся работы по проектированию сетей КРК, использующих спутанные (entanglement) фотоны и устройства с квантовой памятью для создания квантовых повторителей, способных передавать информацию между двумя участниками протокола КРК, соединенными несколькими последовательными квантовыми каналами [71], [107]. Однако, создание квантовой памяти не видится возможным в ближайшие несколько лет, что, например, обсуждалось на конференции QCrypt-2019 в докладе [20], поэтому

существует потребность в альтернативном подходе к преодолению ограничений по длине квантового канала.

На сегодняшний день доступным подходом является применение доверенных промежуточных узлов. В этом случае протокол КРК выполняется между соседними узлами, соединенными одним сегментом квантового канала [108], [109]. После получения квантового ключа на всех сегментах такой сети данные квантовые ключи используются для распределения общего секрета между узлами, соединенными через последовательную цепочку узлов. Такую сеть будем называть сетью квантового распределения ключей (или квантовой сетью). Однако, наименование «квантовая сеть» не совсем корректно и чаще встречается в научно-популярных источниках, не делающих различия между истинно квантовой сетью, реализованной на квантовых повторителях, и сетью с промежуточными узлами.

Схематичное изображение сети с доверенными промежуточными узлами представлено на рисунке 11. Главной научной задачей является задача распределения общего секрета для произвольных пар УКС. Согласно п. 1.2, в основе способа распределения общего секрета лежит передача некоторого квантового ключа по цепочке УКС. Следовательно, для распределения общего секрета необходимо определить цепочку УКС, соединяющую требуемую пару УКС, после чего на определенной цепочке произвести распределения общего секрета.

Введем следующие определения. Зеленым, желтым и синим цветом на рисунке показаны УКС. УКС, на которые распределяется общий секрет, будем называть целевыми. Целевые УКС обозначены синим цветом. В данном случае они являются оконечными, т.е. имеют соединение только с одним другим УКС. Желтым отмечены УКС, входящие в одну из цепочек, соединяющую целевые УКС. К целевым УКС подключена пара СЗИ, между которыми организуется защищенный канал взаимодействия с защитой с применением общего секрета, получаемого от сети КРК.

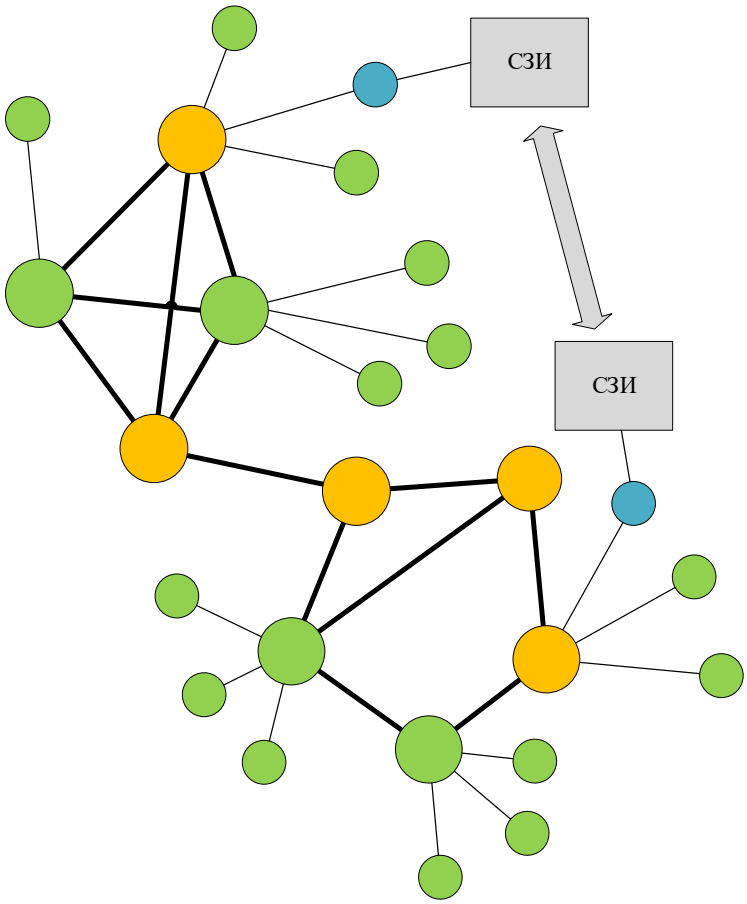


Рисунок 11 – Схематичное изображение сети КРК с доверенными промежуточными узлами

3.1 Сеть квантового распределения ключей магистральной топологии

Каждую цепочку УКС можно рассматривать как подсеть магистральной топологии некоторой сети КРК. Такая магистральная подсеть представлена на рисунке 12. Подключение внешних СЗИ производится к оконечным УКС такой сети. Магистральная сеть является основным конструктивом для распределения общих секретов между оконечными УКС.

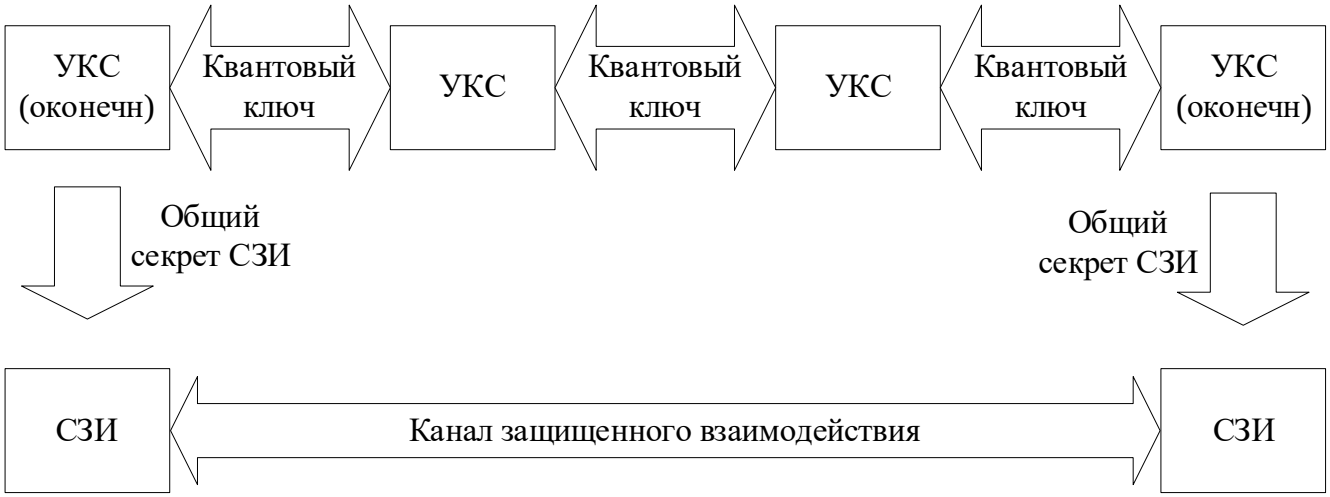


Рисунок 12 – Схема сети КРК топологии «магистраль»

Магистральная сеть КРК распределяет общий секрет между двумя оконечными УКС для дальнейшей его передачи во внешние СЗИ. Внешние СЗИ организуют защищенный канал связи напрямую между собой с использованием полученного общего секрета. Именно вариант такого использования магистральной сети КРК представлен на рисунке 12.

Альтернативный подход описан в работе [110]. В этом случае полученные на сегментах сети квантовые ключи используются непосредственно для организации защищенных каналов для передачи пользовательских данных с последовательным кодированием и раскодированием по сегментам сети. Схема такого использования магистральной сети представлена на рисунке 13.

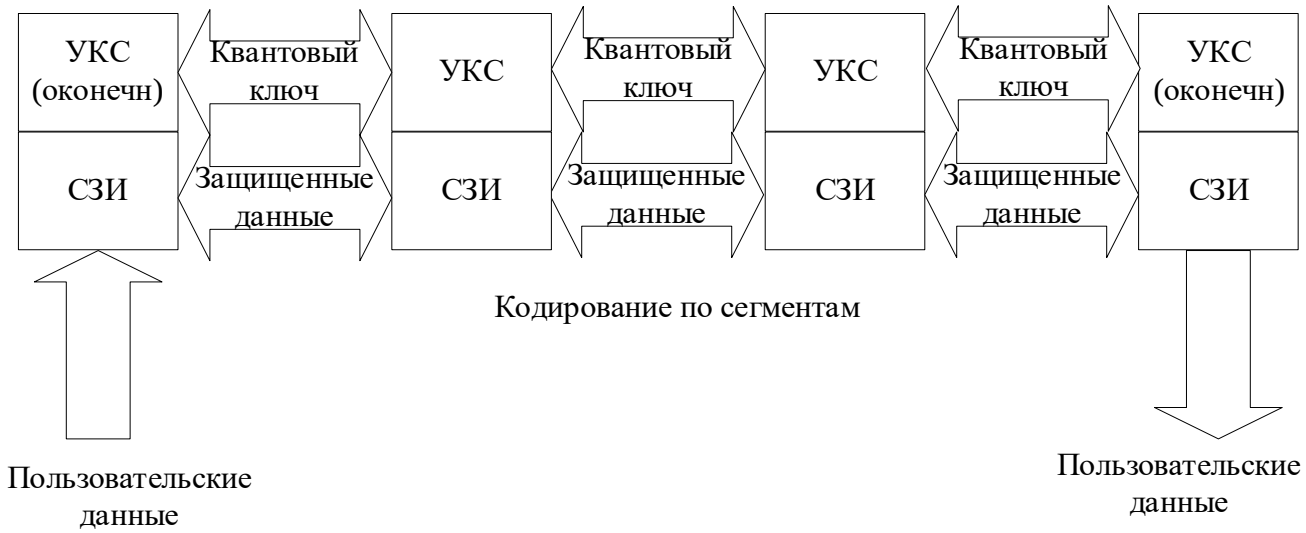


Рисунок 13 – Сценарий использования сети КРК с передачей полезной нагрузки по сегментам

Такой подход имеет следующие недостатки. Во-первых, возникает вопрос доверия владельца информации к промежуточным УКС, на которых его информация появляется в открытом виде при перекодировании. Во-вторых, скорость генерации квантовых ключей недостаточна для предоставления такого сервиса из-за существенных объемов пользовательских данных. Открытые сети связи общего пользования имеют пропускную способность в несколько терабит в секунду, а промышленные СЗИ уровня L2 [111], [112] нацелены на скорости до сотен гигабит данных в секунду. Скорости генерации квантовых ключей в настоящее время не превышают гигабита в секунду.

Таким образом, целесообразнее первый подход применения магистральной сети КРК (см. рисунок 12), что также подтверждается подходами, рекомендуемыми к использованию в сетях КРК, описанными в [37], [38].

3.2 К вопросу об определении цепочки УКС в сети смешанной топологии

Как показано в п. 3.1, для распределения общего секрета в сети КРК смешанной топологии требуется определить цепочку УКС, на которой будет распределяться этот секрет. Процесс определения цепочки УКС в общем случае сложная задача. Для решения данной научной задачи предлагается первым шагом рассмотреть ее решение для простых топологий.

Наиболее простой топологией после магистральной топологии является топология «звезда». Сети КРК топологии «звезда» служат для уменьшения количества связей квантовыми каналами в ситуациях, когда необходимо связать множество узлов, локализованных на небольшой территории (здание, группа зданий, небольшой город). Такой сценарий использования сети КРК обычно применяется в городских сетях [14], [113], [114]. Организация квантовых каналов между всеми узлами городской квантовой сети слишком затратная, так как на каждую пару узлов, между которыми планируется взаимодействие, необходимо установить полный комплект квантовой аппаратуры и проложить выделенный квантовый канал, выделенную оптоволоконную линию.

Известны следующие оптимизации сетей КРК топологии «звезда». Центр звезды оснащается одним полукомплектом квантовой аппаратуры, к которому подключаются несколько квантовых каналов. В периферийные УКС звезды устанавливаются полукомплекты квантовой аппаратуры, каждый из которых может быть сопряжен с полукомплектом в центре звезды. Такой вариант сети КРК использован в китайской квантовой сети в городе Wuhu [78]. В подсети КРК установлен оптический мультиплексор, переключающий квантовые каналы по принципу разделения времени. Схема городской сети города Wuhu приведена на рисунке 14. Преимуществом подобной организации городских сетей в топологии звезда заключается в уменьшении стоимости создания таких сетей, а также увеличении предельной дальности между двумя оконечными УКС, для которых необходимо вырабатывать общий секретный ключ. Расстояние между двумя оконечными УКС будет до двух раз больше, чем при прямом соединении квантовым каналом этих УКС.

Однако управление квантовыми каналами с разделением по времени, а точнее последовательное включение квантовых каналов на равные временные интервалы, как реализовано в сети [78], не является оптимальным, так как не учитывает фактическую потребность пар СЗИ в общих секретах, а также разницу в длине квантовых каналов, а следовательно, разницу в скоростях генерации квантовых ключей на каждом квантовом канале. Поэтому, при построении сетей КРК с объединением квантовых каналов через оптический коммутатор, необходимо использовать управляемое переключение квантовых каналов, реализуемое управляемыми оптическими коммутаторами, с учетом фактической скорости генерации квантовых ключей на каждом квантовом канале и потребности пар СЗИ в общих секретах.

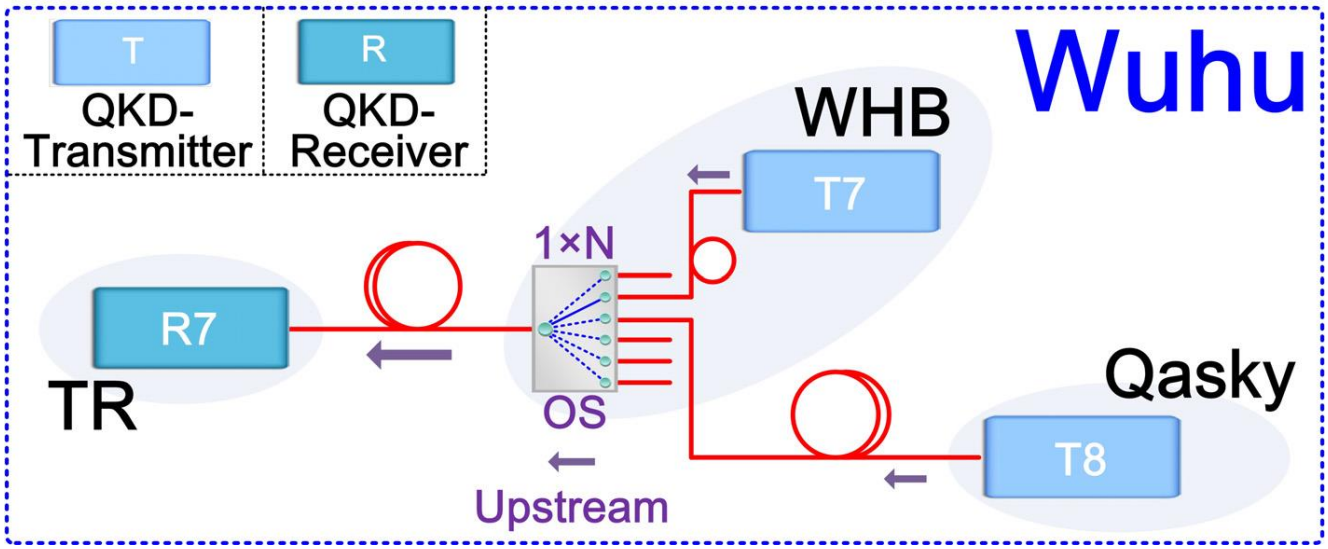


Рисунок 14 – Схема городской подсети КРК города Wuhu

Определение цепочки УКС в сети КРК топологии «звезда» тривиально из-за единственного центра звезды, через который обязательно проходят все возможные цепочки УКС. То есть фактически такая сеть представляет собой совокупность магистральных линий, каждая из которых состоит из трех УКС, причем все магистральные линии пересекаются в промежуточном УКС. При этом существует не единственное отображение такой сети в совокупность магистральных сетей. Это означает, что любой оконечный УКС имеет возможность распределить общий секрет с любым другим оконечным УКС.

Согласно п. 1.2, централизованное управление сетью КРК смешанной топологии при определении требуемых цепочек УКС создает узкое место отказа всей системы. Однако, в простых сетях топологии «звезда» такой центр управления существует в силу самой топологии. Поэтому централизованное управление распределением общих секретов в таких простых сетях предпочтительнее.

Схема сети КРК топологии «звезда» представлена на рисунке 15.

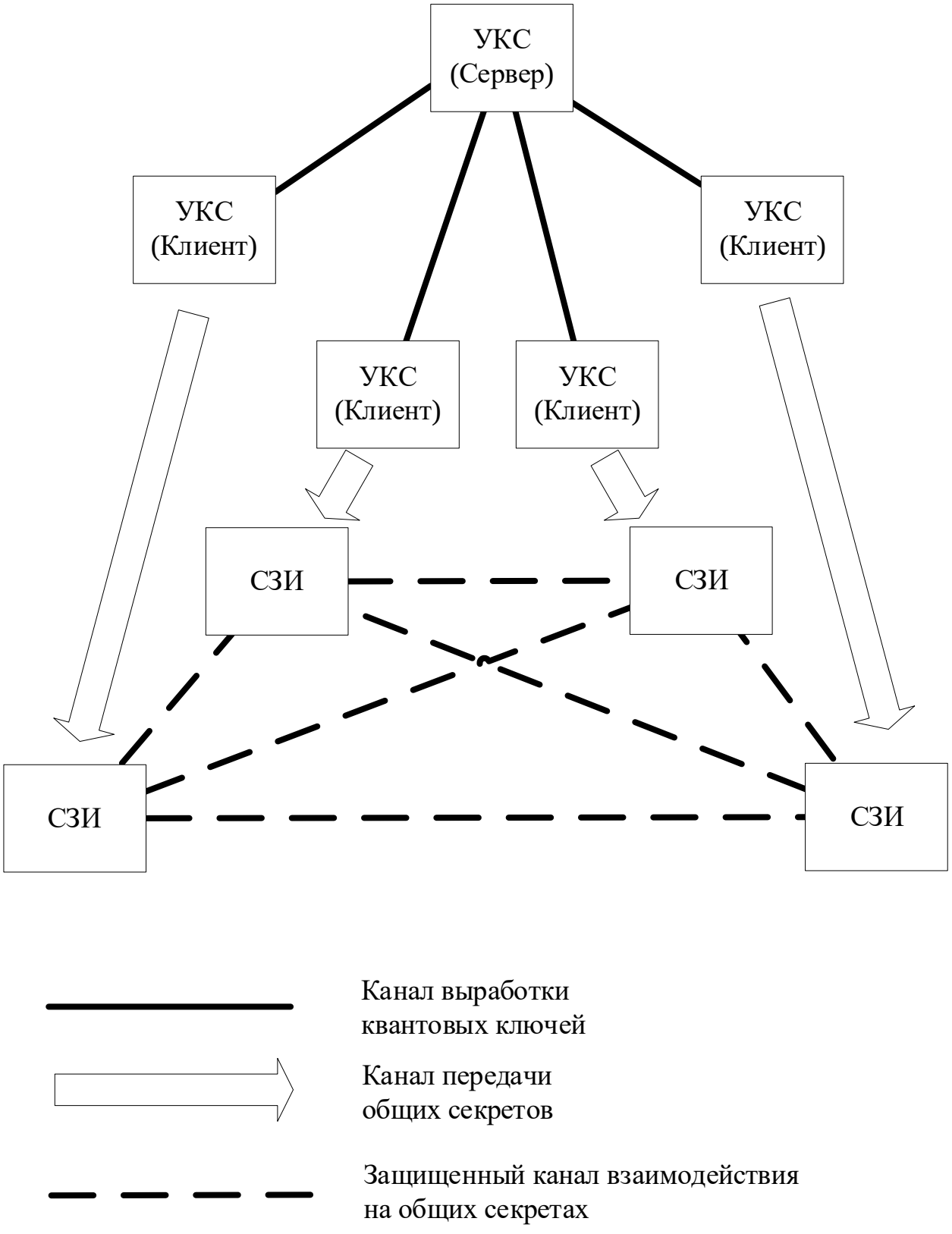


Рисунок 15 – Схема сети КРК топологии "звезда"

Таким образом, при централизованном управлении в сети топологии «звезда» центральный УКС самостоятельно инициирует выполнение протокола КРК, инициирует распределение общего секрета для пары УКС, в том числе

выделяет необходимые пары УКС и, соответственно, цепочки УКС для распределения общего секрета. В результате порядок функционирования сети КРК топологии «звезда» имеет следующий этапы: создание квантовых ключей с каждым периферийным УКС и распределение общих секретов для пар УКС при наличии достаточного количества квантовых ключей.

Этап 1. Создание квантовых ключей с каждым периферийным УКС.

– Центральный УКС выбирает из набора периферийных УКС некоторый УКС, например, имеющий меньший идентификатор.
– Центральный УКС переключает оптический коммутатор таким образом, чтобы был построен непрерывный квантовый канал с выбранным периферийным УКС.
– Центральный УКС инициирует выработку квантовых ключей с выбранным периферийным УКС.
– При накоплении заданного порогового количества квантовых ключей Центральный УКС прерывает выработку квантовых ключей. Пороговое значение определяется используемым способом распределения общего секрета.
– Центральный УКС переходит к созданию квантовых ключей с другим периферийным УКС.

Когда с каждым периферийным УКС выработаны начальные квантовые ключи можно переходить от последовательного выбора периферийных УКС к управляемому выбору, который зависит от необходимой частоты распределения общих секретов для пар оконечных УКС. Важно поддерживать количество доступных квантовых ключей между центральным УКС и каждым оконечным УКС пропорциональным количеству запросов общих секретов между данным оконечным УКС и любым другим оконечным УКС с учетом используемого способа распределения общего секрета.

Этап 2. Распределение общих секретов для пар УКС.

При наличии достаточного числа квантовых ключей хотя бы с двумя периферийными УКС можно переходить к процессу распределения общих секретов.

– Центральный УКС выбирает пару периферийных УКС, с которыми выработаны квантовые ключи.
– Первому периферийному УКС из пары передается команда на формирование общего секрета с указанным вторым периферийным УКС.
– Периферийные УКС реализуют способ распределения общего секрета, а центральный УКС маршрутизирует передачу данных при распределении этого секрета между двумя выбранными периферийными УКС, возможно с перекодированием передаваемых данных с использованием квантовых ключей, выработанных с каждым из этих двух оконечных УКС.

Данные этапы независимы и через некоторое время после начала работы сети КРК могут происходить в сети КРК параллельно, снабжая пары оконечных УКС общими секретами для дальнейшего использования. При необходимости в городских сетях может использоваться приоритизация запросов на формирование общих секретов в зависимости от приоритетов, заданных подключенным потребителям.

Заметим, что приведенный порядок функционирования сети в топологии «звезда» целесообразен для изолированных сетей. Функционирование подсети топологии «звезда» из состава сети смешанной топологии рекомендуется реализовывать в соответствии с общим порядком функционирования сети смешанной топологии (см. п. 4.2).

3.3 Разработка способов распределения общего секрета для оконечных узлов

Основной научной задачей настоящего исследования является разработка и анализ способа распределения общего секрета. Как было показано в п. 3.2, распределение общего секрета в сетях КРК смешанной топологии сводится к задаче распределения общего секрета в магистральной подсети КРК. Далее будет

решаться задача именно в магистральной сети КРК с произвольным числом промежуточных УКС.

Согласно п. 1.2, в основе способа распределения общего секрета на пары УКС лежит передача ключевого материала по цепочке УКС. Работы, посвященные процессам функционирования сетей КРК, например [67], [82], [109], [115], именуют процесс распределения общего секрета «trusted key relay», доверенной передачей ключа, а сам общий секрет именуют квантовым ключом. Такое именование общего секрета вызывает дополнительную путаницу, так как объединяет в себе и истинно квантовые ключи, полученные в результате выполнения протокола КРК, и ключи, полученными иным образом.

Общий секрет, распределенный на пару целевых УКС, в отличие от квантового ключа, получен не в результате протокола КРК, а путем передачи ключевого материала под защитой на квантовых ключах. То есть общий секрет целевых УКС – ключ, созданный сетью КРК, передаваемый по сети КРК с защитой на квантовых ключах. Предлагается ввести термин «квантовозащищенный ключ (КЗК)», обозначающий такие ключи, являющиеся продуктом функционирования сети КРК и предназначенные для целевых УКС. **Квантовозащищенный ключ** (КЗК) – ключ, созданный сетью КРК, ключевой материал для создания которого передавался по сети КРК с защитой на квантовых ключах. КЗК является результатом выполнения способа распределения общего секрета для двух целевых УКС.

3.3.1 Ожидаемые свойства распределения квантовозащищенных ключей

Решая научную задачу распределения КЗК, необходимо определить те свойства данного объекта, которыми он будет обладать в зависимости от способа его распределения.

Примечание – Все приведенные здесь свойства целесообразно рассматривать до передачи КЗК во внешнее СЗИ для дальнейшего использования. Требование о неотличимости от случайного ключа может быть уточнено введением порога на допустимую вероятность этого события.

1) Неотличимость КЗК от случайного числа:
   - для нарушителя с любыми вычислительными ресурсами;
   - для нарушителя с ограниченными вычислительными ресурсами;
   - для нарушителя с ограниченными вычислительными ресурсами даже при компрометации всех квантовых ключей в системе;
2) Недоступность КЗК на промежуточных узлах;
3) Непредсказуемость КЗК в вычислительном смысле даже в случае, когда один из целевых УКС доступен нарушителю.
4) Сохранение защиты от чтения назад для КЗК.

Примечание – Математическое описание изложенных свойств КЗК требует строгого описания модели нарушителя для конкретной сети КРК. Таким образом, точные свойства КЗК можно будет оценить только в конкретной реализации сети КРК. Несмотря на это, проведенное исследование демонстрирует допустимые способы для распределения КЗК и их анализ.

Краткий анализ возможных свойств КЗК

Сеть КРК должна оставаться безопасной даже в случае компрометации всех квантовых ключей. Это означает, что КЗК обязательно должен обладать первым свойством в условии компрометации квантовых ключей. Данное требование связано с тем, что квантовые технологии недостаточно изучены и появляются новые вектора атак на техническую реализацию систем КРК. Такие атаки разрабатываются и моделируются, например, группой В. Макарова [24], [116], [117], [118]. Протокол КРК, стойкий в теоретической модели, может иметь уязвимости в конкретной реализации или могут быть изобретены новые атаки на техническую реализацию. Таким образом, необходимо, чтобы КЗК не были скомпрометированы даже в результате компрометации и/или навязывания одного или нескольких квантовых ключей.

Свойства два и три являются опциональными, их наличие повышает защищенность КЗК в условиях нарушителя, обладающего возможностью влиять на работу некоторого УКС.

Третье свойство предполагает, что в выработке ключевой информации для формирования КЗК участвуют два узла. При этом даже если один узел ведет себя злонамеренно, то ключевой информации, распределенной другим узлом, должно хватать для формирования ключа, неотличимого от случайного в вычислительном смысле. Другими словами, ни один из участников выработки КЗК не должен иметь возможность предсказать итоговый КЗК до начала его формирования. Процедуру выработки КЗК, которая обладает этим свойством, будем называть симметричной.

Симметричность при распределении ключевого материала

Для того, чтобы КЗК обладал третьим свойством, необходимо, чтобы в процессе его выработки оба целевых узла формировали ключевой материал, на основе которого вычисляется КЗК. Кроме того, ни у какого целевого узла, даже если на нем известен ключевой материал другого узла, не должно быть возможности (в вычислительном смысле) так выбрать свой ключевой материал, чтобы итоговый ключ КЗК отличался от случайного ключа в вычислительном смысле. Важно понимать, что при неограниченных вычислительных ресурсах узлов, эта задача не имеет решения, так как объем формируемого ключевого материала каждым узлом ограничен, следовательно, некоторый узел, получив одну часть ключевого материала имеет достаточно ресурсов для полного перебора всех вариантов второй части ключевого материала при необходимости предсказать результат формирования КЗК

Таким образом, на практике решения задачи формирования симметричного КЗК при условии неограниченных вычислительных возможностей нарушителя не существует. Злоумышленнику, который захватил управление одного узла, всегда доступна следующая атака. Зная ключевой материал одного узла, можно перебирать ключевой материал другого узла до тех пор, пока результирующий ключ не будет удовлетворять интересам злоумышленника. Т.е., совершив в среднем 2^t попыток подбора ключевого материала, злоумышленник сможет навязать t бит в результирующий ключ КЗК. Наличие такой возможности не позволяет считать КЗК случайным ключом в вычислительном смысле.

Заметим, что описанная атака имеет экспоненциальную сложность. Поэтому третье свойство реализуемо в условии, что распределение КЗК должно быть неотличимо от равновероятного распределения на множестве из 2^{n-t} элементов, где n – размер ключа, а t – параметр безопасности, который выбирается исходя из вычислительных возможностей нарушителя, даже в том случае, если один из целевых узлов оказался под контролем злоумышленника.

В такой формулировке указанное свойство достигается следующим способом: оба целевых узла формируют свой ключевой материал и обмениваются им; КЗК вычисляется как результат применения хэш-функции ко всему ключевому материалу. Так как хэш-функция обладает стойкостью к поиску первого прообраза, стойкостью к поиску второго прообраза и стойкостью к коллизиям, то она подходит для вычисления КЗК. Так же может использоваться ключевая хэш-функция, например, HMAC.

Примечание – Использование хэш-функции является достаточным условием. Формирование строгих математических требований к свойствам функции, которая бы подходила для формирования КЗК остается не решенной задачей.

С точки зрения эксплуатационных свойств предпочтительнее, чтобы функция вычисления КЗК являлось симметричной по своим аргументам, то есть $F(x,y) = F(y,x)$. Такое свойство позволяет не контролировать порядок аргументов функции на узлах. В качестве такой функции можно предложить следующее решение: в качестве хэш-функции выбрать одну из рекомендованного семейства ГОСТ Р 34.11-2018 [65], а для достижения свойства симметричности, например, упорядочить аргументы по возрастанию: т.е. $F(x,y) = Hash\,(a,b)$, где $a = min(x,y), b = max(x,y)$, функция $min(x,y)$ возвращает наименьший из двух аргументов, а функция $max(x,y)$ возвращает наибольший из двух аргументов.

Защита от чтения назад

Наличие четвертого свойства у КЗК означает, что, зная текущие ключи сети КРК и ранее пересылаемые по каналам данные, вычисление предыдущих ключей

КЗК остается вычислительно сложной задачей для нарушителя. Это свойство можно достичь несколькими способами:

– Используя односторонние преобразования над ключами, например, вычисление производных ключей и удаление исходных ключей. Этот способ требует согласованного перехода узлов сети на новые ключи, в противном случае может произойти потеря синхронизации ключей.
– Вычисляя производные ключи с использованием внешней энтропии, а после вычисления удаляя энтропию. При реализации такого способа необходимо, чтобы используемую энтропию нельзя было восстановить из ранее пересылаемых сообщений и текущих ключей сети КРК. В качестве источника внешней энтропии используются квантовые ключи, так как они обладают сколько угодно малой отличимостью от случайных чисел, и их нельзя восстановить по предыдущим сообщениям [49].

Примечание – Защиту от чтения назад можно обеспечить при помощи протокола Диффи-Хеллмана, но он основан на вычислительной задаче, решение которой не является вычислительно сложной для атакующего с квантовым компьютером. По этой причине подобные механизмы в работе не рассматриваются.

Недоступность КЗК на промежуточных узлах

Второе свойство можно сформулировать в двух вариантах: слабом и сильном. В слабом варианте оно означает, что организационно-техническими мерами противодействия, такими как аутентификация пользователей, разграничение прав доступа пользователей, физическое ограничение доступа до устройства путем создания контролируемой зоны, использование датчиков вскрытия корпуса и т.д., гарантируется, что внутренний или внешний нарушитель не сможет получить доступ к КЗК на узлах сети КРК.

В сильном варианте это свойство означает, что КЗК, находясь на момент передачи на узле сети, защищен алгоритмом с использованием секретного ключа, без знания которого вычислительно сложно нарушить конфиденциальность и

целостность КЗК. Можно сформулировать еще более сильный вариант, заменив вычислительную стойкость на теоретико-информационную.

Для обеспечения второго свойство в сильном варианте необходимо использовать заранее распределенные между целевыми узлами ключи. Если такие ключи имеются и механизмы распределения КЗК предполагают их использование, то указанное свойство достигается.

Таким образом, обязательными для КЗК, полученного в результате реализации некоторого способа распределения являются первое и четвертое свойство. Наличие второго и третьего свойства обеспечивает сохранение защищенности системы в условиях нарушителя, обладающего дополнительно возможностью влиять на некоторый УКС.

3.3.2 Разработка способов распределения КЗК

В этом разделе разрабатываются способы распределения КЗК для решения основных недостатков базового метода распределения КЗК: доступность КЗК на промежуточных УКС сети КРК, необходимость обеспечения доверия к промежуточным УКС, использование квантовых ключей в качестве итоговых КЗК.

КЗК (или ключевой материал, его составляющий) передается по цепочке УКС. Пример такой цепочки приведен на рисунке 16. Количество УКС в цепочке не ограничено, соседние узлы в цепочке имеют общий квантовый ключ. В случае если цепочка состоит только из двух целевых узлов, описанные способы остаются корректными.

Рисунок 16 – Путь между узлами «A» и «C»

На рисунке целевые узлы обозначены «A» и «C», а промежуточные «B_i». В рассматриваемых способах для упрощения описания рисунки будут представлены для конкретного количества узлов пути.

3.3.2.1 Способ одновременной доставки секрета

Предлагаемый способ предназначен для быстрого распределения КЗК между двумя целевыми УКС. При достаточно длинных цепочках УКС последовательная передача КЗК обладает плохими эксплуатационными свойствами, последовательное перекодирование на каждом УКС требует значительных временных ресурсов. Способ предполагает, что все узлы в цепочке являются доверенными. Способ предполагает раскрытие ключей парной связи между всеми участниками цепочки. Преимуществом способа является повышение эксплуатационных характеристик сети КРК за счет уменьшения времени передачи общего секрета на целевые УКС.

Для того чтобы описать способ, достаточно рассмотреть цепочку, состоящую из четырех узлов: узлы «A» и «D» являются целевыми, узлы «B» и «C» являются промежуточным. Узлы «A» и «B» имеют общий ключ K_{AB}, узлы «B» и «C» имеют общий ключ K_{BC}, узлы «C» и «D» имеют общий ключ K_{CD}. Схема такой цепочки приведена на рисунке 17.

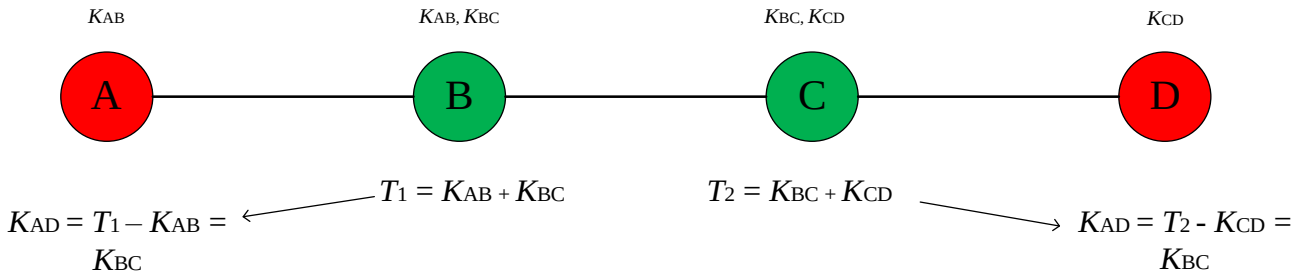


Рисунок 17 – Способ одновременной доставки секрета

Необходимо распределить общий секрет между целевыми УКС «A» и «D». Способ предполагает, что ключи бывают двух видов: целевые ключи и служебные ключи. Один из квантовых ключей становится общим секретом целевых УКС, для его защищенной доставки используются служебные ключи. В рассматриваемом примере ключ K_{BC} является целевым, а все остальные ключи: K_{AB}, K_{CD}, являются служебными ключами. Для того, чтобы выбрать какой именно целевой ключ станет общим секретом целевых УКС необходимо разделить цепь на две подцепи,

расцепив ее посередине, чтобы длины цепей составляли $\left\lfloor \frac{n}{2} + 1 \right\rfloor$ и $\left\lfloor \frac{n}{2} \right\rfloor$. Квантовый ключ расцепленных УКС становится общим секретом целевых УКС.

Для защищенной доставки этого секрета до целевого УКС используются служебные ключи: все узлы подцепи формируют сообщения, в которых защищенным образом записывается информация, в совокупности позволяющая восстановить на целевом узле целевой общий секрет. На рисунке 17 проиллюстрирован способ, который пригоден для квантовых ключей. Узлы подцепи пересылают на свой целевой узел напрямую сумму по модулю два двух квантовых ключей, которые хранятся на узлах. Просуммировав все полученные суммы и добавив к ним известный на целевом узле квантовый ключ, можно вычислить целевой общий секрет.

Подробнее проанализируем предложенный способ. Способ позволяет производить параллельные вычисления и легко масштабируется на большее число узлов. Для цепи из n узлов нужно совершить $n - 1$ защищенную передачу ключей. В предположении, что одна передача происходит за t секунд и узел способен одновременно принять до $\left\lfloor \frac{n}{2} + 1 \right\rfloor$ защищенных ключей, получаем, что распределить общий секрет между двумя целевыми узлами можно за t секунд. Если существует ограничение на количество одновременно принятых пакетов, то способ может быть реализована иерархично, глубина иерархии зависит от ограничения на количество одновременно принятых пакетов. Предположим, что узел может одновременно принимать m сообщений, тогда процесс распределения займет $\left\lceil \frac{\left\lfloor \frac{n}{2}+1 \right\rfloor}{m} \right\rceil \cdot t$ секунд.

Дополнительно необходимо обеспечивать целостность передаваемой информации с использованием алгоритмов соответствующего класса (вычислительно стойких или теоретико-информационно стойких).

Способ обладает следующими достоинствами.

– За счет параллельной отправки способ позволяет быстро распределить информацию, в отличие от передачи информации последовательно по цепи.

– При использовании теоретико-информационно стойких алгоритмов, распределение общих секретов будет теоретико-информационно стойким.

– Для распределения общих секретов между целевыми УКС требуется на одну пересылку ключевой информации меньше, чем при последовательном распределении.

В качестве недостатков способа можно выделить то, что:

– Способ требует большого количества ключевого материала.

– Способ требует наличия классических каналов связи между целевыми УКС и всеми УКС его подцепи.

– Все узлы цепи узнают используемые ключи: целевой ключ и служебные ключи всей цепи.

3.3.2.2 Способ с использованием ключевого контейнера с блочным шифром или шифроблокнотом

Данный способ обобщает базовый способ распределения КЗК, заменяя конкретную передачу с защитой одноразовым шифроблокнотом на передачу в ключевом контейнере, т.е. в конструкции, обеспечивающей конфиденциальность и целостность. В общем случае конкретные примитивы, из которых формируется ключевой контейнер, должны выбираться для каждой сети КРК с учетом модели нарушителя и требуемых свойств безопасности, предъявляемых к создаваемым КЗК.

Для того чтобы описать способ, достаточно рассмотреть путь, состоящий из трёх УКС. Пример такого пути приведен на рисунке 18. Целевыми УКС являются узлы «A» и «C», узел «B» является промежуточным. Узлы «A» и «B» имеют общий ключ K_{AB}, узлы «B» и «C» имеют общий ключ K_{BC}.

Рассмотрим доставку общего секрета от узла «A» к узлу «C» на примере использования ключевого контейнера, который формируется согласно рекомендациям ТК-26 [119].

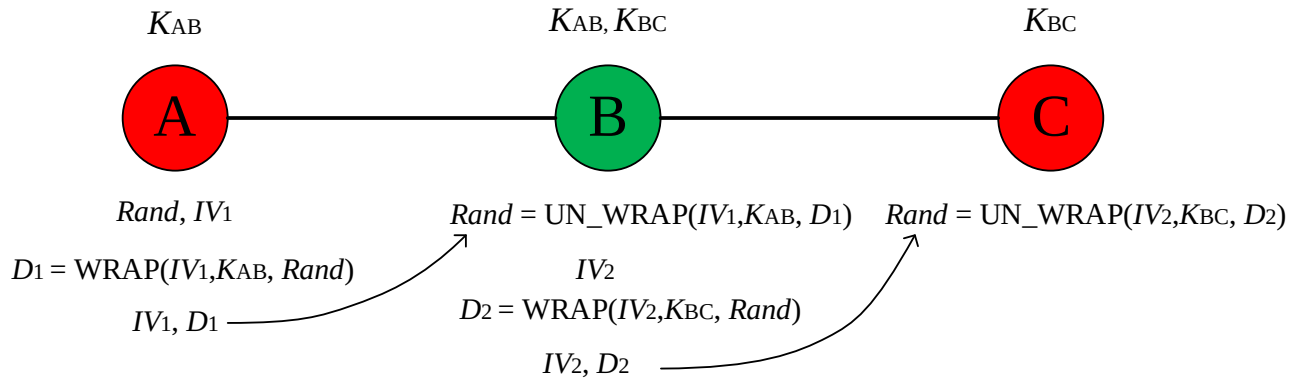


Рисунок 18 – Способ использования ключевого контейнера для передачи общего секрета

На узле «А» генерируется ключевая информация *Rand*, назначаемая общим секретом. На узле «А» формируется IV_1, согласно требованиям функции WRAP. Вычисляется ключевой контейнер $D_1 = WRAP(IV_1, K_{AB}, Rand)$. На узел «В» пересылаются два значения IV_1 и D_1.

На узле «В» осуществляется раскодирование ключевого контейнера D_1 с использованием IV_1 и ключа K_{AB}. В случае успешной проверки имитовставки после раскодирования, значение $Rand$ сохраняется. Для передачи $Rand$ на узел «С» на узле «В» формируется IV_2 и вычисляется $D_2 = WRAP(IV_2, K_{BC}, Rand)$. После этого значения IV_2 и D_2 пересылаются на узел «С». Эти значения могут быть снабжены имитовставкой.

На узле «С» осуществляется раскодирование ключевого контейнера D_2 с использованием IV_2 и ключа K_{BC}. В случае успешной проверки имитовставки, значение Seed считается доставленным.

Примечание – Большинство ключевых контейнеров требуют двух независимых ключей: ключ кодирования и ключ расчета имитовставки. В вычислительной модели стойкости эти ключи могут быть вычислены, как производные ключи из корневого ключа.

Для обеспечения теоретико-информационной стойкости необходимо осуществлять кодирование ключевого материала алгоритмами, стойкими в теоретико-информационном смысле, т.е. одноразовым шифроблокнотом, а аутентичность ключа обеспечивать универсальными хэш-функциями. В таком

случае передаваемая информация $Rand$ кодируется с квантовым ключом сегмента операцией XOR. Имитовставка рассчитывается одной из функций аутентификации, обладающей теоретико-информационной стойкостью (см. п. 2.1). Очевидным минусом такого подхода является одноразовое использование ключей, что означает низкую эксплуатационную характеристику (высокий расход ключей).

Для распределения КЗК допустимы оба варианта, но теоретико-информационный подход требует большого количества ключей. В части передачи общего секрета посредством классических ключей целесообразно использовать ключевые контейнеры, которые имеют вычислительную стойкость, так как тяжело обеспечить нужное количество независимых классических ключей.

Возможен компромиссный подход, при котором конфиденциальность КЗК обеспечивается теоретико-информационно стойкими алгоритмами, а целостность вычислительно стойкими. Кодирование осуществляется одноразовым шифроблокнотом, а целостность обеспечиваться имитовставкой по ГОСТ [100], например, функцией OMAC. Такой подход позволяет сократить количество используемых для формирования контейнера ключей почти в два раза.

Обеспечение теоретико-информационной стойкости при передаче общих секретов целесообразно, если алгоритмы, используемые в протоколе КРК, являются теоретико-информационно стойкими. В противном случае, целесообразно ограничиться вычислительно стойкими алгоритмами.

Положительными сторонами использования ключевого контейнера являются:

– В сочетании с OMAC требуется наличия только блочного шифра без дополнительных примитивов типа хэш-функции и HMAC.
– Допускает многоразовое использование ключей защиты.
– Позволяет создавать высокопроизводительные реализации: быструю запаковку и распаковку ключевого контейнера.
– Распространенный способ передачи ключевого материала, есть множество реализаций в стандартных библиотеках.

– Реализация с блочными шифрами согласно ГОСТ Р 34.12-2018 и имитовставкой согласно ГОСТ Р 34.13-2018 полностью соответствует рекомендациям [4].

Недостатками являются:

– Использование блочного шифра предполагает фиксированный размер блока, что может приводить к частичному раскрытию информации о ключе: накладываемая гамма в режиме гаммирования обладает уникальностью каждого блока, значит, в случае совпадения блоков закодированного текста, можно утверждать, что части ключа не равны между собой.

– Если для кодирования используется шифроблокнот, а имитовставка вычисляется при помощи универсальной хэш-функции, то ключи могут использоваться только один раз, что накладывает дополнительные сложности при реализации способа в части синхронизации.

3.3.2.3 Способ предварительного формирования ключей перекодирования

Данный способ является вариантом решения проблемы появления передаваемой ключевой информации на промежуточных УКС в открытом виде. Для описания способа рассмотрим магистральную сеть КРК из шести УКС, представленную на рисунке 19. В качестве распределяемого КЗК будет выступать случайное число *Rand*, сформированное ДСЧ одного из оконечных УКС.

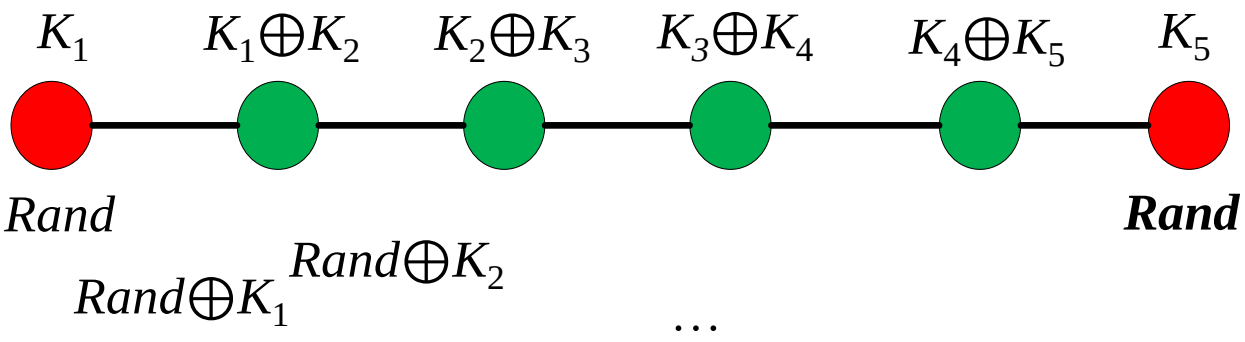


Рисунок 19 – Способ формирования КЗК с предварительным формированием ключей перекодирования

В качестве функции кодирования ключевой информации на сегментах сети КРК используется одноразовый шифроблокнот, т.е. закодированные данные на i-м сегменте сети КРК вычисляются как $C_i = X \oplus K_{i,i+1}$, где X – передаваемая ключевая информация, а $K_{i,i+1}$ – квантовый ключ между i-м и (i+1)-м УКС.

Для предотвращения раскодирования передаваемой ключевой информации предлагается заменить функции раскодирования на одном квантовом ключе и закодирования на другом квантовом ключе на композицию этих функций (17):

$$C_{i+1} = E_{i+1}\big(D_i(C_i)\big) = C_i \oplus K_{i,i+1} \oplus K_{i+1,i+2} = C_i \oplus K_{i,i+2} = E'_{i+1}(C_i). \qquad (17)$$

Для такого преобразования на каждом промежуточном УКС необходимо заранее рассчитать ключ кодирования, представляющий собой сумму по модулю два квантовых ключей соседних сегментов. После этого исходные квантовые ключи удаляются, а на УКС сохраняется только их сумма.

Для добавления свойства симметричности КЗК передачу ключевой информации для данного способа необходимо произвести в два направления, от левого оконечного УКС до правого и наоборот. При этом для каждого направления нужен свой набор квантовых ключей и, соответственно, свои сохраненные суммы квантовых ключей. После доставки двух частей ключевой информации на оба оконечных УКС они объединяются некоторой функцией свертки. Вид и характеристики функции свертки выходят за рамки данного подраздела.

Достоинствами применения данного способа являются:

– теоретико-информационная стойкость защиты при передаче секретов;
– перекодирование передаваемых секретов происходит без их появления в открытом виде на УКС.

Способ обладает эксплуатационным недостатком. В случае сетей КРК с топологией, отличной от топологии «магистраль», существенно вырастает количество квантовых ключей, которые необходимо предварительно выработать квантовой аппаратуре. Так как в случае соединения некоторого УКС с более чем двумя соседними УКС существует C_n^2 способов выбрать пару квантовых каналов

для формирования суммарного ключа перекодирования. Т.е. вместо n квантовых ключей необходимо хранить C_n^2 уникальных пар.

3.3.2.4 Способ распределения КЗК, использующий свойство коммутативности функций кодирования

Данный спсоб призван решить проблему появления передаваемых КЗК на промежуточных УКС в открытом виде.

Для сохранения передаваемой информации в защищенном виде даже внутри одного УКС рассмотрим свойство одноразового шифроблокнота, позволяющее комбинировать операции закодирования и раскодирования на различных ключах в произвольном порядке с сохранением результата итогового преобразования. Данное свойство проиллюстрировано в формуле (18):

$$X = \mathrm{D}_{K1}\big(\mathrm{E}_{K1}(X)\big) = \mathrm{D}_{K2}\big(\mathrm{E}_{K2}(X)\big) = \mathrm{D}_{K1}\Big(\mathrm{D}_{K2}\Big(\mathrm{E}_{K1}\big(\mathrm{E}_{K2}(X)\big)\Big)\Big) = \cdots, \qquad (18)$$

Где D_{Ki} – функция раскодирования на ключе Ki,

E_{Ki} – функция кодирования на ключе Ki,

Кi – используемый ключ кодирования,

X – сообщение.

Соответственно, если сначала выполнять кодирование на ключе следующего сегмента, а потом производить раскодирование на ключе предыдущего сегмента, то в каждый момент времени на промежуточном УКС передаваемая информация всегда находится в защищенном виде, обеспечивается ее конфиденциальность.

Фактически предлагается способ передачи некоторой информации в защищенном виде по цепочке узлов, последовательно соединенных квантовыми каналами связи. Схематичное изображение такой цепочки узлов приведено на рисунке 20.

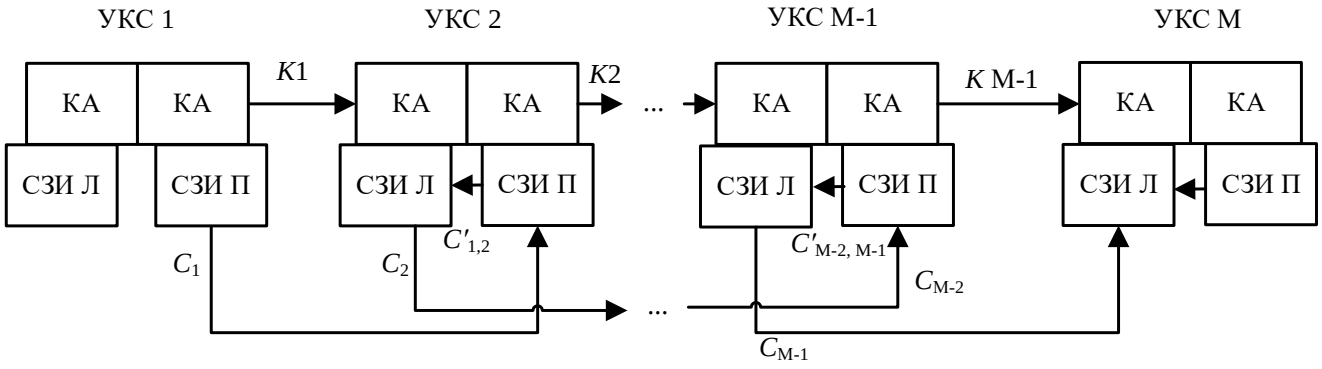


Рисунок 20 – Схема передачи ключа по цепочке УКС

Любой УКС можно рассматривать как комплекс из полукомплектов квантовой аппаратуры (КА) и СЗИ, организующих защищенные классические каналы с соседними УКС с использованием квантовых ключей.

Обратимся к схеме магистральной сети КРК на рисунке 20. Между УКС 1 и УКС 2 передается закодированное сообщение $C_1 = \mathrm{E}_{K1}(X)$. Между УКС 2 и УКС 3 передается закодированное сообщение $C_2 = \mathrm{E}_{K2}(X)$. Из соотношения (18) получим соотношение (19):

$$\mathrm{D}_{K1}\left(\mathrm{E}_{K2}\left(\mathrm{E}_{K1}(X)\right)\right) = \mathrm{E}_{K2}(X), \qquad (19)$$

где D_{Ki} – функция раскодирования на ключе Ki,

E_{Ki} – функция кодирования на ключе Ki,

Ki – используемый ключ кодирования,

X – сообщение.

Модифицируем УКС сети КРК таким образом, чтобы в передаче сообщения X участвовало два СЗИ, обозначенные СЗИ Л и СЗИ П. Тогда закодированное на первом сегменте сообщение C_1 в СЗИ П преобразуется в промежуточный закодированный текст $C'_{1,2} = \mathrm{E}_{K2}(C_1) = \mathrm{E}_{K2}\left(\mathrm{E}_{K1}(X)\right)$. В общем случае $\mathrm{C}' \neq X$.

Затем в результате второго преобразования в СЗИ Л получают для передачи на следующий УКС выходное закодированное сообщение $C_2 = \mathrm{D}_{K_1}\ (C')$. В силу свойства (19) для рассматриваемого алгоритма кодирования $C_2 = \mathrm{E}_{K_2}\ (X)$. Таким образом, передаваемое сообщение X не появляется на УКС в открытом виде.

Отмеченным свойством обладает не только кодирование одноразовым шифроблокнотом, но и некоторые другие алгоритмы, такие как поточный алгоритм кодирования (кроме самосинхронизирующихся поточных алгоритмов), блочный алгоритм кодирования в режиме гаммирования, блочный алгоритм кодирования в режиме связи по выходу (OFB).

На различных участках сети КРК допустимо использовать различные алгоритмы кодирования, удовлетворяющие свойству (18). Выбор алгоритма кодирования для конкретного участка может производиться исходя из скорости генерации квантовых ключей на данном участке, а также требуемой стойкости кодирования. Выбор алгоритма кодирования необходимо производить до начала формирования общего секретного ключа.

На описываемый способ получен патент РФ № 2708511 [53].

3.3.2.5 К вопросу об источнике ключевой информации для КЗК

Базовый способ распределения КЗК использует квантовый ключ некоторого сегмента сети КРК. Нарушитель обладает некоторой, пусть малой, долей информации об этом ключе [10], [18], [120], [121]. При этом квантовая аппаратура в составе УКС обязательно содержит датчик случайных чисел, который может быть использован для формирования ключевой информации (общих секретов).

Отдельно отметим, что тот УКС, который формирует исходный ключевой материал для КЗК, будь то последовательность с датчика случайных чисел или квантовый ключ, имеет возможность навязывать КЗК целевым УКС. Если такой УКС не совпадает ни с одним целевым УКС узлом, то допустимость вероятности такого навязывания необходимо рассматривать при проектировании конкретной сети КРК. Процессы, происходящие в сетях с централизованным управлением, централизованным созданием ключевой информации для КЗК более предсказуемы, но такой центральный узел требует максимальных усилий по его защите и ему должны доверять все участники информационного взаимодействия. При этом любой способ, требующий передачи КЗК по цепочке УКС строго от одного целевого УКС до второго целевого УКС, адаптируется для централизованной сети

КРК путем построения двух цепочек УКС и передачи одного и того же КЗК до целевых УКС от центрального узла.

В случае децентрализованных систем, где затруднительно выделить специальный узел и обеспечить для него высокую степень защиты, целесообразнее формировать ключевую информацию для создания КЗК непосредственно на целевых УКС. Однако, в этом случае, с учетом фактической модели угроз для конкретной сети КРК необходимо предотвращать возможность навязывание КЗК, так как возможность навязывания создает вектор атаки для потенциального нарушителя, если он сможет некоторым образом влиять на данный оконечный узел.

Для решения проблемы навязывания КЗК необходимо использовать симметричные схемы, в которых каждый из двух целевых УКС вносит равный вклад в создание КЗК. Фактически необходимо расширять способ распределения КЗК таким образом, чтобы каждый целевой УКС формировал свою часть ключевой информации, передавал ее второму целевому УКС, после чего они независимо друг от друга объединяли две части ключевой информации для получения требуемого общего секрета. Правильный выбор способа объединения позволит исключить возможность навязывания и/или предсказывания итогового КЗК любым из целевых УКС до непосредственно формирования этого ключа.

3.3.2.6 Способ на основе схемы разделения секрета

В основе предлагаемого способа лежит метод разделения секрета. В данном случае разделяются ключевые системы таким образом, чтобы при полном взломе защиты с применением одной ключевой системы, защита на второй ключевой системе сохранялась и обеспечивала достаточный уровень стойкости формируемых КЗК. В отличие от простого разделения секрета и передачи долей секрета с защитой на разных квантовых ключах в предлагаемом способе повышается безопасность КЗК, так как нарушителю необходимо осуществлять принципиально разные атаки: атаки на квантовую аппаратуру и протоколы КРК, а также атаки на вторую используемую ключевую систему, которая может быть реализована на предварительно распределенных ключах, на постквантовых

алгоритмах или иных принципах, стойких к атакам нарушителя, обладающего квантовым компьютером.

Пример реализации способа проиллюстрирован на рисунке 21.

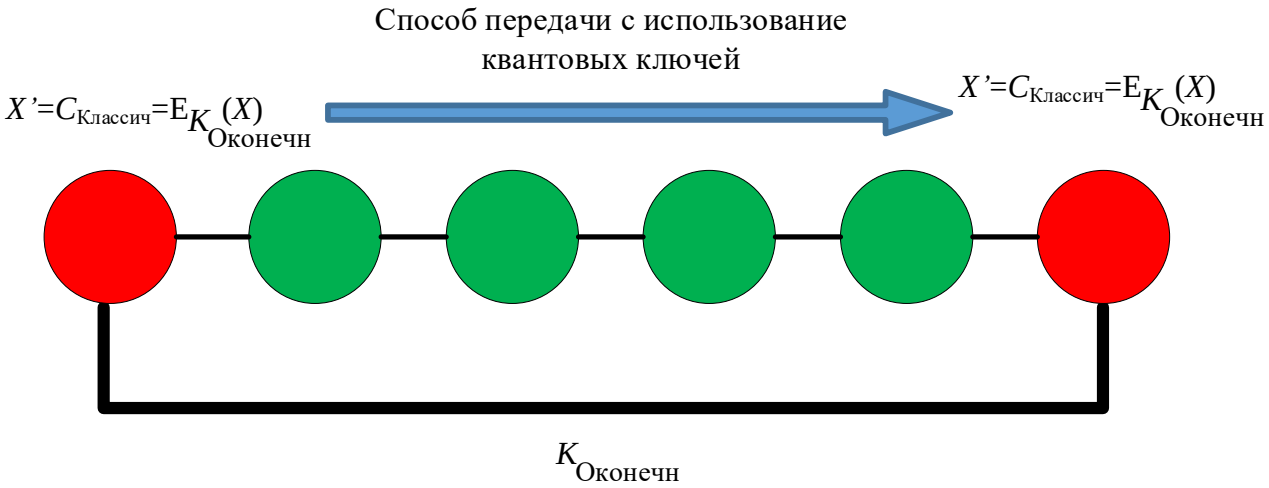


Рисунок 21 – Способ распределения общего секрета с использованием разделения секрета

В сети КРК реализуются две независимые ключевые системы. К описанной ранее ключевой системе, основанной на выработке квантовых ключей, добавляются предварительно распределенные классические ключи $K_{\text{Оконечн}}$ между парой оконечных УКС. Способ рассматривается в допущении, что нарушитель атакует каналы взаимодействия между УКС в том числе с использованием квантового компьютера, а атаки непосредственно на УКС производятся с применением только классических методов. Данное допущение справедливо в силу повышенных организационно-технических мер защиты расположения УКС по сравнению с мерами защиты и контролю доступа к каналам взаимодействия двух УКС.

КЗК формируется из передаваемой ключевой информации, представляющей собой случайную последовательность X заданной длины, полученную с датчика случайных чисел квантовой аппаратуры оконечного узла.

Ключевая информация X на первом оконечном узле защищается с помощью ключа классической ключевой системы. Получаем промежуточный шифртекст $C_{\text{классич}} = E_{K_{\text{оконечн}}}(\text{X})$. Этот промежуточный закодированный текст используется в качестве передаваемой ключевой информации для способов, описанных выше для

ключевой системы, основанной на квантовых ключах. Таким образом, даже в случае необходимости перекодирование передаваемой ключевой информации на промежуточных УКС, в открытом виде на них появится промежуточный закодированный текст $C_{\text{классич}}$. Оконечный УКС, обладая секретными ключами обеих ключевых систем, способен раскодировать полученный закодированный текст и получить переданную ключевую информацию X.

В случае успешного взлома квантовой аппаратуры и компрометации квантовых ключей рассматриваемой магистральной сети КРК, передаваемые КЗК остаются защищенными на классических ключах. В случае компрометации классической ключевой системы, нарушитель не получит доступа к передаваемым между УКС закодированным текстам, так как они защищены на квантовых ключах. Следовательно, чтобы провести успешную атаку на передаваемую ключевую информацию необходимо провести успешную атаку на обе ключевые системы.

Достоинствами применения способа с разделением ключевых систем в таком виде являются:

– сохранение стойкости передаваемых КЗК в случае компрометации одной из ключевых систем, но не двух сразу;
– защита передаваемых КЗК от раскодирования на промежуточных УКС;
– возможность использования стандартизованных ключевых контейнеров, соответствующих рекомендациям [4].

Недостатки способа на основе схемы разделения секрета:

– повышается сложность реализации за счет использования двух ключевых систем;
– требуется бóльшее количество ключевого материала.

Важно заметить, что применение вложенной схемы требует подробных исследований стойкости для конкретной реализации сети КРК для случая компрометации внутреннего (классического) ключа защиты, а также контроля нагрузки на внешний и внутренний ключи, чтобы показать невозможность компрометации передаваемой ключевой информации. В то же время схема разделения на независимые ключевые подсистемы может быть выполнена путем

передачи разных частей КЗК, например, полученных так же некоторой схемой разделения секрета, полностью на ключах разных подсистем с последующим финальным смешиванием уже на целевых УКС. Тогда даже компрометации одной ключевой подсистемы, в том числе получения доступа к некоторому промежуточному УКС в части ключей одной подсистемы, не дает нарушителю никакой информации о части КЗК, передаваемой под защитой ключей другой ключевой подсистемы.

3.4 Классификация способов распределения общего секретного ключа

В предыдущем разделе были разработаны способы, позволяющие устранить выявленные недостатки при распределении КЗК по базовому способу. Существует множество путей решения выявленных научных проблем, что порождает различные способы. В целях анализа будущих способов решения задачи распределения общего секрета на целевые УКС целесообразно сформировать подходы классификации таких способов.

В качестве критериев классификации предлагается рассматривать следующие группы критериев [46]:

– критерии, относящиеся к конструктивным особенностям, предъявляемым к системе;
– критерии, относящиеся к эксплуатационным свойствам способа;
– критерии, относящиеся к свойствам безопасности, достигаемым при применении способа.

К критериям, касающихся конструктивных особенностей, относятся те аспекты применения способа, которые влияют на его входные параметры. Для способов распределения общего секрета, заключающихся в его передаче по УКС, к таким критериям относятся:

– источник формирования ключевого материала и требуемый объем ключевого материала;

– требования к структуре УКС или организационно-технические меры защиты, предъявляемые к УКС;

Эксплуатационные критерии для способов распределения общего секрета:

– количество требуемых преобразований (в элементарных операциях, нормированных по числу узлов в цепочке УКС);
– скорость формирования КЗК;
– величина дополнительных данных, необходимых для формирования КЗК;
– возможность и степень распараллеливания выполнения способа.

Количественно эта группа критериев может быть рассчитана для конкретных систем КРК исходя из их конструктивных особенностей и принятых принципиальных технологических и конструктивных решений, однако качественное сравнение возможно на этапе теоретического анализа способов.

Критерии, относящиеся к свойствам безопасности, в рамках настоящего исследования интересны в контексте недостатков, выявленных по результатам анализа известных решений в п. 1.2. Поэтому, в последней группе критериев будем рассматривать:

– класс используемых примитивов, на базе которого построен способ;
– требования доверия к промежуточным УКС;
– обеспечение основных свойств безопасности КЗК (конфиденциальности, целостности, аутентичности);
– возможность навязывания итогового КЗК нечестным УКС (подверженным действиям нарушителя);
– стойкость итогового КЗК.

В таблице 2 приводится классификация известных и разработанных способов по приведенным критериям. Эксплуатационные критерии указаны качественно.

Таблица 2 – Классификация способов формирования общего ключа целевых УКС

Способы	**Источник ключевой информации**	**Способ передачи ключевой информации**	**Класс используемых примитивов**	**Требование доверия к УКС**	**Эксплуатационные особенности**
Базовый способ (п. 1.2)	Первый УКС цепочки (квантовый ключ)	Последовательный от первого к последнему (УКС)	Теоретико-информационно стойкие	Максимальное	Постоянный объем передаваемых данных для любой длины цепочки УКС
Способ «матрешки» (п. 1.2)	Первый УКС цепочки (квантовый ключ)	Последовательный от первого к последнему (УКС)	Вычислительно-стойкие	Среднее	Значительное увеличение объема передаваемых данных пропорционально длине цепочки УКС
Способ одновременной доставки (п. 3.3.2.1)	Произвольный УКС цепочки (квантовый ключ)	Параллельный от источника до целевых УКС	Теоретико-информационно стойкие	Максимальное	Постоянный объем передаваемых данных для любой длины цепочки УКС
Способ передачи в контейнере (п. 3.3.2.2)	Первый УКС (ключевой материал с ДСЧ УКС)	Последовательный от первого к последнему (УКС)	Зависит от выбранного контейнера	Максимальное	Постоянный увеличенный объем данных для любой цепочки УКС (увеличение за счет доп. информации для формирования контейнера)
Способ предварительного преобразования ключей защиты (п. 3.3.2.3)	Первый УКС (ключевой материал с ДСЧ УКС)	Последовательный от первого к последнему (УКС)	Теоретико-информационно стойкие	Среднее	Повышенный объем хранимых ключей защиты на УКС
Способ с применением специальных свойств преобразований (п. 3.3.2.4)	Первый УКС (ключевой материал с ДСЧ УКС)	Последовательный от первого к последнему (УКС)	Зависит от выбранной функции, удовлетворяющей свойству (18)	Низкое	Специальная структура УКС для повышения защищенности КЗК на промежуточных УКС
Способ разделения секрета (п. 3.3.2.6)	Первый УКС (ключевой материал с ДСЧ УКС)	Последовательный от первого к последнему (УКС)	Зависит от выбранного способа передачи частей КЗК	Низкое	Повышенный объем ключей защиты. В совокупности с способом разделения секрета по п. 1.2 увеличение числа цепочек УКС при повышении защищенности итогового КЗК

Из таблицы видно, что способы, предъявляющие меньше требований к используемым примитивам, не предоставляют защиты передаваемых КЗК непосредственно на УКС и требуют повышенного доверия к УКС, что на практике приводит к реализации дополнительных организационно-технических мер защиты

и особых правил размещения и/или эксплуатации УКС. Если способ обеспечивает защиту передаваемых КЗК в том числе и при обработке на УКС, то появляются дополнительные ограничения к допустимым примитивам и ухудшаются эксплуатационные характеристики способа.

Способы распределения общего секрета различаются по небольшому количеству критериев. Объединение разных способов, затрагивающих разные критерии и отличающихся в разных конструктивных особенностях, позволит синтезировать подходящий для каждой конкретной сети КРК способ распределения КЗК, характеризующийся установленными в конкретном случае параметрами безопасности для сети КРК и обладающий приемлемыми эксплуатационными характеристиками.

3.5 Методика распределения КЗК на пары узлов сети КРК магистральной топологии

В предыдущих разделах были разработаны способы распределения КЗК для двух целевых УКС, с указанием преимуществ и недостатков каждого способа. В данном подразделе будет синтезирована методика, сочетающий основные выявленные преимущества разных способов.

Зафиксируем свойства КЗК, которые требуется достичь при его формировании.

– Ни один из участников формирования КЗК не должен иметь возможность предсказать его значение до начала распределения КЗК.
– Компрометация только квантовых ключей не приводит к компрометации КЗК.
– Компрометация только вспомогательных классических ключей не приводит к компрометации КЗК.
– Промежуточные УКС не могут восстановить КЗК только с использованием передаваемой через них информации.

Для выполнения данных свойств объединим следующие способы распределения КЗК.

– В формировании ключевой информации, из которой вычисляется КЗК, участвуют оба целевых УКС в равной степени, способ симметричный.
– Каждый из пары целевых УКС формирует две составные части КЗК. Одна передается строго с использованием квантовых ключей по цепочке соседних УКС. Вторая передается строго второму целевому УКС с использование классических ключей, не содержащих квантовой энтропии. Такое разделение на основе способа с разделением секрета позволяет достичь свойства стойкости КЗК при компрометации ключей защиты одного из типов.
– При передаче частей КЗК применяется способ передачи в ключевом контейнере на соответствующих ключах защиты.

Графическое изображение методики в нотации IDEF0 приведено на рисунке 22.

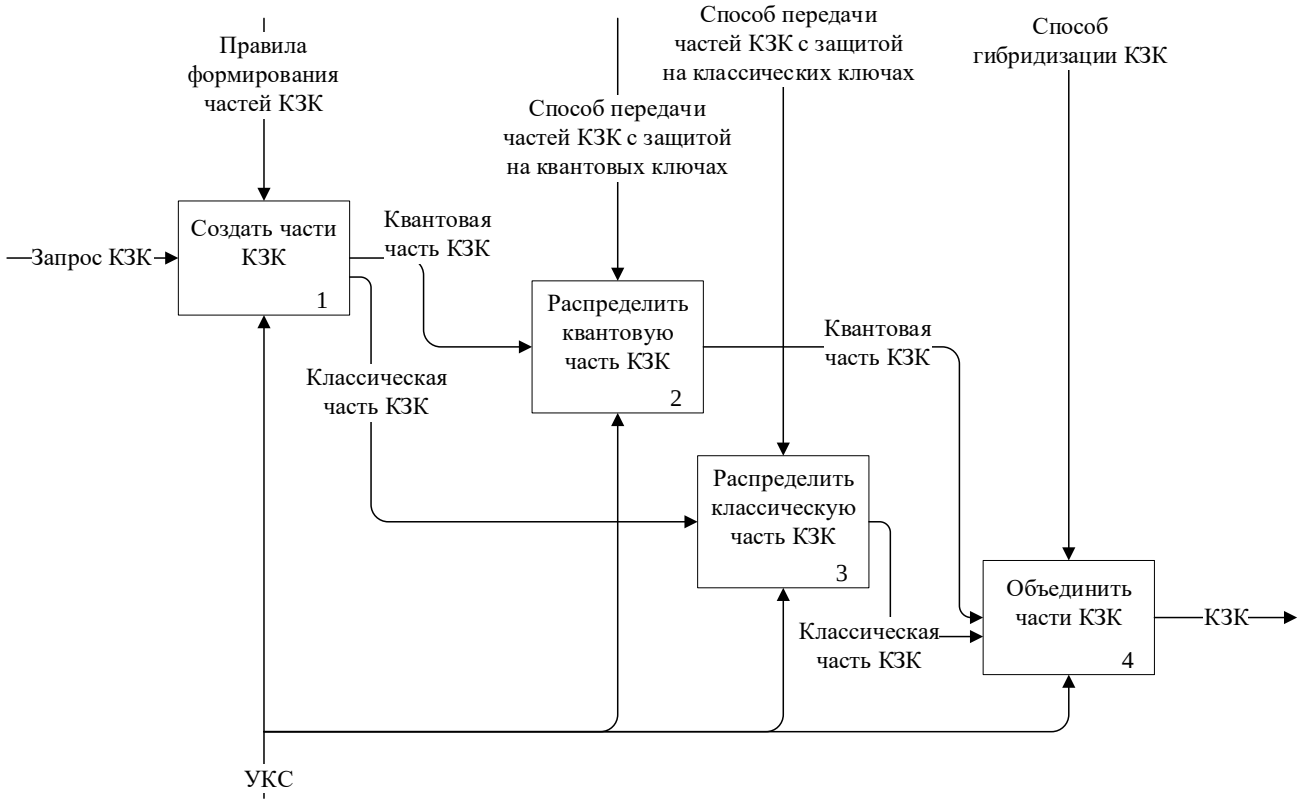


Рисунок 22 – Методика распределения КЗК

Методика распределения КЗК на магистральной линии из *N* УКС, целевыми из которых являются УКС 1 и УКС N, состоит в следующем.

Для распределения КЗК должны быть выполнены предусловия.

1) Между всеми парами соседних УКС в цепочке от УКС 1 до УКС N создано достаточное количество квантовых ключей. Достаточность определяется выбранными алгоритмами формирования ключевых контейнеров.
2) На УКС 1 и УКС N загружен классический мастер-ключ или достаточное количество классических ключей для осуществления предлагаемого способа (далее ключей защиты КЗК).

Непосредственно методика распределения КЗК заключается в следующем.

1) Два целевых УКС формируют каждый по две части КЗК. Назовем их $Rand_{1,N}$ и $QRand_{1,N}$ для частей, формируемых УКС 1 в адрес УКС N и $Rand_{N,1}$ и $QRand_{N,1}$ для частей, формируемых УКС N в адрес УКС 1, соответственно. Части КЗК должны являться ключевой информацией, соответствующей требованиям к ключевой информации [4].
2) УКС 1 передает часть КЗК $Rand_{1,N}$ с защитой на ключе защиты КЗК в адрес УКС N. УКС N передает часть КЗК $Rand_{N,1}$ с защитой на ключе защиты КЗК в адрес УКС 1. Передача осуществляется защищенным образом в ключевом контейнере с обеспечением конфиденциальности и целостности передаваемой ключевой информации, а также с обеспечением целостности необходимых атрибутов этой ключевой информации, таких как идентификаторы целевых УКС, для которых создана ключевая информация; вектор инициализации, требуемый в алгоритме защиты; идентификационная информация ключевой информации и др. Защиту передачи ключевой информации целесообразно выполнять за счет передачи ее в экспортном представлении, например, с использованием ключевого контейнера, согласно рекомендациям по стандартизации [119].

3) УКС 1 передает часть КЗК $QRand_{1,N}$ с последовательным перекодированием по цепочке УКС с защитой на квантовых ключах соответствующих сегментов магистральной подсети КРК. Требования к защите передаваемой ключевой информации аналогичны шагу 2 описываемой методики. Заметим, что применение квантовых ключей в качестве ключей кодирования для алгоритма экспорта ключа согласно [119] и применение предварительно распределенных классических ключей между двумя целевыми УКС для обеспечения сквозной целостности передаваемой ключевой информации позволяет применять способ передачи, описанный в п. 3.3.2.4. Передача части КЗК $QRand_{N,1}$ от УКС N до УКС 1 производится аналогично.
4) УКС 1 и УКС N получают полный комплект частей КЗК, который смешивают в КЗК с помощью некоторой функции. Назовем ее функцией гибридизации.

В качестве функции гибридизации возможно рассмотреть функцию выработки производных ключей согласно рекомендациям по стандартизации [122], которая использует ключевую информацию и случайную соль для формирования производных ключей. На каждом целевом УКС имеется ключевой материал для формирования КЗК. Необходимо определить, какую часть ключевого материала считать солью для функции выработки производного ключа, а какую ключевой информацией. С точки зрения создания частей КЗК они являются равноценными, поэтому в конкретной системе ключевой информацией целесообразно положить ту часть КЗК, которая передавалась на более защищенных ключах (классических или квантовых), что определяется множеством факторов, таких как частота использования ключей защиты, реализация УКС, в том числе применяемые алгоритмические и организационно-технические меры защиты УКС как в части выработки квантовых ключей, так и в части функционирования УКС как классического СЗИ. Подробный анализ реализованных мер защиты необходимо проводить для конкретной системы, поэтому он находится за рамками данной

работы. Необходимость гибридизации и сравнение способов выработки гибридных ключей подробно рассмотрены в работе [49].

Для невозможности предсказания результирующего КЗК каждым УКС до получения частей КЗК от второго целевого УКС каждый тип частей КЗК до использования в функции гибридизации необходимо объединять с помощью хорошей функции хэширования, например, согласно ГОСТ 34.11-18 [65]. Т.е., например, ключевая информация для функции гибридизации вычисляется как $\mathrm{Hash}_{256}(QRand_{1,N}||QRand_{N,1})$, случайная соль как $\mathrm{Hash}_{256}(Rand_{1,N}||Rand_{N,1})$, где Hash_{256} –функция хэширования с длиной выхода 256 бит.

Предложенная методика позволяет для конкретной системы варьировать скорость расходования ключей защиты (квантовых и классических) за счет однократного или многократного использования ключей защиты для соответствующих частей КЗК при формировании ключевых контейнеров. Более того, предлагаемая функция гибридизации позволяет создавать несколько КЗК из одного комплекта частей КЗК. Допустимые предельные значения числа создаваемых КЗК должны определяться в рамках тематических исследований для конкретной системы. Также при достаточной обоснованности для конкретной системы можно отказаться от классических частей КЗК, а следовательно, от необходимости распределять предварительные классические ключи между парами целевых УКС, что позволяет реализовать предлагаемую методику с примитивами, обладающими теоретико-информационной стойкостью.

Предложенная методика положена в основу проекта методических рекомендаций ТК 26 «Информационная технология. Криптографическая защита информации. Ключевая система полносвязной многоарендаторной сети шифрованной связи на базе ККС ВРК с ДПУ» [123].

3.6 Выводы по главе

В данной главе рассмотрена научная проблема распределения общего секрета для сетей КРК простых топологий «магистраль» и «звезда». В качестве

базового конструктива для сетей КРК, называемого сегментом сети КРК, полагается комплекс устройств из двух экземпляров квантовой аппаратуры и двух СЗИ, описанный в главе 2.

Введен термин квантовозащищенный ключ (КЗК) для описания объекта, распределяемого между двумя целевыми УКС, не соединенных напрямую квантовым каналом.

Проанализированы возможные свойства КЗК, а также разработаны подходы решения недостатков базового способа распределения КЗК, обладающие различными свойствами безопасности и эксплуатационными характеристиками, позволяющие достичь выполнения некоторых из возможных свойств КЗК.

Базовый способ предлагает решение конфиденциальности передачи ключевой информации. В п. 3.3.2.2 проводится обобщение способа защиты передачи общего секрета путем формирования ключевого контейнера, обеспечивающего конфиденциальность и целостность передаваемого секрета.

Проблема появления ключевой информации на промежуточных УКС решается за счет предварительного преобразования ключей защиты (см. п. 3.3.2.3), использования свойств коммутативности применяемых функций при защите передачи ключевой информации (см. п. 3.3.2.4), а также применения метода разделения секрета на уровне разделения ключевых систем, используемых для защиты при передаче общих секретов (см. п. 3.3.2.6).

Дополнительно проведено обобщение источника ключевой информации, позволяющее использовать не только квантовые ключи некоторого сегмента сети КРК, но и последовательность с ДСЧ из состава УКС сети КРК, для формирования КЗК (см. п. 3.3.2.5).

Описанные способы были представлены в докладах на конференциях QCrypt-2019 [50], QCrypt-2020 [51]. Материалы докладов справочно приведены в приложении А.

Предлагаются критерии классификации способов распределения КЗК, разделенные на группы конструктивных критериев, критериев свойств безопасности распределенного КЗК и эксплуатационных критериев.

Предложенные группы критериев позволят проводить сравнительный анализ существующих и вновь разрабатываемых методов, а также способов, синтезированных на их основе.

В этой главе синтезирована методика распределения КЗК в магистральной сети КРК на основе разработанных способов формирования КЗК. Синтезированная методика устраняет недостатки базового способа распределения КЗК. Методика положена в основу разрабатываемого проекта методических рекомендаций ТК 26 «Информационная технология. Криптографическая защита информации. Ключевая система полносвязной многоарендаторной сети шифрованной связи на базе ККС ВРК с ДПУ» [123].

Применение указанной методики позволило повысить безопасность системы на базе изделия «Квазар-СКР» за счет гибридизации КЗК из двух компонент, переданных по независимым каналам связи, улучшить протяженность транспортного канала изделия пропорционально количеству сопряженных с ним пар узлов квантовой сети и сократить на 50% время ожидания изделием одной из компонент КЗК при реализации способа распределения КЗК на основе коммутативных функций.

4 МЕТОДИКА ПОСТРОЕНИЯ СЕТИ КРК СМЕШАННОЙ ТОПОЛОГИИ

В этой главе содержатся рекомендации по решению практических задач по построению сетей КРК смешанной топологии на основе разработанной методики распределения общих секретов целевых УКС и способа доставки этих секретов в пользовательские устройства. Методика, разработанная в предыдущей главе, является заделом для построения сети КРК смешанной топологии. Однако, простого объединения сегментов типа «точка-точка» (см. главу 2) оказывается недостаточно. Распределение КЗК для сложных топологий основывается на принципах и методике, разработанной в главе 3.

Разработка методики построения сетей КРК смешанной топологии, включая требования к структуре такой сети и способу ее функционирования, проводится на основе анализа результатов работ международных организаций, посвященных применению технологии КРК (см. п. 1.2).

4.1 Разработка требований к структуре сети КРК

В п. 1.2 проанализированы два наиболее проработанных варианта структуры сетей КРК. В данном разделе проводится разработка требований к структуре сети КРК, учитывающих выявленные недостатки проектов европейских сетей.

Сеть КРК описывается в уровневой модели. Уровневая модель позволяет разбить сложную систему на простые элементы с ограниченным, строго определенным функционалом, что способствует полному и понятному описанию системы, а также возможности независимой разработки частей системы различными производителями. По опыту построения классических сетей будем проектировать сеть КРК из расчета, чтобы нижние уровни сети предоставляли ресурс, которым будут пользоваться вышестоящие уровни. Такой принцип заложен, например, в сетевой модели ISO/OSI [124].

В процессе анализа проектов зарубежных сетей КРК и квантовой аппаратуры, реализующей протоколы КРК, было выявлено следующее.

1) Квантовые ключи, производимые квантовой аппаратурой, являются случайной последовательностью нефиксированной длины, причем различной длины от сеанса к сеансу выработки квантовых ключей. Необходимо обеспечивать формирование квантовых ключей из случайной последовательности, учитывая возможность случайных или преднамеренных сбоев при формировании, хранении и передаче квантовых ключей.
2) Сеть КРК предоставляет парам СЗИ квантовозащищенные ключи. Такие ключи распределяются на некоторой цепочке УКС, которую можно считать подсетью магистральной топологии. Необходим способ определения такой цепочки, а также способ распределения квантовозащищенного ключа на рассчитанной цепочке.
3) Управление процессом выработки квантовых и квантовозащищенных ключей можно производить локально или удаленно, централизованно или децентрализовано. Необходимо определить способ управления.
4) Взаимная аутентификация УКС и их составных частей, а также взаимодействия с внешними СЗИ требует дополнительной проработки. Привычные способы построения больших классических сетей не применимы в силу невозможности использования методов генерации общего ключа и аутентификации узлов, основанных на вычислительно сложных математических задачах.

Централизованная система управления и контроля сети КРК менее надежна, чем децентрализованное управление. Подобный центр управления является точкой отказа всей сети. Напротив, если функции управления распределены по УКС, то выход из строя одного УКС прерывает работу не всей сети, а только некоторого ее сегмента.

Анализ проектов сетей КРК, а также потенциальных потребителей технологии [42], [125] показывает, что внешние СЗИ необходимо подключать не ко

всем УКС. В сети КРК возникнут промежуточные УКС, выполняющие только роль увеличения длины квантового канала, а не источника ключей для внешних потребителей. Следовательно, целесообразно выделить непостоянную часть УКС, отвечающую за взаимодействие с внешним СЗИ-потребителем в отдельный слой сети. В результате некоторые УКС могут иметь упрощенную структуру с отсутствующей функцией выдачи КЗК.

Предлагается трехуровневое деление сети КРК, включающее уровень выработки квантовых ключей, уровень выработки квантовозащищенных ключей и уровень управления квантовозащищенными ключами (уровень взаимодействия с внешним потребителем). Дополнительно для дальнейших пояснений введем уровень потребителей, представленный парами СЗИ-потребителей, в том числе не объединенных в единую сеть. Уровень потребителей является внешним по отношению к сети КРК. В зарубежных источниках он часто именуется уровнем приложений.

Можем представить сеть КРК в виде совокупности уровней сети, как показано на рисунке 23.

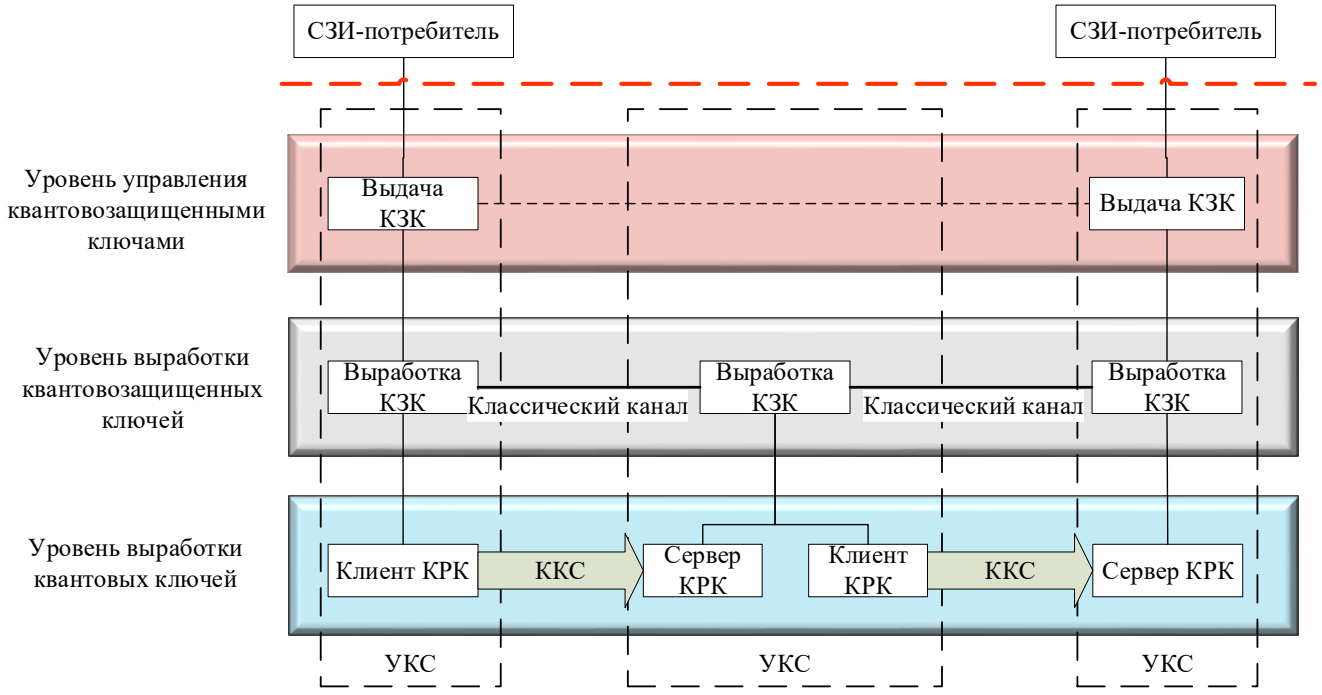


Рисунок 23 – Структура сети КРК (по уровням)

При введении трехуровнего деления сети КРК появляются три интерфейса взаимодействия между уровнями:

– интерфейс между квантовой аппаратурой и управляющим СЗИ (уровнем выработки КЗК) – интерфейс передачи квантовых ключей;
– внутренний интерфейс узла сети КРК между уровнем выработки КЗК и уровнем управления КЗК – интерфейс доверенного узла;
– интерфейс между Сетью КРК и Потребителем – интерфейс с сетью КРК.

На рисунке 24 представлены интерфейсы взаимодействия между различными уровнями сети.

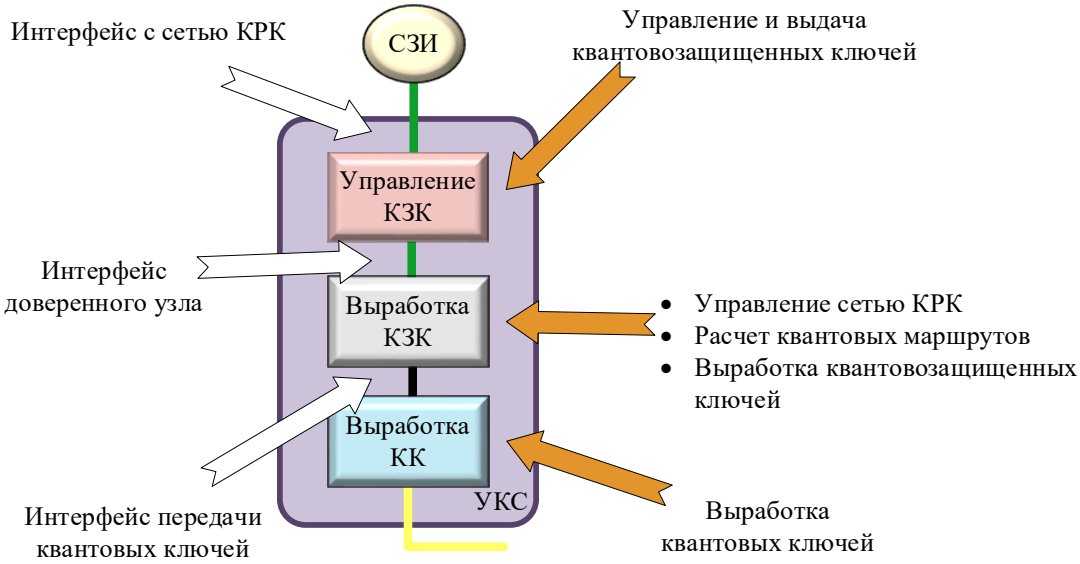


Рисунок 24 – Интерфейсы УКС

Стоит отметить, что уровень выработки квантовозащищенных ключей сам по себе является СЗИ, так как осуществляет выработку и хранение ключевой информации, а также ее использование для обеспечения конфиденциальности, целостности и аутентичности данных в сети КРК.

Квантовая аппаратура, непосредственно вырабатывающая квантовые ключи, может быть реализована различными производителями, основана на разных протоколах КРК, но для предлагаемой сети КРК такая вариативность не должна иметь значения. Сеть КРК целиком должна работать независимо от конкретной реализации пар квантовой аппаратуры. Таким образом, интерфейс взаимодействия

между квантовой аппаратурой и СЗИ является базовым для реализации любой сети КРК. Для подобной взаимозаменяемости необходима проработка стандарта взаимодействия между квантовой аппаратурой и внешним оборудованием. Такая работа в настоящее время ведется в рабочей группе ТК26 [126]. Утверждены методические рекомендации ТК26 «Защищенный протокол взаимодействия квантово-криптографической аппаратуры выработки и распределения ключей и средства криптографической защиты информации».

Интерфейс внутреннего взаимодействия УКС между уровнем выработки и уровнем управления квантовозащищенными ключами – это интерфейс между неразрывно связанными частями УКС. Целью этого интерфейса является ограничение доступа из внешней сети к внутренним процессам сети КРК. Необходим контроль за реализованным функционалом данного интерфейса. При этом в отличие от двух других интерфейсов, которые соединяют объекты, потенциально способные работать независимо друг от друга и изготавливаемые различными производителями, данный интерфейс не требует проработки стандартизованного взаимодействия между модулями двух уровней.

Последний интерфейс – интерфейс связи с конечным потребителем. Как и интерфейс с квантовой аппаратурой, он требует разработки стандарта взаимодействия, так как реализует взаимодействие объектов множества разных производителей. А с точки зрения потребителя должна осуществляться поддержка произвольной сети КРК.

4.1.1 Требования к уровню потребителей

Уровень потребителей состоит из СЗИ, которые имеют функцию получения КЗК от сети КРК. Важной особенностью сети КРК является то, что каждый потребитель должен иметь возможность подключаться к любому УКС, имеющему в составе модуль уровня управления квантовозащищенными ключами.

СЗИ-потребители связаны с другими СЗИ-потребителями независимо от сети КРК. Потребителям необходимо осуществлять защищенную передачу данных согласно этим связям.

Примечание – Два СЗИ-потребителя могут подключаться как к разным узлам сети КРК, так и к одному узлу сети КРК.

Цель СЗИ-потребителя при взаимодействии с сетью КРК – получить КЗК для взаимодействия с другим сопряженным с ним СЗИ-потребителем. При этом СЗИ-потребитель должен знать идентификационную информацию сопряженного СЗИ-потребителя и может не знать, к какому узлу сети КРК подключен его сопряженный СЗИ-потребитель.

Возможны различные варианты контроля легитимности запросов КЗК от СЗИ-потребителей:

– на уровне потребителей – СЗИ-потребители самостоятельно определяют с кем могут связываться, а сеть КРК выполняет запросы без проверки легитимности запроса;
– на уровне сети КРК – потребитель запрашивает КЗК, а сеть КРК самостоятельно проверяет, имеет ли такие права потребитель.

Целесообразно осуществлять проверку легитимности запроса на уровне сети КРК, что позволит предотвратить компрометацию передаваемых общих секретов при получении нарушителем доступа к одному из СЗИ-потребителей.

Отметим, что СЗИ-потребитель может быть как стационарным, т.е. постоянно подключенным к сети КРК, так и мобильным, т.е. способным легко менять узел сети КРК, к которому он подключен в данный момент. Поэтому необходимо закладывать возможность смены узла привязки СЗИ к сети.

4.1.2 Требования к уровню выработки квантовых ключей

Данный уровень представляет собой попарно соединенные модули квантовой аппаратуры. На концах одного сегмента обязательно находится аппаратура одного производителя (по крайней мере до тех пор, пока не будут унифицированы протоколы КРК, а также используемые оптические схемы).

Возможны несколько подходов к функционированию данного уровня в части управления квантовыми каналами, а также взаимной идентификации модулей уровня в сети КРК. Одним из вариантов является условно самостоятельная

квантовая аппаратура, самостоятельно организующая аутентифицированный канал, включая адресацию при передаче данных между экземплярами квантовой аппаратуры, и самостоятельно управляющая квантовыми каналами, в том числе их переключение. Уровень выработки квантовых ключей в этом случае должен рассчитывать объем запросов на квантовые ключи, определять допустимую частоту запросов, исходя из собственных возможностей (согласно используемому протоколу КРК, качеству и длине квантового канала и пр.), а также осуществлять согласованное переключение квантовых каналов в соответствии с совокупностью запросов квантовых ключей. В результате такой подход существенно усложняет работу «физического» уровня сети КРК.

Выработанный на этом уровне квантовый ключ предается для дальнейшего использования на следующий уровень – уровень выработки квантовозащищенных ключей.

Второй подход к управлению квантовыми каналами предполагает, что управление переключением каналов выносится на следующий уровень сети КРК. Модули уровня выработки квантовых ключей работают попарно. Вопрос построения квантового канала в таком случае не является задачей уровня выработки квантовых ключей, а переносится на уровень выработки квантовозащищенных ключей. Фактически управление квантовым каналом неразрывно связано с запросами квантовых ключей, которые формирует уровень выработки квантовозащищенных ключей. Квантовая аппаратура работает строго в топологии точка-точка, следовательно, ей не важно каким способом и каким оборудованием был предоставлен квантовый канал. В свою очередь вышестоящий уровень фактически оркестрирует запросы квантовых ключей и вместе с запросом предоставляет условия для его успешного выполнения. Оптический коммутатор, как описано в разделе 3.2, управляется из центра подсети топологии «звезда».

Примечание – Природа квантового протокола обеспечивает синхронное получение квантовых ключей на обеих сторонах квантового канала (либо одновременно есть ключ с двух сторон, либо нет). Невозможна ситуация, когда с одной стороны квантовый ключ получен, а с другой нет.

При передаче квантовых ключей на вышестоящий уровень необходимо осуществлять формирование ключей из случайной последовательности, назначение идентификаторов ключей и прочей метаинформации, а также контроль идентичности ключей перед помещением в хранилище. Взаимодействие в части передачи ключей осуществляется согласно способу по п. 2.2.

В сети КРК предлагается хранение квантовых ключей на вышестоящем уровне, который использует квантовые ключи в качестве ресурса для выполнения своих функций.

Модули выработки квантовых ключей имеют связи по квантовому каналу и по классическому каналу. Классический канал целесообразнее реализовывать с транспортом через модули верхнего уровня для упрощения адресации данных в сети КРК согласно способу по п. 2.2.

4.1.3 Требования к уровню выработки квантовозащищенных ключей

Второй уровень сети КРК оказывается наиболее нагруженным в части выполняемых функций. В дальнейшем развитии сетей КРК может быть проведено выделение дополнительных уровней при расширении вспомогательного функционала, такого как, например, расчет и прогнозирование ожидаемой нагрузки на сегменты сети КРК в течение некоторого периода времени вследствие неоднородности запросов ключей от СЗИ-потребителей.

На уровне выработки квантовозащищенных ключей происходят два независимых крупных процесса: управление выработкой квантовых ключей и непосредственно выработка квантовозащищенных ключей.

Модуль уровня выработки квантовозащищенных ключей отвечает за формирование запросов на квантовые ключи и обеспечение классического канала между соседними узлами сети КРК, если это необходимо. Необходимость возникает при подключении множества экземпляров квантовой аппаратуры соседних УКС к экземпляру квантовой аппаратуры некоторого узла с разделением по времени. Квантовая аппаратура может иметь собственный классический канал, однако целесообразнее уменьшить число модулей, отвечающих за сетевое межузловое взаимодействие, т.е. предоставить связь для модулей уровня

выработки квантовых ключей через модули уровня выработки КЗК. Канал строится между модулями выработки КЗК и пробрасывает (проксирует) данные квантовой аппаратуры, возможно дополнительно с аутентификацией, если аппаратура КРК не способна выполнять ее самостоятельно.

После выработки квантовых ключей и передачи их в модули выработки квантовозащищенных ключей необходимо обеспечить хранение полученных ключей с присвоением необходимых метаданных, включая метку времени создания квантового ключа, идентификационную информацию сегмента сети КРК на котором был создан ключ, длину и идентификатор самого ключа. Рекомендуется, чтобы интерфейс передачи квантовых ключей на уровень выработки КЗК поддерживал контроль синхронной выдачи квантовых ключей на двух концах квантового канала.

При перемещении квантовых ключей в хранилище квантовых ключей, находящееся на рассматриваемом уровне, в зависимости от используемого способа распределения КЗК, необходимо оперативно обновлять характеристики сегмента сети КРК (метрики сегмента), используемые при расчете цепочки УКС между целевыми УКС сегмента сети, для которого создан новый квантовый ключ. Удаление квантового ключа из хранилища влечет за собой обновление метрик сегмента сети, сообщать о которых даже важнее для обеспечения корректного выбора цепочки УКС при распределении КЗК.

Дополнительно уровень выработки КЗК должен обеспечивать управление сопутствующим оборудованием УКС для нормального функционирования уровня выработки квантовых ключей, таким как оптические коммутаторы, используемые для организации множества квантовых каналов.

Следующий процесс, происходящий на рассматриваемом уровне, – это обработка запросов от вышестоящего уровня управления квантовозащищенными ключами. По получению запроса с указанием целевого УКС, модуль выработки квантовозащищенных ключей должен определить и зарезервировать цепочку УКС, по которой будут формироваться КЗК между текущим и целевым УКС, т.е. цепочку УКС, последовательно соединенных квантовыми каналами. Цепочка определяется

на основе метрик сегментов сети, включающих в том числе количество имеющихся квантовых ключей в хранилище квантовых ключей, скорость выработки квантовых ключей на сегменте, скорость расходования квантовых ключей (или число зарезервированных квантовых ключей прочими маршрутами). Необходимо резервировать маршрут для предотвращения использования ресурса квантовых ключей другими цепочками, которые могут пытаться зарезервировать сегмент данной цепочки (зарезервировать ресурс квантовых ключей) уже после начала распределения КЗК на ней. Подробный способ определения цепочки вынесен за рамки данной работы. После определения цепочки осуществляется непосредственно распределение КЗК способом по п. 3.5, в результате которого расходуется ресурс квантовых ключей на цепочке УКС, а между целевыми УКС распределяется КЗК. Сформированный ключ вместе с метаданными, включающими идентификатор ключа, длину, метку времени создания, идентификационную информацию пары целевых УКС, необходимо передать обратно в модули управления КЗК на хранение и дальнейшее использование. Как и в случае квантовых ключей, необходимо обеспечивать контроль идентичности ключей, помещаемых в хранилище.

Таким образом, для обработки запросов на распределение КЗК необходимо осуществление следующих процессов.

1) Построение и поддержание в актуальном состоянии топологии сети КРК. Задача аналогична задаче в классических сетях и не рассматривается в данной работе. Необходимо обратить внимание, что требуется передавать значение метрик сегментов сети КРК, используемых в способе определения маршрута для выработки квантовозащищенного ключа.
2) По известной топологии и известным метрикам сегментов сети определение цепочки УКС для формирования КЗК. В качестве базовой идеи способа определения маршрута можно использовать поиск пути в взвешенном графе.
3) Распределение КЗК согласно выбранному способу, предоставляющему ключи с требуемыми свойствами (см. п. 3.3).

4) Контроль целостности и идентичности передаваемых на вышестоящий уровень ключей (см. п. 2.2).

Модули рассматриваемого уровня имеют связи, как минимум повторяющие квантовые каналы, т.е. прямое общение возможно между модулями соседних узлов. Для организации защиты взаимодействия между модулями соседних узлов достаточно использовать вырабатываемые квантовые ключи. Для организации прямого взаимодействия модулей несоседних узлов необходима загрузка предварительно распределенных ключей для защиты такого взаимодействия или формирование служебных КЗК, т.е. формируемых для нужд непосредственно УКС, без необходимости дальнейшей передачи таких КЗК в СЗИ.

Необходима единая идентификация узлов сети, чтобы по запросу КЗК от вышестоящего уровня, содержащему идентификатор целевого УКС, модуль выработки квантовозащищенных ключей мог однозначно определить этот целевой УКС и построить цепочку УКС для распределения КЗК.

Расчет цепочки УКС для распределения КЗК должен осуществлять узел, на котором произведен запрос КЗК. Пересчет цепочки производится, если по заданной цепочке ключ не выработан (разрыв сетевого соединения между узлами маршрута, выход из строя промежуточного узла и т.д.) или произошел отказ в резерве цепочки. Отказ в резерве должен быть выдан, если в рассчитанную цепочку попал сегмент сети, метрики которого существенно изменились, например, был получен и подтвержден резерв другой цепочки, что изменило количество доступных квантовых ключей.

При получении отказа в резерве хотя бы от одного сегмента сети КРК уже подтвержденный резерв сегментов сети должен отзываться, а маршрут пересчитывается для обеспечения бесперебойности функционирования сети и уменьшения числа отказов при непосредственно распределении КЗК. Для этого модули рассматриваемого уровня должны оперативно оповещать друг друга о рассчитанных и занятых цепочках, что влечет за собой изменение значений метрик сегментов сети и загрузку промежуточных узлов. Таким образом сеть КРК в каждый момент времени сможет разрешать запросы на КЗК наилучшим способом.

Именно для этого рекомендуется реализация в том числе прямой связи между узлами на классических предварительно распределенных ключах или служебных КЗК.

В предлагаемой структуре сети КРК необходимо выполнение следующих функций на рассматриваемом уровне.

1) Управление выработкой квантовых ключей, в том числе:
    а) формирование запросов на выработку квантовых ключей к нижестоящему уровню;
    б) управление вспомогательным оборудованием (оптическими коммутаторами) (опционально);
    в) построение очереди запросов квантовых ключей (для УКС с подключенными оптическими коммутаторами).
2) Хранение квантовых ключей.
3) Обработку запросов на выработку квантовозащищенных ключей от вышестоящего уровня.
4) Поддержание актуальной карты сети КРК, включая топологию квантовых каналов и топологию служебных каналов, защищаемых на классических ключах, для определения цепочек УКС.
5) Распределение квантовозащищенных ключей согласно поступающим запросам, включая:
    а) определение и резервирование маршрута выработки квантовозащищенных ключей;
    б) непосредственно распределение квантовозащищенного ключа согласно выбранному способу (способы распределения разрабатываются в разделе 3.3).

4.1.4 Требования к уровню управления квантовозащищенными ключами

Как описывалось ранее, рассматриваемый уровень необходим для организации взаимодействия с СЗИ-потребителями, а также ограничения доступа извне сети КРК к критичным процессам по выработке КЗК.

Взаимодействие с СЗИ-потребителем в минимальном объеме включает в себя обработку запросов на КЗК от СЗИ-потребителя, затем определение пары узлов, за которыми закреплены СЗИ-потребители, сформировавшие запрос, и реакция на обработанный запрос.

Возможны следующие варианты подключения СЗИ-потребителей:

1) Пара потребителей закреплена за одним и тем же УКС.
2) Пара потребителей закреплена за УКС, связанными прямым квантовым каналом.
3) Пара потребителей закреплена за УКС, не связанными прямым квантовым каналом.

Работа сети КРК и уровня управления квантовозащищенными ключами определяется в самой общем варианте №3.

В ответ на запрос ключа СЗИ-потребителю должен выдаваться запрошенный КЗК, определенный идентификатором ключа, размером и идентификационной информацией пары СЗИ, для которых он выдан. Одновременные запросы от каждого из пары СЗИ перекладывают на сеть КРК определение дублирующих запросов и выбора одного из них. При этом пара СЗИ до получения первых ключей от сети КРК должна обладать возможностью построения защищенного канала взаимодействия, например, для синхронизации введения нового ключа в эксплуатацию. В целях повышения определенности в работе сети КРК необходима модификация взаимодействия пары СЗИ таким образом, чтобы для каждого запроса КЗК один из пары был назначен ведущим, осуществляющим первый запрос к сети. После успешного получения корректного ответа сопряженный СЗИ получит возможность запросить конкретный ключ, уже переданный в первый СЗИ.

Как указано выше, запрос КЗК должен содержать идентификационную информацию пары СЗИ, для которых он запрашивается. Контроль легитимности пары производится на рассматриваемом уровне. С учетом вышесказанного, необходимо выполнять контроль двух видов.

– *Первичный*, при котором от пары СЗИ не было запроса КЗК ни с одного из двух СЗИ. В результате проверки, если запрос разрешен, то формируется запрос на нижестоящий уровень или выдача КЗК из ключевого хранилища при наличии запаса КЗК.

– *По имеющемуся ключу*, при котором для пары СЗИ был сформирован ключ по результатам запроса от ведущего СЗИ, а сопряженный обращается за конкретным КЗК по идентификатору. В данном случае проверка заключается в поиске ключа по идентификатору и сравнении информации о запросившем СЗИ с информацией о паре СЗИ, для которых был выработан ключ, которая хранится в метаданных ключа.

Успешная первичная проверка запроса на КЗК требует перевода запроса на понятный для сети КРК язык, а именно перевода идентификационной информации пары СЗИ в идентификационную информацию пары УКС, к которым подключены эти СЗИ. Одним из пары УКС, соответственно, является УКС, получивший запрос. Для определения второго УКС все УКС сети должны вести и поддерживать в актуальном состоянии базу данных подключенных СЗИ, содержащую пары соответствия СЗИ и УКС.

Взаимодействие с уровнем выработки квантовозащищенных ключей сводится к запросу квантовозащищенного ключа с указанием целевого УКС. В ответ на запрос КЗК может быть получен разными способами в зависимости от того, как расположена пара СЗИ-потребителей. При подключении СЗИ-потребителей к соседним УКС становится возможна передача КК в качестве КЗК, а при подключении к одному УКС – передача последовательности с ДСЧ из состава УКС в качестве КЗК.

Аналогично передаче квантовых ключей от квантовой аппаратуры необходимо обеспечивать синхронизацию КЗК между узлами сети КРК, что подразумевает не только синхронизацию КЗК, получаемых от уровня выработки КЗК, но и поддержание в синхронизированном состоянии ключевых хранилищ, а также обеспечение передачи синхронизированных КЗК в СЗИ-потребители с контролем целостности при передаче.

Хранение квантовозащищенных ключей требует применение алгоритмов защиты хранимых ключей. При этом стоит рассчитывать на долговременное хранение ключей. В идеальном случае сеть КРК должна анализировать частоту и объемы запросов от СЗИ и предоставлять дополнительный объем КЗК заблаговременно для того, чтобы сократить время ожидания пользователя и предоставлять при запросе СЗИ-потребителем заранее распределенный КЗК.

Связи модулей на рассматриваемом уровне должны повторять связи на уровне потребителей для оперативного обмена информацией при формировании и актуализации базы данных подключенных потребителей, контроле идентичности получаемых и передаваемых КЗК и др. Положим, что модули этого уровня имеют связи все-со-всеми, соответственно должны иметь ключи для взаимной попарной аутентификации. С учетом специфики технологии КРК, требуются ключи и способы обеспечения конфиденциальности и целостности информации между модулями данного уровня, стойкие к атакам квантовым компьютером.

Для оптимизации работы сети КРК в целом и повышения ее эксплуатационных характеристик целесообразно осуществлять предварительное накопление КЗК на парах УКС. В неоптимизированном случае запрос нового КЗК для пары СЗИ производится независимо и сгенерированный ключ назначается конкретной паре СЗИ-потребителей. В случае предварительного накопления при наличии нескольких пар СЗИ закрепленных за одной и той же парой УКС распределение КЗК впрок позволяет ускорить работу сети КРК за счет того, что в метаданные КЗК прописывается пара СЗИ, для которых он предназначен, только после выдачи этого ключа на одном из УКС в СЗИ-потребитель. Назовем такой вид накопления «по расписанию». В случае его применения уменьшается время простоя сети КРК, так как в свободное время производится распределение КЗК на высоконагруженных участках без непосредственного запроса от СЗИ.

В части хранения и передачи ключей необходимо, чтобы:

– квантовозащищенные ключи, предназначенные для одного потребителя, никаким образом не могли попасть другому потребителю, подключенному к этому же узлу сети КРК;

– квантовозащищенные ключи, выработанные для данного потребителя для связи с различными потребителями (закрепленными как за одним, так и за разными узлами сети КРК), должны быть различимы.

Таким образом, уровень управления квантовозащищенными ключами должен осуществлять следующие основные функции.

1) Взаимодействие с СЗИ-потребителем, в том числе получение запросов на КЗК и преобразование идентификаторов целевых СЗИ на идентификаторы целевых УКС, используемые в сети КРК.
2) Запросы квантовозащищенных ключей к нижестоящему уровню.
3) Контроль целостности и идентичности КЗК при получении, хранении и передаче.
4) Хранение КЗК.

4.2 Рекомендуемая структура сети КРК

В результате анализа процессов, происходящих в сети КРК, и требований к функциям уровней сети предложим рекомендованную структуру сети КРК и требования к ее функциям. Структура сети КРК в виде узлов и связей между ними представлена на рисунке 25. Используются следующие обозначения.

ККС – квантовый канал связи.

КАК – Классический аутентифицированный канал.

КА – квантовая аппаратура.

Розовым цветом обозначены модули уровня управления КЗК, серым – модули уровня выработки КЗК, а синим – модули уровня выработки квантовых ключей.

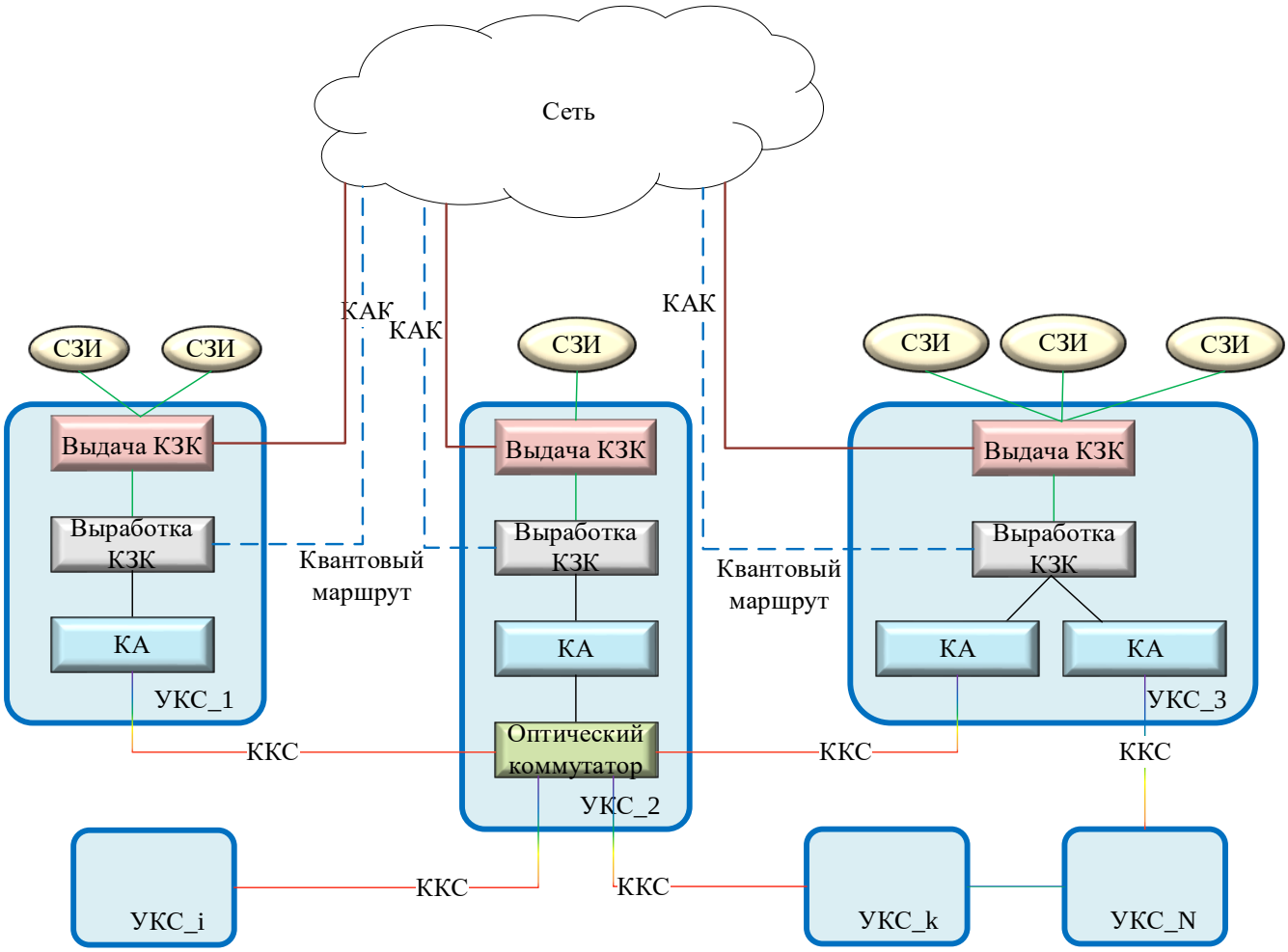


Рисунок 25 – Структура сети КРК (по узлам)

Уровень потребителей имеет следующие функции:

– запрос квантовозащищенного ключа, возможно с указанием желаемых или требуемых параметров запрашиваемого ключа;
– получение КЗК согласно запросу;
– использование ключа согласно предписанию в устройствах этого уровня.

Уровень управления КЗК должен обладать следующими функциями:

– организация хранилищ квантовозащищенных ключей;
– синхронизация ключевых хранилищ попарно (по наличию связи);
– мониторинг запросов на квантовозащищенные ключи (прогнозирование);
– обработка запросов квантовозащищенных ключей от внешних СЗИ;
– поддержание актуальной базы соответствия СЗИ-потребителей и УКС, к которым они подключены;

– формирование запросов квантовозащищенных ключей к нижестоящему уровню выработки квантовозащищенных ключей;
– получение квантовозащищенных ключей от уровня выработки квантовозащищенных ключей;
– передача квантовозащищенных ключей СЗИ-потребителю.

Уровень выработки КЗК должен обладать следующими функциями:

– поддержание актуальной карты сети;
– построение оптимальных цепочек УКС для формирования КЗК;
– распределение КЗК на определенных цепочках УКС;
– организация хранилищ квантовых ключей;
– организация каналов, защищенных на квантовых ключах (для формирования КЗК);
– построение аутентифицированного канала для уровня выработки квантовых ключей (опционально);
– организация запросов квантовых ключей;
– получение квантовых ключей от уровня выработки квантовых ключей;
– передача квантовозащищенных ключей на уровень управления квантовозащищенными ключами в ответ на запрос таких ключей.

Уровень выработки квантовых ключей должен обладать следующими функциями:

– выработка квантовых ключей;
– передача квантовых ключей на уровень выработки квантовозащищенных ключей.

Таким образом, разработаны требования к трехуровневой структуре сети КРК и функциям каждого уровня. Вышестоящие уровни используют результат работы нижестоящего уровня для своего функционирования. Вырабатываемые ключи хранятся не на том уровне, где были созданы. Уровень выработки КЗК менее нагружен выполняемыми функциями по сравнению с европейскими аналогами за

счет переноса части функций на уровень управления КЗК. При этом допускается унификация всех УКС без выделения специальных типов УКС (магистральных, доступа, пользовательских).

В случае необходимости подключения подсети топологии «звезда» (реализованной по п. 3.2), т.е. на основе специальных типов УКС, то подключение реализуется центральным УКС Сервером. При этом порядок работы подсети не изменяется, а формирование КЗК с некоторым внешним по отношению к подсети УКС осуществляется между внешним УКС и УКС Сервером согласно общему порядку формирования КЗК для сети КРК смешанной топологии [123]. Соседний УКС сети КРК смешанной топологии не, являвшийся УКС Клиентом, не рассматривается как периферийный узел УКС Сервера для реализации порядка функционирования подсети топологии «звезда» по п. 3.2.

4.2.1 Порядок распределения КЗК в сети КРК

Учитывая все сформированные ранее требования к сети КРК и ее структуре, имеем следующий порядок работы такой сети при создании КЗК.

Блок-схема процесса создания КЗК представлена на рисунке 26. Цвета блоков соответствуют цвету уровня сети КРК, на котором производится указанное действие. Для выполнения первого сеанса КРК и начала работы сети КРК в целом необходимо предварительное распределение первичных ключей.

Результаты разработки структуры сети КРК и порядок распределения КЗК в такой сети использованы при выполнении работ комплексного проекта "Разработка технологии и аппаратуры сетей квантового распределения криптографических ключей с использованием доверенных узлов", выполняемого по соглашению с Министерством промышленности и торговли РФ № 020-11-2019-933 от 19.11.2019. На описанную сеть КРК, структуру УКС и способ формирования квантовозащищенных ключей получен патент на изобретение [44].

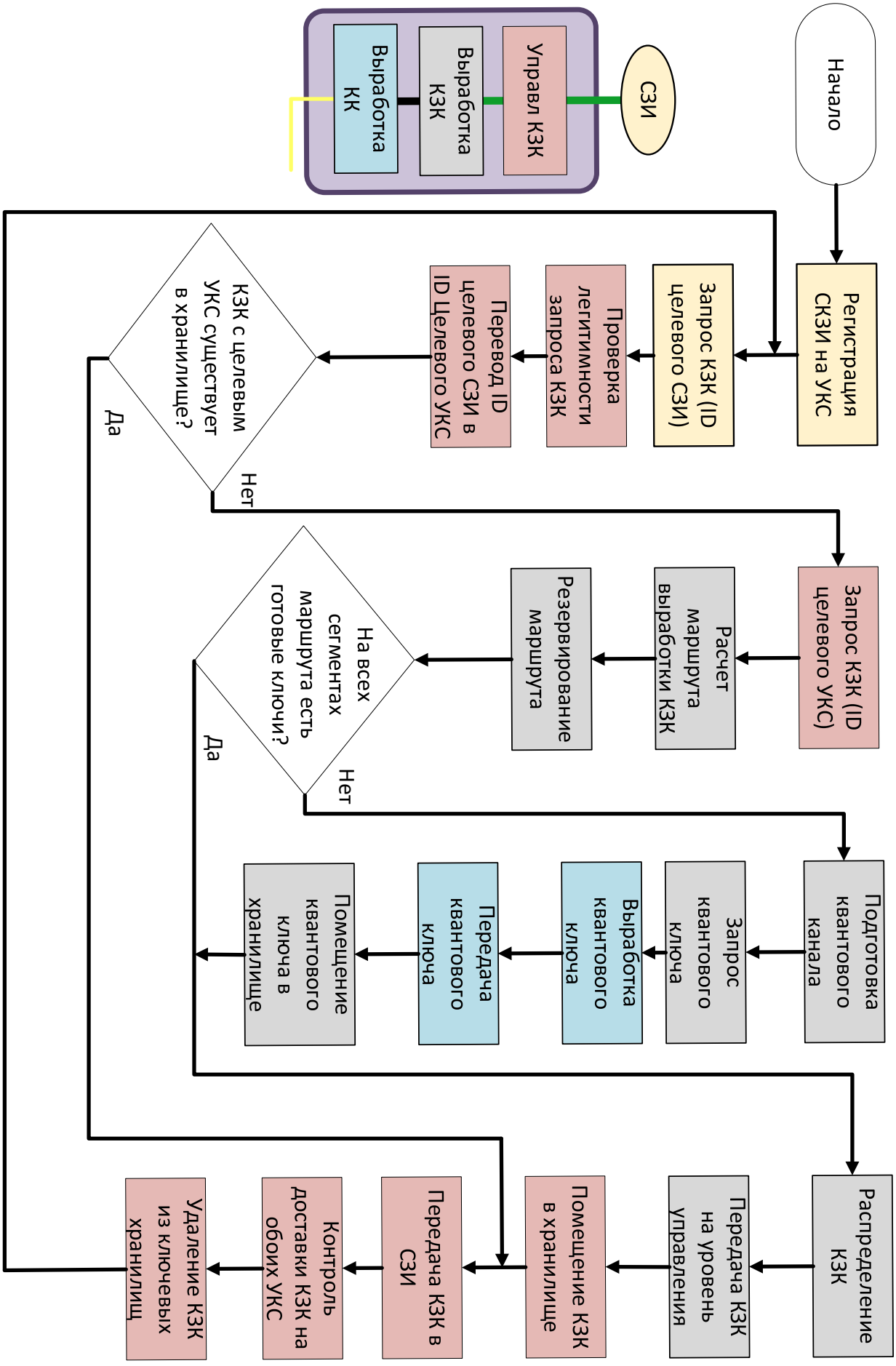


Рисунок 26 – Блок-схема процесса распределения КЗК

4.3 Методика построения сети КРК смешанной топологии

В данном разделе формулируется методика построения сети КРК смешанной топологии на основе разработанных ранее требований к структуре сети и методики распределения КЗК в сети магистральной топологии. Графическое изображение методики в нотации IDEF0 приведено на рисунке 27.

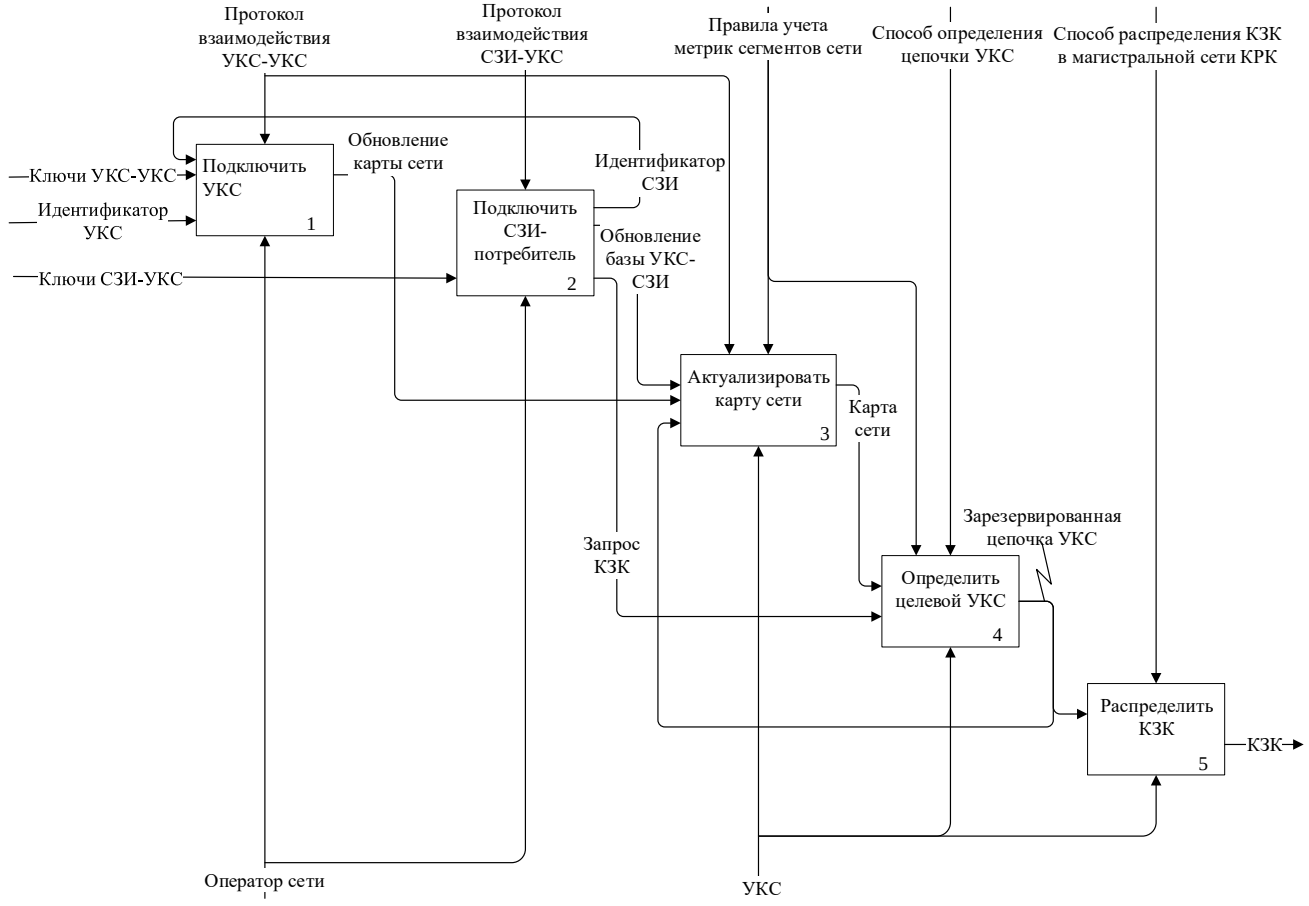


Рисунок 27 – Методика построения сети КРК

Сеть КРК строится из доверенных узлов сети, к каждому из которых могут подключаться внешние пользовательские устройства, СЗИ-потребители. Каждый узел сети содержит не менее одного полукомплекта квантовой аппаратуры и соединен квантовым каналом связи не менее чем с одним соседним узлом сети. Граф связей квантовыми каналами сети КРК должен быть связным.

Рекомендуемая структура узла сети приведена в п. 4.1. Каждый узел сети КРК содержит один или более модулей выработки квантовых ключей, реализованных квантовой аппаратурой. На текущий момент из-за отсутствия

единого полностью стандартизованного протокола КРК на двух концах каждого квантового канала должна располагаться аппаратура, реализованная одним производителем и выполняющая один протокол КРК. На каждом сегменте сети КРК возможно применение различной квантовой аппаратуры. Максимальная длина квантового канала каждого сегмента определяется предельными значениями потерь квантового канала, выбранного на этом сегменте протокола КРК.

Для начала работы сети КРК, а именно начала выработки квантовых ключей для дальнейшей возможности распределения КЗК, необходимо предварительно распределить требуемые наборы ключей, в частности для аутентификации классического канала квантовой аппаратуры, на пары соседних УКС, соединенных квантовым каналом.

Распределение КЗК между парами УКС осуществляется согласно методике по п. 3.5. Расчет магистральной подсети производится тем узлом, на который поступил запрос КЗК на основе актуальной карты сети КРК, включающей метрики сегментов сети. Рекомендации по составу рассматриваемых метрик приведены в п. 4.1. Для определения пар целевых УКС, на которые необходимо распределить КЗК в соответствии с запросом СЗИ-потребителя, необходимо поддерживать актуальную базу соответствия УКС и подключенных к ним СЗИ-потребителей для всей сети. При этом идентификация всех УКС в сети должна быть уникальной для однозначного определения целевых УКС.

Сеть КРК может строится итерационно, путем подключения новых УКС к существующей сети КРК. Для подключения нового УКС к существующей сети КРК необходимо выполнить следующие условия.

– Соединить новый УКС с существующим квантовым каналом. Квантовый канал может быть к имеющемуся в УКС свободному модулю выработки квантовых ключей, к оптическому коммутатору, если УКС поддерживает множественные квантовые каналы в одном модуле выработки квантовых ключей, к новому модулю выработки квантовых ключей, подключенного к существующему УКС для работы с новым подключаемым УКС.

– Загрузить в существующий и новый УКС предварительно распределенные ключи для построения классического аутентифицированного канала квантовой аппаратуры в составе этой пары УКС. Предварительно распределяемые ключи могут создаваться с помощью ДСЧ из состава УКС с последующей доставкой до нового УКС доверенным курьером. После успешного сеанса КРК с новым УКС данный УКС считается подключенным к сети КРК.
– В качестве классических ключей защиты КЗК для распределения КЗК для СЗИ-потребителей могут использоваться КЗК, распределенные с защитой только на квантовых ключах по сети КРК между новым УКС и всеми требуемыми целевыми УКС.

4.4 Выводы по главе

Сформулированы рекомендации по структуре сетей КРК и требования к ее функциям, полученные на основе разработанных способов распределения КЗК и выявленных особенностей квантовой аппаратуры. Такая сеть позволяет распределять квантовозащищенные ключи и передавать их в пары сопряженных СЗИ-потребителей исходя из запрошенного обеспечения СЗИ-потребителей ключами, решая научную проблему регулярной доставки и смены ключей кодирования.

Разработана методика построения сетей КРК на основе сформулированных рекомендаций по структуре сети и функциям ее составных частей, а также методики распределения КЗК в сети магистральной топологии.

Структура сети КРК, соответствующая сформированным рекомендациям, применена при реализации комплексного проекта "Разработка технологии и аппаратуры сетей квантового распределения криптографических ключей с использованием доверенных узлов", выполняемого по соглашению с Министерством промышленности и торговли РФ № 020-11-2019-933 от 19.11.2019.

Внедрение методики построения сети КРК при создании Университетской квантовой мети в МГУ имени М.В.Ломоносова позволило сократить время развертывания на 20%.

ЗАКЛЮЧЕНИЕ

С учетом интенсивно развивающихся потребностей в скоростной и защищенной передаче данных, а также не менее стремительном росте технических возможностей, созданных для этого, необходимо заблаговременно разрабатывать варианты, позволяющие сохранить защищенность данных при их передаче. Регулярная смена секретных ключей в географически разнесенных средствах защиты информации, особенно в случае обеспечения независимости таких ключей, позволяет успешно решить эту задачу.

Для решения вопроса регулярной доставки секретных ключей предложено применение технологии квантового распределения ключей. Однако, технология имеет существенное ограничение предельной допустимой удаленности двух экземпляров квантовой аппаратуры друг от друга, составляющей 100 км, – предельной величины потерь в квантовом канале, при котором протокол КРК остается стойким. В настоящее время единственным осуществимым вариантом преодоления этого ограничения является построение сетей квантового распределения ключей с доверенными промежуточными узлами, осуществляющих классическое перекодирование распределяемых общих секретов.

В работе выявлены и решены научные проблемы, препятствующие построению сетей КРК смешанной топологии. Разработано решение задачи сопряжения пары СЗИ с парой экземпляров квантовой аппаратуры для согласованной выработки общих секретов в простейшей сети «точка-точка». Такой комплекс устройств предложен в качестве базового элемента для построения сетей квантового распределения ключей смешанной топологии.

Выявлены научные проблемы, возникающие в сетях квантового распределения ключей простых топологий «магистраль» и «звезда». Введено понятие квантовозащищенного ключа (КЗК), соответствующее общему секрету, распределяемому между парами оконечных узлов магистральной сети КРК. Введение нового понятия позволяет различать квантовые ключи, создаваемые квантовой аппаратурой из состава сети КРК, и общие секреты, передаваемые

внешним парам внешних пользовательских устройств, распределенных без непосредственного использования принципов квантовой механики. Разработана методика распределения квантовозащищенных ключей для пар оконечных узлов сети КРК магистральной топологии. Данная методика решает существующую проблему появления в открытом виде передаваемых КЗК на промежуточных узлах. Решение для магистральной сети квантового распределения ключей предложено в качестве базовой логической единицы в сетях смешанной топологии. В результате внедрения методики распределения квантовозащищенных ключей сокращен процесс разработки проекта методических рекомендаций ТК26 на 30%.

Проведен анализ существующих мировых решений, касающихся структур, способов функционирования и сценариям применения сетей квантового распределения ключей. Выявлены недостатки рассмотренных решений. На основе проанализированных структур сетей, а также разработанных способа взаимодействия квантовой аппаратуры с СЗИ и методики распределения квантовозащищенных ключей сформулированы требования к структуре и функциям сети КРК смешанной топологии. В результате сформирована методика построения сетей КРК смешанной топологии.

Внедрение методики построения сетей КРК позволило сократить время развертывания Университетской квантовой сети на 20%, ускорило процесс эскизного проектирования аппаратуры сетей квантового распределения ключей с использованием доверенных узлов на 15% и позволило унифицировать аппаратную платформу доверенных узлов.

Направления дальнейших исследований

В качестве дальнейших направлений исследований можно выделить следующие научные и практические задачи.

Технология квантового распределения ключей позволяет вырабатывать независимые секретные ключи, стойкие в теоретико-информационном смысле. Необходима дальнейшая проработка вопроса применения квантовых ключей при

распределении квантовозащищенных ключей для сохранения высокого уровня стойкости ключей. Задача требует как решения практических проблем по ускорению выработки квантовых ключей, включающих создание строго однофотонных источников, повышения частоты и дальности передачи информации в квантовом канале, разработку высокоскоростных физических датчиков случайных чисел, так и теоретических проблем по анализу квантовозащищенных ключей на идеальность, т.е. неотличимость от истинной случайной последовательности с учетом утечки информации при передаче этих ключей по сети квантового распределения ключей. Отдельным аспектом применения технологии квантового распределения ключей является решение вопроса аутентификации канала, необходимого для выполнения протокола КРК.

Важной научной задачей для дальнейших исследований является разработка методики определения цепочки узлов сети КРК, необходимой для распределения квантовозащищенных ключей, в том числе выявление необходимых и достаточных метрик сегментов сети, влияющих на определение таких цепочек. Моделирование сетей КРК в части процессов определения цепочек и распределение квантовозащищенных ключей позволит в дальнейшем определить оптимальный набор и вес метрик для расчета оптимальных цепочек узлов сети КРК.

Утвержденные дорожные карты по программам цифровой экономики, касающиеся квантовых коммуникаций и квантовых вычислений, показывают заинтересованность в успешной реализации технологии КРК в Российской Федерации на высшем уровне. Детальная проработка технических задач, поставленных в дорожных картах, позволит создавать сети квантового распределения ключей на государственном и международном уровне. Дальнейшее развитие техники и технологии должно привести к созданию так называемого квантового интернета, в котором все существующие виды коммуникаций защищаются с применением квантовых технологий, включая локальные и глобальные сети передачи информации, устройства интернета вещей, интеграцию мобильных устройств в стационарные сети связи.

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

ВОЛС	волоконно-оптическая линия связи
ДСЧ	датчик случайных чисел
КЗК	квантовозащищенный ключ
КРК	квантовой распределение ключей
СЗИ	средство защиты информации
УКС	узел сети КРК
ETSI	European Telecommunications Standards Institute
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
NIST	National Institute of Standards and Technology
QBER	quantum bit error rate
QKD	quantum key distribution

СПИСОК ТЕРМИНОВ

1 аппаратура КРК (квантовая аппаратура): Программно-аппаратные средства, реализующие квантовый протокол выработки и распределения ключей с целью изготовления квантовых ключей для пространственно-распределенных СЗИ.

2 квантовозащищенный ключ: Общий секрет, созданный сетью КРК, части для создания которого передавались по сети КРК с защитой на квантовых ключах.

3 квантовый канал: Логический канал, используемый квантовой аппаратурой для передачи квантовых информационных состояний.

4 квантовый ключ: Случайная последовательность, полученная в процессе выполнения протокола КРК из очищенного ключа в результате процедуры усиления секретность.

5 классический аутентифицированный канал: Логический канал, используемый квантовой аппаратурой при выполнении протокола КРК на этапах настройки квантового канала и постобработки последовательности, переданной через квантовый канал.

6 клиент КРК: Экземпляр квантовой аппаратуры, содержащий источник одиночных фотонов.

7 нарушитель: Участник, выполняющий действия, не предписанные протоколом, с целью нарушения его конфиденциальности, целостности.

8 очищенный ключ: Случайная последовательность, полученная в процессе выполнения протокола КРК из просеянного ключа в результате процедуры исправления ошибок.

9 просеянный ключ: Случайная последовательность, полученная в процессе выполнения протокола КРК из сырого ключа в результате процедуры согласования базисов.

10 протокол КРК: Протокол кодирования, состоящий из передачи случайно последовательности по квантовому каналу с использованием принципов

квантовой механики и последующей обработки этой последовательности по классическому аутентифицированному каналу с целью получения квантового ключа.

11 сеанс КРК: Одна итерация выполнения протокола КРК.

12 сегмент сети КРК: Часть сети КРК, состоящая из двух узлов сети КРК, соединенных одним квантовым каналом.

13 секретный ключ: Специальный параметр протокола (схемы), известный одному или нескольким участникам и не известный нарушителю.

14 сервер КРК: Экземпляр квантовой аппаратуры, содержащий детектор одиночных фотонов.

15 сеть КРК: Организованная совокупность программно-аппаратных средств, физических и логических каналов их соединяющих, обеспечивающая выработку квантовых ключей между узлами, соединенными напрямую квантовым каналом, и распределение квантовозащищенных ключей между произвольной парой узлов.

16 СЗИ-потребитель: СЗИ, являющееся внешним устройством по отношению к сети КРК, получающее КЗК от УКС для связи с другим СЗИ-потребителем, подключенном к УКС (возможно тому же).

17 соседние УКС: Узлы квантовой сети, соединенные квантовым каналом, способные вырабатывать общий квантовый ключ.

18 сырой ключ: Случайная последовательность, полученная двумя участниками протокола КРК в результате передачи случайной последовательности по квантовому каналу.

19 узел сети КРК: Элемент сети КРК, состоящий из одного или нескольких экземпляров квантовой аппаратуры и одного или нескольких служебных СЗИ, соединенный с другими узлами сети КРК как минимум одним квантовым каналом и предназначенный для формирования квантовых и квантовозащищенных ключей с другими узлами сети КРК

20 целевые УКС (оконечные УКС): Пара узлов сети КРК, к которым подключена пара СЗИ-потребителей, для которых необходимо распределить квантовозащищенный ключ для передачи в эти СЗИ-потребители.

СПИСОК ЛИТЕРАТУРЫ

1. Quantum Safe Cryptography and Security [Электронный ресурс]. – ETSI. – Режим доступа: http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf, свободный (дата обращения: 20.09.2020).

2. ID Quantique SA. Quantum-safe Security. White Paper. Understanding Quantum Cryptography 2020. [Электронный ресурс]. – Режим доступа: https://marketing.idquantique.com/acton/attachment/11868/f-020d/1/-/-/-/-/Understanding%20Quantum%20Cryptography_White%20Paper.pdfб свободный (дата обращения: 20.09.2020).

3. Barker E. Recommendation for Key Management, Part 1: General. [Электронный ресурс] // NIST. – 2016. – Режим доступа: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf, свободный (дата обращения: 23.05.2018)

4. Р 1323565.1.012-2017 Рекомендации по стандартизации «Принципы разработки и модернизации шифровальных (криптографических) средств защиты инфрпмации». // Москва: Росстандарт. – 2016.

5. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Journal on Scientific and Statistical Computing. – 1997. – Vol. 26, No. 5. – P. 1484–1509.

6. Schnorr C.P. Fast Factoring Integers by SVP Algorithms [Электронный ресурс]. – Режим доступа: https://eprint.iacr.org/eprint-bin/getfile.pl?entry=2021/232&version=20210409:151242&file=232.pdf, свободный (дата обращения: 12.12.2021)

7. ID Quantique. Clavis300 Quantum Cryptography Platform Brochure. [Электронный ресурс] // 2019. – Режим доступа: https://marketing.idquantique.com/acton/attachment/11868/f-42e4a1b3-46a2-4f2f-8fcd-ba9118954c3a/1/-/-/-/-/Clavis300_QKD_Brochure.pdf, свободный (дата обращения 20.09.2020)

8. Quantum Key Distribution Products [Электронный ресурс] // TOSHIBA CORPORATION. – Режим доступа: https://www.toshiba.co.jp/qkd/en/products.htm, свободный (дата обращения: 20.09.2020).

9. ОАО "ИнфоТеКС". ViPNet Quandor. Система автоматической доверенной доставки криптографических ключей. Брошюра [Электронный ресурс]. – Режим доступа: https://quantum-crypto.ru/upload/medialibrary/96c/quant_brochure.pdf, свободный (дата обращения: 20.09.2020).

10. Bennet C.H. Quantum Cryptography: Public Key Distribution and Coin Tossing / C.H. Bennet, G. Brassard. // Theoretical Computer Science – 2014. –Vol. 560, pt. 1. – P. 175–179.

11. Continuous-variable quantum key distribution with Gaussian modulation – the theory of practical implementations / F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, H. Hübel // Adv. Quantum Technol. – 2018. – Vol. 1, No. 1. – P. 1870011

12. Quantum Key Distribution: A Networking Perspective / M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, M. Voznak // ACM Comput. Surv. – 2021. – Vol. 53, no. 5. – P. 1–41.

13. 600-km repeater-like quantum communications with dual-band stabilization / M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, A. J. Shields // Nature Photonics. – 2021. – Vol. 15. – З. 530–535.

14. Quantum networks in the UK / A. Wonfor, C. White, A. Lord, R. Nejabati, T. P. Spiller, J. F. Dynes, A. J. Shields, R. V. Penty // Proc. SPIE 11712, Metro and Data Center Optical Networks and Short-Reach Links IV. – 2021. – P. 1171207.

15. Молотков С.Н. О стойкости волоконной квантовой криптографии при произвольных потерях в канале связи: запрет измерений с определенным исходом // Письма в ЖЭТФ. – 2014. – Т. 100, вып. 6. – С. 457–464.

16. Кронберг Д.А. Двойственность квантовых каналов связи и коллективная атака прием-перепосыл на квантовое распределение ключей с дифференциально-фазовым кодированием / Д.А. Кронберг, С.Н. Молотков // Письма в ЖЭТФ. –2014. – Т. 100. – С. 305.

17. Молотков С.Н. Аналог дифференциально-фазовой квантовой криптографии на когерентных состояниях с доказуемой криптографической стойкостью // Письма в ЖЭТФ. – 2015. –Т. 102, вып. 6. – С. 436–443.

18. Практическая квантовая криптография / К.А. Балыгин, В.И. Зайцев, А.Н. Климов, А.И. Климов, С.П. Кулик, С.Н. Молотков // Письма в ЖЭТФ. – 2017. – Т. 105, вып. 9. – С. 570–576.

19. The security of practical quantum key distribution / V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dusek, N. Lutkenhaus, M. Peev // Reviews of Modern Physiscs. – 2009. – Vol. 81, No. 3. – P. 1301.

20. Mosca M. Cybersecurity in an era with quantum computers: will we be ready? // IEEE Security & Privacy. – 2018. – Vol. 16, No. 5. – P. 38–41.

21. Mulholland J. The Day the Cryptography Dies / J. Mulholland, M. Mosca, J. Braun // IEEE Security & Privacy. – 2017. – Vol. 15, No. 4. – P. 14–21.

22. Creation of backdoors in quantum communications via laser damage / V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, S. Sajeed // Phys. Rev. A. – 2016. – Vol. 94, No. 3. – P. 030302.

23. Eavesdropper's ability to attack a free-space quantum-key-distribution receiver in atmospheric turbulence / P. Chaiwongkhot, K.B. Kuntz, Y. Zhang, A. Huang, J.P. Bourgoin, S. Sajeed, N. Lutkenhaus, T. Jennewein, V. Makarov // Phys. Rev. A. – 2019. – Vol. 99, No. 6. – P. 062315.

24. Implementation vulnerabilities in general quantum cryptography / A. Huang, S. Barz, E. Andersson, V. Makarov // New journal of Physics. – 2018. – Vol. 20. – P. 103016.

25. Courtland R. China’s 2,000-km Quantum Link Is Almost Complete // IEEE spectrum. – 2016. – Vol. 53, No. 11. – P. 11–12.

26. An integrated space-to-ground quantum communication network over 4,600 kilometres / Y.A. Chen, Q. Zhang, T.Y. Chen, W.Q. Cai, S.K. Liao, J. Zhang, K. Chen, J. Yi, J.G. Ren, Z. Chen, S.L. Han // Nature. – 2021. – Vol. 589. – P. 214–219.

27. Current status of the DARPA quantum network / C. Elliot, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, H. Yeh // Proceedings Volume 5815, Quantum Information and Computation III. – 2015. – Vol. 8515. – DOI: 10.1117/12.606489

28. The Madrid Quantum Network: A Quantum-Classical Integrated Infrastructure / V. Martin, A. Aguado, P. Salas, A.L. Sanz, J.P. Brito, D. R. Lopez, V. Lopez, A. Pastor, J. Folgueira, H. H. Brunner, S. Bettelli, F. Fung, L. C. Comandar, D. Wang, A. Poppe, M. Peev // Proceedings OSA Advanced Photonics Congress (AP) 2019 (IPR, Networks, NOMA, SPPCom, PVLED). – 2019. – p. QtW3E.5

29. Field trial of multi-node, coherent-one-way Quantum Key Distribution with encrypted 5×100G DWDM transmission system / A. Wonfor, C. White, A. Bahrami, J. Pearse, G. Duan, A. Straw, T. Edwards, T. Spiller, R. Penty, A. Lord // 45th European Conference on Optical Communication (ECOC 2019). – 2019. – pp. 1–4.

30. Испытание комплекса квантовой криптографической аппаратуры защиты информации на городских волоконно-оптических линиях связи / А.В. Борисова, А.Е. Жиляев, С.В. Алферов, В.Л. Елисеев, Ю.В. Кармазиков, А.Н. Климов, К.А. Балыгин // Вестник российского нового университета. Серия: сложные системы: модели, анализ и управление. – 2019. – № 4. – С. 100–110.

31. Demonstration of a quantum key distribution network in urban fibre-optic communication lines / E.O. Kiktenko, N.O. Pozhar, A.V. Duplinskiy, A.A. Kanapin, A.S. Sokolov, S.S. Vorobey, A.V. Miller, V.E. Ustimchik, M.N. Anufriev, A.T. Trushechkin, R.R. Yunusov, V.L. Kurochkin, Yu.V. Kurochkin and A.K. Fedorov // Quantum Electronics. – 2017. – Vol. 47, No. 9. – P. 798.

32. Егоров В.И., Глейм А.В., Рупасов А.В. Система квантового распределения ключа на поднесущих частотах модулированного излучения с компенсацией искажений сигнала / В.И. Егоров, А.В. Глейм, А.В. Рупасов // Ученые записки Казанского университета. Серия: физико-математические науки. – 2013. – Т. 155, вып. 1. – С. 59–65.

33. Квантовая коммуникация на боковых частотах со скоростью 1Мбит/с в городской сети / А.В. Глейм, В.В. Чистяков, О.И. Банник, В.И. Егоров, Н.В. Булдаков, А.Б. Васильев, А.А. Гайдаш, А.В. Козубов, С.В. Смирнов, С.М. Кынев,

С.Э. Хоружников, С.А. Козлов, В.Н. Васильев // Оптический журнал. – 2017. – Т. 84, вып. 6. – С. 4–9.

34. Перечень докладов конференции QCrypt-2018 [Электронный ресурс] // Режим доступа: http://2018.qcrypt.net/scientific-program, свободный (дата обращения: 20.09.2020).

35. Перечень докладов конференции QCrypt-2019 [Электронный ресурс] // Режим доступа: http://2019.qcrypt.net/scientific-program/, свободный (дата обращения: 19.02.2020).

36. Large scale quantum key distribution: challenges and solutions / Q. Zhang, F. Xu, Y.A. Chen, C.Z. Peng, J.W. Pan // Optics Express. – 2018. – Vol. 26. – P. 24260.

37. Industry Specification Group (ISG) on Quantum Key Distribution for users (QKD) [Электронный ресурс] // ETSI: [сайт]. – Режим доступа: https://www.etsi.org/committee/1430-qkd, свободный (дата обращения: 20.09.2020).

38. Study Group 13 Recommendations Treeview [Электронный ресурс] // ITU-T Recommendations: [сайт]. –Режим доступа: https://www.itu.int/ITU-T/recommendations/index_sg.aspx?sg=13, свободный (дата обращения: 20.09.2020).

39. ISO/IEC WD 23837-1.3. Information technology security techniques — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements [Электронный ресурс] // Режим доступа: https://www.iso.org/standard/77097.html, свободный (дата обращения: 20.08.2020).

40. Open-QKD [Электронный ресурс]. –Режим доступа: https://openqkd.eu/, свободный (дата обращения: 20.08.2020).

41. Дорожная карта развития "сквозной" цифровой технологии "Квантовые технологии" [Электронный ресурс]. –Режим доступа: https://digital.gov.ru/uploaded/files/07102019kvantyi.pdf, свободный (дата обращения: 17.6.2020).

42. Королев И. Паспорт "дорожной карты" развития высокотехнологичной области "квантовые коммуникации" на период до 2024 года. 2020. [Электронный ресурс]. –Режим доступа: https://digital.ac.gov.ru/upload/iblock/a28/%D0%94%D0%BE%D1%80%D0%BE%D0

%B6%D0%BD%D0%B0%D1%8F%20%D0%BA%D0%B0%D1%80%D1%82%D0%B0%20%D0%BA%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D1%8B%D0%B5%20%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D0%BD%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B8.pdf, свободный (дата обращения: 20.08.2020).

43. Пат. 2 736 870 РФ МПК H 04 L 9/08. Комплекс для защищенной передачи данных в цифровой сети передачи данных с использованием однопроходной системы квантового распределения ключей и способ согласования ключей при работе комплекса / А.Г. Втюрина, А.Е. Жиляев. –№ 2019144324: заявл. 27.12.2019: опубл. 23.11.2020, Бюл. № 33. – 6 с.

44. Пат. 2 752 844 РФ, МПК H 04 L 9/08. Система выработки и распределения ключей и способ распределенной выработки ключей с использованием квантового распределения ключей (варианты) / А.Е. Жиляев. –№ 2020140774: заявл. 10.12.2020: опубл. 11.08.2021, Бюл. №23. – 9 с.

45. Реализация средства криптографической защиты информации, использующего квантовое распределение ключей / А.Г. Втюрина, В.Л. Елисеев, А.Е. Жиляев, А.С. Николаева, В.Н. Сергеев, А.В. Уривский// Доклады ТУСУР. – 2018. – Т. 21. – № 2. –С. 15–21.

46. Жиляев А.Е. Классификация схем выработки и распределения ключей в сетях квантового распределения ключей произвольной топологии // Доклады ТУСУР. – 2021. – Т. 24. – № 4. –С. 33–39.

47. Подход к формированию уровней доверия для оценки рисков ошибок аутентификации / А.Е. Жиляев, А.Г. Сабанов, П.А. Шелупанова, Д.С. Брагин, А.А. Мицель, М.Ю. Катаев // Вопросы защиты информации. –2022. – № 1. – С. 17–22.

48. Zhilyaev A.E. On the question of the authentication tag length based on reed-solomon codes / A.E. Zhilyaev, E.B. Gurova // Moscow Workshop on Electronic and Networking Technologies, MWENT 2018 – PROCEEDINGS. – 2018. –P. 1–5.

49. Borodin M. Key generation schemes for channel authentication in quantum key distribution protocol / M. Borodin, A. Zhilyaev, A. Urivskiy // IET Quant. Comm. – 2021. – Vol. 2 – № 3. – pp. 90– 97. – doi: 10.1049/qtc2.12020.

50. Zhilyaev A., Nikolaeva A., Borodin M., Sergeev V. Multilayer Structure of a Scalable Quantum Key Distribution (QKD) Network [Электронный ресурс] // Poster. – 2019. – Режим доступа: http://2019.qcrypt.net/scientific-program/posters/, свободный (дата обращения: 05.07.2020).

51. Borodin M., Urivskiy A., Zhilyaev A. On Key Generation Schemes with QKD for Applications [Электронный ресурс]. // Poster. – 2020. –Режим доступа: https://2020.qcrypt.net/posters/QCrypt2020Poster073Zhilyaev.pdf, свободный (дата обращения: 20.08.2020).

52. Жиляев А. Квантовая сеть и сервисы управления криптографическими ключами // IX Симпозиум "Современные тенденции в криптографии". – 2020. – Режим достпа: https://ctcrypt.ru/files/files/4_Zhilyaev.pdf, свободный (дата обращения: 20.09.2020).

53. Пат. 2 708 511 РФ, МПК H 04 L 9/08, G 06 F 21/72. Способ формирования ключа между узлами вычислительной сети с использованием системы квантового распределения ключей / А.Е. Жиляев. – № 2019102923: заявл. 04.02.2019: опубл. 09.12.2019, Бюл. № 34. – 2 с.

54. ViPNet Quandor [Электронный ресурс] // Квантовая криптография для защиты информации: [сайт]. – Режим доступа: https://quantum-crypto.ru/projects/vipnet-quandor/, свободный (дата обращения: 01.02.2022).

55. ViPNet Quantum Security System [Электронный ресурс] // Квантовая криптография для защиты информации: [сайт]. – Режим доступа: https://quantum-crypto.ru/projects/vipnet-qss/, свободный (дата обращения: 01.02.2022).

56. Квантовый генератор случайных чисел, основанный на пуассоновской статистике фотоотсчетов, со скоростью около 100 Мбит/с / К.А. Балыгин, В.И. Зайцев, А.Н. Климов, С.П. Кулик, С.Н. Молотков // Письма в ЖЭТФ. – 2018. – Т. 153, вып. 6. – С. 879–894.

57. Satellite-to-ground quantum key distribution / L. Sheng-Kai, C. Wen-Qi, L. Wei-Yue, Z. Liang, L. Yang, R. Ji-Gang, Y. Juan, S. Qi, C. Yuan, L. Zheng-Ping, L. Feng-Zhi, C. Xia-Wei, S. Li-Hua, J. Jian-Jun, W. Jin-Cai, J. Xiao-Jun, W. Jian-Feng, H. Yong-Mei, W. Qiang, Z. Yi-Lin, D. Lei, X. Tao, M. Lu, H. Tai, Z. Qiang, C. Yu-Ao, L. Nai-

Le, W. Xiang-Bin, Z. Zhen-Cai, L. Chao-Yang, S. Rong, P. Cheng-Zhi, W. Jian-Yu, P. Jian-Wei // Nature. –2017. – Vol. 549. –P. 43–47.

58. Quantum-limited measurements of optical signals from a geostationary satellite / K. Günthner, I. Khan, D. Elser, B. Stiller, Ö. Bayraktar, C. Müller, K. Saucke, D. Tröndle, F. Heine, S. Seel, P. Greulich, H. Zech, B. Gütlich, S. Philipp-May, C. Marquardt, G. Leuchs, // Optica. –2017. – Vol. 4, No. 6. – P. 611–616.

59. Entanglement-based quantum communication over 144 km / R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, A. Zeilinger // Nature Physics. – 2007. – Vol. 3, No. 7. – P. 481–486.

60. Активная стабилизация оптической части в волоконной квантовой криптографии / К.А. Балыгин, А.Н. Климов, С.П. Кулик, С.Н. Молотков // Письма в ЖЭТФ. –2016. –Т. 103, вып. 6. –С. 469–474.

61. Волокно оптическое стандартное с низким пиком воды для систем связи E3 (G652D) [Электронный ресурс]. – Режим доступа: https://www.rusfiber.ru/assets//files/products/Specification_E3(G652D)_rus.pdf, свободный (дата обращения: 17.01.2022).

62. ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры. // Межгосударственный совет по стандартизации, метрологии и сертификации. – 2018.

63. Piani M., Mosca M., Neill B. Quantum Random-Number Generators: Practical Considerations and Use Cases [Электронный ресурс]. – Режим доступа: https://www.evolutionq.com/quantum-safe-publications/qrng-report-2021-evolutionQ.pdf, свободный (дата обращения: 03.04.2021).

64. Молотков С.Н. О фундаментальном пределе скорости генерации случайных последовательностей в квантовых генераторах с непрерывной переменной // Письма в ЖЭТФ. – 2020. – Т. 157, вып. 3. – С. 442–453.

65. ГОСТ 34.11-2018 Информационная технология. Криптографическая защита информации. Функция хэширования. // Межгосударственный совет по метрологии, стандартизации и сертификации. – 2019.

66. Abidin A., Larsson J.A. Security of Authentication with a Fixed Key in Quantum Key Distribution [Электронный ресурс]. – 2011. –Режим доступа: https://arxiv.org/abs/1109.5168, свободный (дата обращения: 17.07.2016)

67. Mosca M. Quantum Key Distribution in the Classical Authenticated Key Exchange Framework / M. Mosca, D. Stebila, B. Ustaoglu // Post-Quantum Cryptography. PQCrypto 2013. Lecture Notes in Computer Science. – 2013. – Vol. 7932. – P. 136-154. – DOI: 10.1007/978-3-642-38616-9_9

68. Lo H.K. Measurement-Device-Independent Quantum Key Distribution / H.K. Lo, M. Curty, B. Qi // phys. Rev. Lett. – 2020. – Vol. 108, No. 13. – P. 130503.

69. Large scale quantum key distribution: challenges and solutions / Q. Zhang, F. Xu, Y.A. Chen, C.Z. Peng, J.W. Pan // Optics Express. – 2018. – Vol. 26, No. 18. – P. 24260–24273.

70. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters / M. Lucamarini, Z.L. Yuan, J.F. Dynes, A.J. Shields // Nature. –2018. – № 557. – P. 400–403.

71. On the Capacity Region of Bipartite and Tripartite Entanglement Switching / G. Vardoyan, S. Guha, P. Nain, D. Towsley // ACM SIGMETRICS Performance Evaluation Review. – 2020. – Vol. 48, No. 3. – P. 45–50.

72. On the Analysis of a Multipartite Entanglement Distribution Switch / P. Nain, G. Vardoyan, S. Guha, D. Towsley // Proceedings of the ACM on Measurement and Analysis of Computing Systems. – 2020. – Vol. 4, No. 2. – P. 1–39.

73. Advances in quantum cryptography / S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, P. Wallden // Advances in Optics and Photonics. – 2020. – Vol. 12, No. 4. – P. 1012–1236

74. Secure quantum key distribution with realistic devices / F. Xu, X. Ma, Q. Zhang, H.K. Lo, J.W. Pan J.W // Reviews of Modern Physics. – 2020. – Vol. 92, No. 2. – P. 025002.

75. Yang C. Quantum key distribution network: Optimal secret-key-aware routing method for trust relaying / C. Yang, H. Zhang, J. Su // China Communications. – 2018. – Vol. 15, No. 2. – P. 33–45.

76. Quantum key distribution network for multiple applications / A. Tajima, T. Kondoh, T. Ochi, M. Fujiwara, K. Yoshino, H. Iizuka, T. Sakamoto, A. Tomita, E. Shimamura, S. Asami // Quantum Science and Technology. – 2017. – Vol. 2, no. 3. – P. 034003.

77. A secure communication network infrastructure based on quantum key distribution technology / Y. Tanazawa, R. Takahashi, H. Sato, A. Dixon, S. Kawamura // IEICE trans. Commun. – 2016. – Vol. E99–B. No. 5. – P. 1054–1069.

78. Field and long-term demonstration of a wide area quantum key distribution network / S. Wang, W. Chen, Z.Q. Yin, H.W. Li, D.Y. He, Y.H. Li, Z. Zhou, X.T. Song, F.Y. Li, D. Wang // Optics Express. –2014. –Vol. 22, no. 18. – P. 21739–21756.

79. Пат. 2 697 696 РФ, МПК H 04 L 9/08. Способ передачи сообщения через вычислительную сеть с применением аппаратуры квантового распределения ключей / А.М. Поздняков (РФ). – № 2 019 101 393; заявл. 18.01.19; опубл. 16.08.19, Бюл. № 23. – 3 с.

80. Zapareto V. Secure quantum key distribution with a subset of malicious devices / V. Zapareto, M. Curty // npj Quantum Information. – 2021. – Vol. 7. – P. 26.

81. Fu. Y., Liu S., Gao Y., Chen X. Quantum key distribution system, method and apparatus based on trusted relay // United States patent US10348493. – H04L9/0858. – Jul 9, 2019.

82. The SECOQC quantum key distributin network in Vienna / M. Peev, C. Pacher, R. Alleaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O.

Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, A. Zeilinger // New Jour. Of Phys. – 2009. – Vol. 11. – P. 075001.

83. ETSI GS QKD 004 v.2.1.1 Quantum Key Distribution (QKD); Application Interface [Электронный ресурс]. – Режим доступа: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/02.01.01_60/gs_QKD004v020101p.pdf, свободный (дата обращения: 11.12.2021).

84. ETSI GS QKD 014 V1.1.1 Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API [Электронный ресурс]. –2019. – Режим доступа: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_QKD014v010101p.pdf, свободный (дата обращения 20.09.2020)

85. ITU-T Recommendation Y.3800: Overview on networks supporting quantum key distribution [Электронный ресурс]. – Режим доступа: https://www.itu.int/rec/T-REC-Y.3800-202004-I!Cor1/en, свободный (дата обращения: 11.12.2021).

86. ITU-T Recommendation Y.3805: Quantum key distribution networks – Software defined networking control. [Электронный ресурс]. – 2021. – Режим доступа: https://handle.itu.int/11.1002/1000/14770, свободный (дата обращения: 11.12.2021).

87. Quantum cryptography / N. Gisin, G. Ribordy, T. Wolfgang, H. Zbinden // Reviews of modern physics. –2002. – Vol. 74, No. 1. – P. 145.

88. Kiryukhin V.A. An algorithm for computing the upper bound for non-minimum weight differentials in 2-round LSX-ciphers // Математические вопросы криптографии. – 2021. – Т. 12. №. 2. – С. 93–109.

89. Wegman M.N. New hash functions and their use in authentication / M.N. Wegman, L. Carter // J. Comput. Syst. Sci. – 1981. – No. 22. – P. 265–279.

90. Abidin A. Authentication in Quantum Key Distribution: Security Proof and Universal Hash Functions // Dissertation. –Division of Information Coding, Linkoping University, Linkoping, Sweden. – 2013. – ISBN 978-91-7519-625-1.

91. Calimani S. Unconditionally secure authentication for quantum key distribution // Dissertation. – Facoltà di Ingegneria, UNIVERSITÀ DEGLI STUDI DI PADOVA, Padova, Italy. – 2011. – 98 P.

92. Atici M. Universal hashing and multiple authentication / M. Atici, D.R. Stinson // Advances in Cryptology – CRYPTO '96. Lecture Notes in Computer Science. – 1996. – Vol. 1109. – P. 16–30.

93. Cederof J. Security Aspects of the Authentication Used in Quantum Cryptography / J. Cederof, J. Larsson // IEEE Transaction on information Theory. –2008. – Vol. 54, No. 4. – P. 1735–1741.

94. Stinson D.R. Universal hash families and the leftover hash lemma, and applications // J. Combin. Math. Combin. Comput. – 2002. – No. 42. – P. 3–31.

95. den Boer B. A simple and key-economical unconditional authentication scheme // J. Comp. Sec. – 1993. – Vol. 2. – pp. 65–72.

96. Bierbrauer J. On families of hash functions via geometric codes and concatenation / J. Bierbrauer, T. Johansson, G. Kabatianskii, B. Smeets// Advances in Cryptology – CRYPTO ’93. Lecture Notes in Computer Science. – 1994. – Vol. 773. – P. 331–342.

97. Mansour Y. The computational complexity of universal hashing / Y. Mansour, N. Nisan, P. Tiwari // STOC '90: Proceedings of the twenty-second annual ACM symposium on Theory of Computing. – 1990. – P. 235–243.

98. Жиляев А.Е. К вопросу об аутентификации классического канала в системах квантового распределения ключей // Безопасные информационные технологии : Сборник трудов Восьмой всероссийской научно-технической конференции. – Москва. – 2017. – С. 202–205.

99. О коррекции ошибок в системах квантовой криптографии / К.А. Балыгин, А.Н. Климов, С.П. Кулик, С.Н. Молотков // Письма в ЖЭТФ. –2016. – Т. 104, вып. 5. – С. 349–355.

100. ГОСТ 34.13-2018. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. // Межгосударственный совет по метрологии, стандартизации и сертификации. – 2019.

101. Kabushiki K. Communication device, communication method and communication system // US Patent 201800554304. – Feb 15, 2017.

102. Wan S., Hong C., Jeong Y., Kwon O., Ko H.S., Jang J., Kwon D. Authentication apparatus and method for quantum cryptography communication // US Patent Application 20190238326. – Aug 01, 2019.

103. Berzanskis A., Jankovich P. Standards-compliant encryption with QKD. // US PatentApplication 20050063547. – Mar 24, 2005.

104. Quantum Repeaters for Quantum Communication / H.J. Briegel , J.I. Cirac, W. Dur, G. Giedke, P. Zoller // Vienna Circle Institute Yearbook. – 1999. – Vol. 7. – P. 147–154.

105. Extending Quantum Links: Modules for Fiber- and Memory-Based Quantum Repeaters / P. Loock, W. Alt, C. Becher, O. Benson, H. Boche, C. Deppe, J. Eschner, S. Hofling, D. Meschede, P. Michler, F. Schmidt, H. Weinfurter // Advances Quantum Technologies. – 2020. – Vol. 3, No. 11. – P. 1900141. – DOI: 10.1002/qute.201900141.

106. Холево А.С. Квантовые системы, каналы, информация // МЦМНО. – 2010. – 328 с.

107. Satoh T. Quantum network coding for quantum repeaters / T. Satoh, F.L. Gall, H. Imai // phys.Rev.A. – 2012. – Vol. 86. – P. 032331.

108. Optimal architectures for long distance quantum communication / S. Muralidharan, L. Li, J. Kim, N. Lutkenhaus, M.D. Lukin, L. Jiang // Scientific Reports. – 2016. – Vol. 6. – P. 20463.

109. The Status of Quantum-Key-Distribution-Based Long-Term Secure Internet Communication / M. Geihs, O. Nikiforov, D. Demirel, A. Sauer, D. Butin, F. Günther, G. Alber, T. Walther, J. Buchmann // IEEE Transactions on Sustainable Computing. – 2021. – Vol. 6, No. 1. – P. 19–29.

110. Elliot C. Building the quantum network // New Journal of Physics. – 2002. – Vol. 4, No. 1. – P. 46.

111. ViPNet Channel Protection. Решения для защиты каналов связи [Электронный ресурс]. – Режим доступа:

https://russianfieldday.ru/upload/iblock/a0a/Channel_Protection_A4_2020_web.pdf, свободный (дата обращения: 20.09.2020).

112. Senetas Corporation Ltd. CN6000 Series Encryptors:CN6040 1G Ethernet / 4G Fibre Channel Encryptor, CN6100 10G Ethernet Encryptor [Электронный ресурс]// Computer security resource center NIST. – Режим доступа: https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2231.pdf, свободный (дата обращения: 20.09.2020).

113. Cambridge quantum network / J.F. Dynes, A. Wonfor, W.W.-S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z.L. Yuan, A.R. Dixon, J. Cho, Y. Tanizawa, J.-P. Elbers, H. Greißer, I. H. White, R. V. Penty, A. J. Shields // npj Quantum Information. – 2019. – Vol. 5. – P. 101. –DOI: 10.1038/s41534-019-0221-4.

114. Жиляев А.Е. Квантовое распределение ключей для защиты информации в городской сети банкоматов / А.Е. Жиляев, А.С. Николаева // Сборник научных работ участников ежегодной международной молодежной научно-практической конференции в рамках V Международного форума «Как попасть в пятерку?». Москва. – 2018. – С. 161–163.

115. Molotkov S.N. Quantum key distribution through untrusted nodes: exact solution for single-photon states / S.N. Molotkov, I.V. Sinilshchikov // Laser Physics Letters. – 2019. – Vol. 16. – P. 105205.

116. Garsia-Escartin J. Attacking quantum key distribution by light / J. Garsia-Escartin, S. Sajeed, V. Makarov // PLoS ONE. – 2020. – Vol. 15, No. 8. – P. e0236630.

117. Laser seeding attack in quantum key distribution / A. Huang, A. Navarete, S.H. Sun, P. Chaiwongkhot, M. Curty, V. Makarov // Phys. Rev. Applied. – 2019. – Vol.12, Iss.6. –P. 064043. –DOI: 10.1103/PhysRevApplied.12.064043.

118. Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption / A. Huang, S. Sajeed, P. Chaiwongkhot, M. Soucarros, M. Legre, M. Makarov // IEEE Journal of Quantum Electronics. –2016. – Vol. 52, No. 11. – P. 1–11.

119. Р 1323565.1.017-2018 Рекомендации по стандартизации. Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифровании // Москва: Стандартинформ. – 2018.

120. Al-Ghamdi A.B. On the security and confidentiality of quantum key distribution / A.B. Al-Ghamdi, A. Al-Sulami, A.O. Aljahdali // Security and Privacy. – 2020. – Vol. 3, No. 5. – P. e111. –DOI: 10.1002/spy2.111.

121. Arbekov I.M. Criteria of key security // Mat. Vopr. Kriptogr. – 2016. – Vol. 7, No. 1. – P. 39–56.

122. Р 1323565.1.022–2018 Рекомендации по стандартизации. Информационная технология. Криптографическая защита информации. Функции выработки производного ключа //– Москва: Стандартинформю – 2018.

123. Проект методических рекомендаций ТК 26 «Ключевая система полносвязной многоарендаторной сети шифрованной связи на базе ККС ВРК с ДПУ» [Электронный ресурс] // Технический комитет по стандартизации "криптографическая защита инфомрации". – 2021. – Режим доступа: https://tc26.ru/upload/iblock/612/%D0%A2%D0%9A26%D0%9A%D0%A1_%D0%BF%D0%BE%D0%BB%D0%BD%D0%BE%D1%81%D0%B2%D1%8F%D0%B7%D0%BD%D0%B0%D1%8F_v1.pdf, свободный (дата обращения: 07.07.2021).

124. ГОСТ Р ИСО/МЭК 7498-1-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.

125. Коленцова О. Узлы связи: в России построят первую коммерческую квантовую сеть. [Электронный ресурс] // Режим доступа: https://iz.ru/941187/olga-kolentcova/uzly-sviazi-v-rossii-postroiat-pervuiu-kommercheskuiu-kvantovuiu-set, свободный (дата обращения: 20.09.2020)

126. МР 26.4.004-2021 Методические рекомендации. Защищенный протокол взаимодействия квантово-криптографической аппаратуры выработки и распределения ключей и средства криптографической защиты информации. // Москва: Технический комитет по стандартизации «Криптографическая защита информации». –2021

СПИСОК ИЛЛЮСТРАТИВНОГО МАТЕРИАЛА

Список иллюстраций

Список таблиц

ПРИЛОЖЕНИЕ А

(Справочное)

Multilayer Structure of a Scalable Quantum Key Distribution (QKD) Network

PRESENTER: **Andrey** Zhilyaev
Andrey.Zhilyaev@infotecs.ru

AIMS:

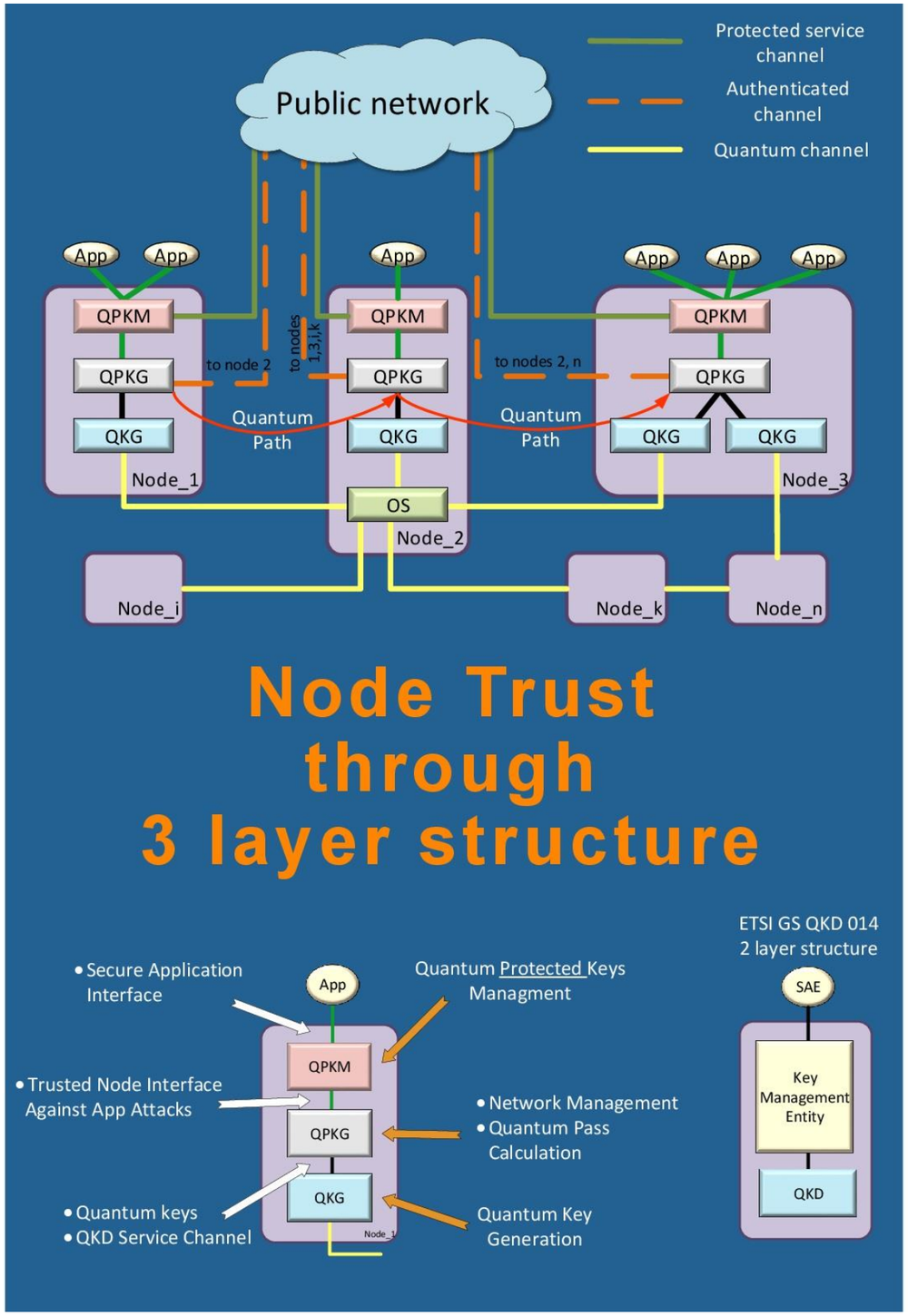
- **Provide** Symmetric keys for application on distance more then 100km
- **Construct** QKD network based on trusted nodes
- **Design** Scalable network easily reconfigurable
- **Clarify** trusted node properties
- **Consider** different QKD devices from different vendors
- **Introduce** term “Quantum Protected Key”

SOLVED PROBLEMS:

1. Quantum key distribution management
2. Quantum channels management
3. Building topology of whole QKD network
4. Quantum Protected Key generation via dynamically calculated *Quantum path*
5. Quantum Protected Keys management
6. Interaction with Secure Application to provide Quantum Protected Keys
7. Trust of Trusted node clarified

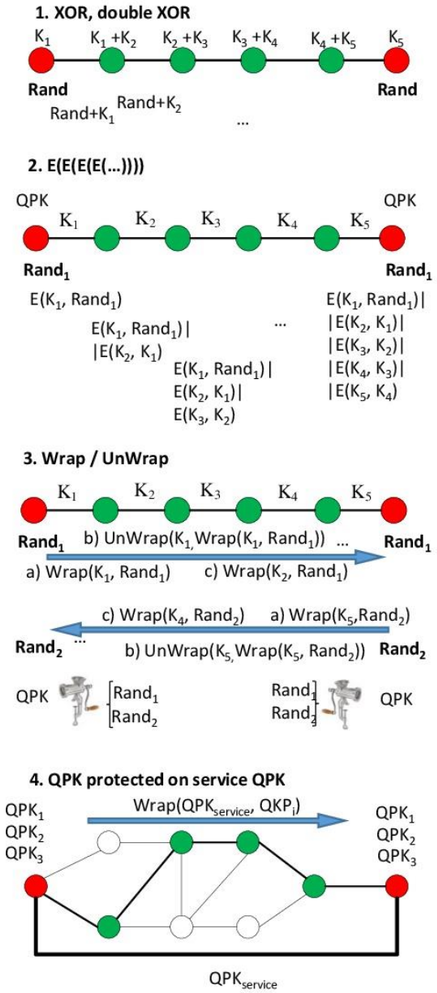
RESULTS:

- Concept of Scalable multipoint network with quantum key distribution
- Automatic management of Quantum channels
- Automatic Quantum Protected keys generation
- 3 Layer structure of Trusted Node provides protection against APP attacks
- Different methods to generated Quantum Protected Keys for different cases



Quantum Protected Key Generation

- In case of low Key Rate
- Data bigger then quantum key
- Both participants are equal
- Related-key attack protection



Andrey Zhilyaev,
Anastasiia Nikolaeva,
Mikhail Borodin and
Vladimir Sergeev

infotecs

Рисунок А.1 – Иллюстрация к докладу на конференции QCrypt-2019

On Key Generation Schemes with QKD for applications

PRESENTER: **Andrey** Zhilyaev
Andrey.Zhilyaev@infotecs.ru

Problems:

- QKD protocol consumes keys to generate quantum keys (QK)
- Some systems further use quantum keys to generate working keys (K)
- What is the best way to use one keys to generate another keys and improve the key stream properties?

Our Proposal:

- The hybridization of quantum keys and classical pre-shared keys to construct the optimal key generation and distribution scheme (KGDS)
- Use the best properties of both classic and quantum key generation schemes
- Computation secure MAC can be used for QKD authentication for low speed QKD devices

Approach to analyze KGDS:

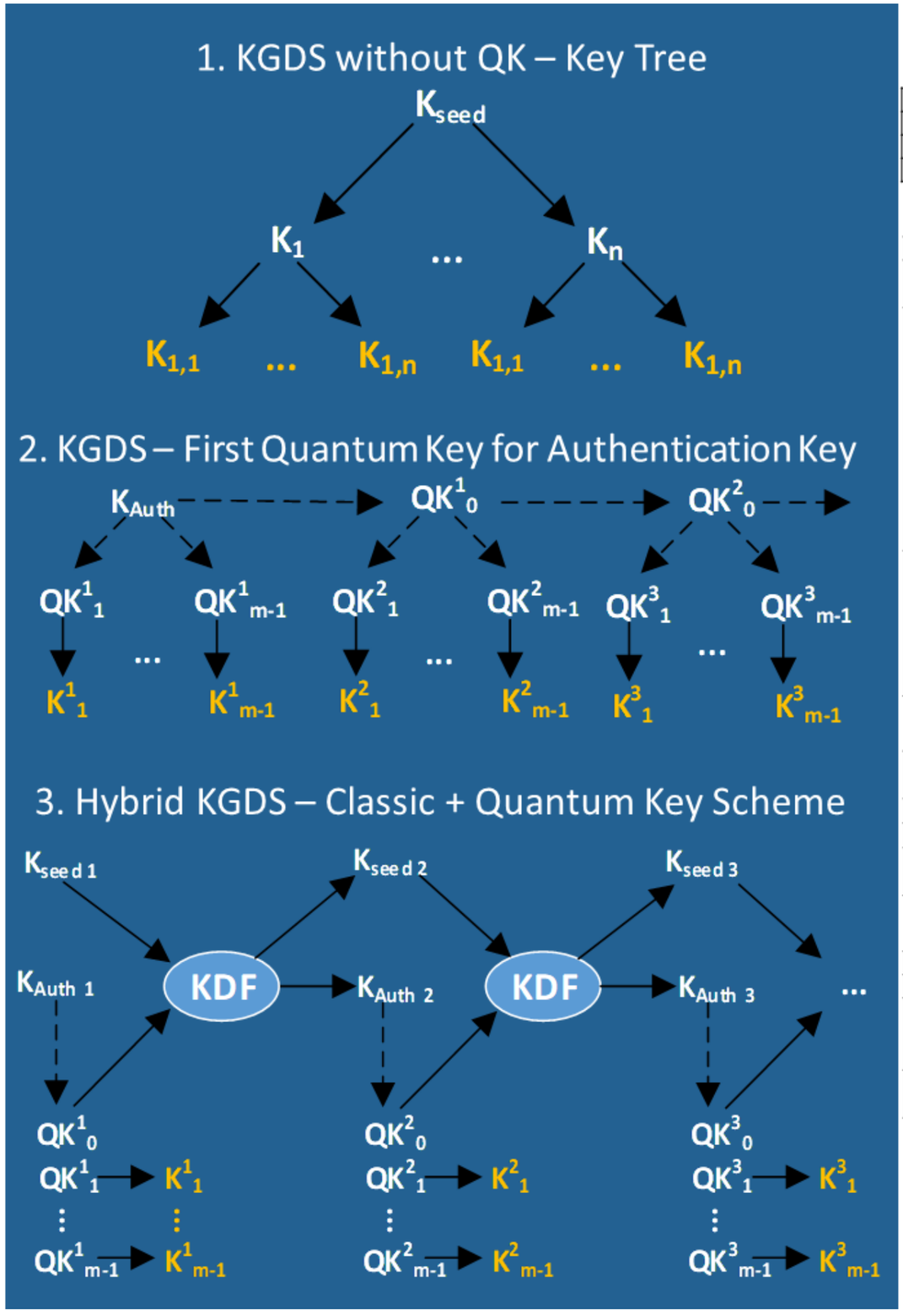
- **Cryptographic properties**
  - Impersonation attack on Authentication key
  - Known-text attack on Authentication key
  - Known text attack on Working key
  - An influence of an untrusted courier
  - Consequences of the attacks
- **Operational properties**
  - Initialization problems
  - Key storage problems
  - Key synchronization problems

Hybrid KGDS Advantages:

- Perfect forward secrecy can be achieved
- Hybrid Schemes more resistant against considered attacks
- An adversary have limited time to perform an attack
- Partial compromise of generated keys
- An untrusted courier have significantly complicated attack conditions

Wherein

- MAC length must be at least equal to the length of the key
- Order of QK usage is important
- Loss of the key synchronization may lead to irreversible problems



Key Generation and Distribution Schemes

Perfect Forward Secrecy Property

KGDS	**Perfect forward secrecy**
Without QK	No
QK for KAuth	Yes
Hybrid KQDS	Yes

Key Compromise Consequences

KGDS	**Key Compromise**
Without QK	Compromise of one derived key compromise all keys
QK for KAuth	• Compromise of QK used for K_{Auth} compromises all QK generated with authentication on this K_{Auth} • Compromise of K_{Auth} before first QKD session on this K_{Auth} compromises all keys • Compromise of K_{Auth} after first QKD session on this K_{Auth} compromises all QK generated with authentication on this K_{Auth}
Hybrid KGDS	• Compromise of K_{Auth} compromises all QK generated with authentication on this K_{Auth} • Compromise of K_{seed} and QK_0 (or K_{Auth}) compromises all keys except previous generated QK

Best Attack Probabilities

KGDS	**MAC length 128 bit**	**MAC length 256 bit**
Without QK	2^{-199}	2^{-199}
QK for K_{Auth}	2^{-125}	2^{-215}
Hybrid Scheme	2^{-125}	2^{-215}

Best Attack Consequences

KGDS	**Best attack consequences**
Without QK	All keys are compromised
QK for K_{Auth}	All further keys are compromised. Already generated keys stay secret
Hybrid Scheme	Only keys generated with authentication on recovered K_{Auth}

Mikhail Borodin,
Alexey Urivskiy and
Andrey Zhilyaev
infotecs

Рисунок А.2 – Иллюстрация к докладу на конференции QCrypt-2020

ПРИЛОЖЕНИЕ Б
АКТЫ ВНЕДРЕНИЯ

УТВЕРЖДАЮ
Декан физического факультета
МГУ имени М.В.Ломоносова,
директор Центра квантовых технологий,
профессор Н.Н.Сысоев
08 апреля 2022г.

Акт

о внедрении результатов диссертационной работы
Жиляева Андрея Евгеньевича

Комиссия в составе: председателя – проф. С.П. Кулика и членов комиссии: проф. С.Н. Молоткова, в.н.с. К.С. Кравцова, доцента Ю.В. Владимировой.

Результаты диссертационного исследования А.Е. Жиляева «Методика построения сетей квантового распределения ключей смешанной топологии», представленной на соискание ученой степени кандидата технических наук, используются в учебном процессе МГУ имени М.В. Ломоносова на физическом факультете при чтении курсов: «Квантовая обработка информации и квантовые технологии» (лектор проф. С.П. Кулик), «Квантовая криптография» и «Протоколы квантовой криптографии: от теории к практике» (лектор проф. С.Н. Молотков) для подготовки специалистов, обучающихся в рамках магистерской программы «Прикладная квантовая связь».

В курсах «Квантовая криптография» и «Протоколы квантовой криптографии: от теории к практике» используются результаты А.Е. Жиляева по разработке методики построения сетей КРК смешанной топологии.

В курсе повышения квалификации «Квантовая обработка информации и квантовые технологии» используются результаты А.Е. Жиляева по разработке методики распределения квантовозащищенных ключей в сетях КРК магистральной топологии.

На территории МГУ имени М.В. Ломоносова развернута Университетская квантовая сеть, построенная по методике, предложенной в работе А.Е. Жиляева. Внедрение методики позволило сократить время развертывания сети на 20%.

Члены комиссии:

профессор, д.ф.-м.н.	С.П. Кулик
профессор, д.ф.-м.н.	С.Н. Молотков
в.н.с., к.ф.-м.н.	К.С. Кравцов
доцент, к.ф.-м.н.	Ю.В. Владимирова

Акционерное общество
«Информационные технологии
и коммуникационные системы»
(**АО «ИнфоТеКС»**)

Юридический адрес: улица Мишина,
дом 56, стр.2, этаж 2, пом. IX, комната 29
Москва, 127083

Почтовый адрес: а/я № 80,
улица Отрадная, дом 2Б, стр. 1
Москва, 127273
Тел. (495)737-61-92 Факс (495)737-72-78
e-mail: soft@infotecs.ru

ОГРН 1027739185066
ИНН/КПП 7710013769/771401001
http://www.infotecs.ru

20 АПР 2022 № И-2022-0409

На №.....от.....

УТВЕРЖДАЮ

Генеральный директор
АО «ИнфоТеКС»

_____ А.А. Напчаев

«20» апреля 2022 г.

АКТ
о внедрении результатов диссертационной работы Жиляева А.Е. в деятельность АО «ИнфоТеКС» при разработке квантового-криптографических средств выработки и распределения ключей

Комиссия в составе: председатель – руководитель Центра научных исследований и перспективных разработок Елисеев В.Л., к.т.н., и членов комиссии: заместитель директора Центра разработок программных продуктов Поташников А.В., к.ф.-м.н., исследователь Центра научных исследований и перспективных разработок Попов В.Г., к.ф.-м.н. составила настоящий Акт о том, что результаты диссертационной работы Жиляева А.Е. «Методика построения сетей квантового распределения ключей смешанной топологии», представленной на соискание ученой степени кандидата технических наук, внедрены в деятельность АО «ИнфоТеКС» в процессе создания средств защиты информации с использованием систем квантового распределения ключей.

Комиссия установила, результаты диссертационной работы применены:

— При разработке комплекса ViPNet Quandor, выполненной в рамках проекта 03.G25.31.0254 при финансовой поддержке Министерства образования и науки Российской Федерации, реализованы способ построения классического аутентифицированного канала между сервером КРК и клиентом КРК из состава комплекса, а также способ его

взаимодействия со средством криптографической защиты основаны на соответствующих положениях работы Жиляева А.Е.

— При разработке системы ViPNet QSS в основу ключевой системы QSS Server и QSS Point положена методика распределения квантовозащищенных ключей в сети КРК магистральной топологии, адаптированная Жиляевым А.Е. для сети топологии «звезда».

— В основу комплексного проекта "Разработка технологии и аппаратуры сетей квантового распределения криптографических ключей с использованием доверенных узлов", выполняемого по соглашению с Министерством промышленности и торговли РФ № 020-11-2019-933 от 19.11.2019 положена многоуровневая структура сети КРК и методика построения сетей КРК смешанной топологии, предложенная Жиляевым А.Е. Внедрение методики позволило ускорить процесс эскизного проектирования аппаратуры на 15% и унифицировать аппаратную платформу узлов сети КРК.

Председатель комиссии: _____/Елисеев В.Л./

Члены комиссии _____/Поташников А.В./

_____/Попов В.Г./

УТВЕРЖДАЮ

Ответственный секретарь

Технического комитета по стандартизации

«Криптографическая защита информации» (ТК 26),

Генеральный директор АО «ИнфоТеКС»*

_____ А.А. Чапчаев

«___» _____ 2022 г.

Акт

о внедрении результатов диссертационной работы Жиляева А.Е.
в документы национальной системы стандартизации в области защиты информации

Комиссия в составе: председатель – заместитель ответственного секретаря ТК26 Уривский А.В., к.ф-м.н., и членов комиссии: руководитель аппарата секретариата ТК26 Пискунов М.Б., к.т.н., ведущий специалист Линник Е.В.

составила настоящий Акт о том, что результаты диссертационной работы Жиляева А.Е. «Методика построения сетей квантового распределения ключей смешанной топологии», представленной на соискание ученой степени кандидата технических наук, использованы при разработке проекта методических рекомендаций ТК 26.

Комиссия установила, что в проекте методических рекомендаций ТК 26 «Информационная технология. Криптографическая защита информации. Ключевая система полносвязной многоарендаторной сети шифрованной связи на базе ККС ВРК с ДПУ» ключевая система сети связи основана на методике распределения квантовозащищенных ключей в сети магистральной топологии, предложенной Жиляевым А.Е.

Внедрение методики позволило сократить процесс разработки проекта методических рекомендаций на 30%. В дальнейшем полученные наработки

будут использованы в разработке документов национальной системы стандартизации, которые включены в программу национальной системы стандартизации, шифр задания 1.11.026-1.021

*Примечание: Приказом Федерального агентства по техническому регулированию и метрологии «Об организации деятельности технического комитета по стандартизации «Криптографическая защита информации» от 09.06.2017 № 1319дсп, на АО «ИнфоТеКС» возложены функции по ведению секретариата технического комитета по стандартизации.

Председатель комиссии: _____ /Уривский А.В./

Члены комиссии _____ /Пискунов М.Б./

_____ /Линник Е.В./

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«Системы практической безопасности»
ОКПО 59492613, ОГРН 1147847303867, ИНН 7802869750, КПП 780201001
194021, г. Санкт-Петербург, ул. Политехническая, д. 22, литера А,
помещение 1-Н, офис 298
тел./факс: +7 (812) 468-15-61, e-mail: info@systempb.ru

УТВЕРЖДАЮ

Генеральный директор
ООО «Системы практической безопасности»
_____ Д. Л. Смирнов
«__» _____ 2022 г.

АКТ
о внедрении результатов диссертационной работы
«Методика построения сетей квантового распределения ключей
смешанной топологии»
Жиляева Андрея Евгеньевича

Комиссия в составе: председателя – заместитель генерального директора по НТР Мареева Е.В., и членов комиссии: технический директор Александров С.В руководитель направления, кандидат физико-математических наук Емельянов В. М., руководитель отдела системных исследований Герасимова А.Г., составила настоящий Акт о том, что результаты диссертационной работы Жиляева А. Е., представленной на соискание ученой степени кандидата технических наук, внедрены в деятельность ООО «СПБ» в процессе работы над средством криптографической защиты информации, сопряженным с системой квантового распределения ключей (изделие «Квазар-СКР»).

Комиссия установила, что при разработке решения для протяженных квантовых сетей на базе изделия «Квазар-СКР» использована методика распределения квантовозащищенных ключей (КЗК) в магистральной сети.

Применение указанной методики позволило:

– повысить безопасность изделия за счет использования в нем ключей, полученных с помощью функции гибридизации двух компонент, переданных в составе ключевых контейнеров по независимым каналам связи;

– улучшить протяженность транспортного канала изделия пропорционально количеству сопряженных с ним пар узлов квантовой сети;

– сократить на 50% время ожидания изделием одной из компонент формирования КЗК в случае сопряжения с системой квантового распределения ключей, использующей метод коммутативных функций.

Председатель комиссии: _____ /Е. В. Мареева/

Члены комиссии: _____ /С. В. Александров/

_____ /В. М. Емельянов/

_____ /А. Г. Герасимова/

ПРИЛОЖЕНИЕ В
ПАТЕНТЫ НА ИЗОБРЕТЕНИЯ РФ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ

№ 2736870

Комплекс для защищенной передачи данных в цифровой сети передачи данных с использованием однопроходной системы квантового распределения ключей и способ согласования ключей при работе комплекса

Патентообладатель: ***Открытое акционерное общество "Информационные технологии и коммуникационные системы" (RU)***

Авторы: ***Втюрина Анна Георгиевна (RU),***
Жиляев Андрей Евгеньевич (RU)

Заявка № **2019144324**

Приоритет изобретения **27 декабря 2019 г.**

Дата государственной регистрации в Государственном реестре изобретений Российской Федерации **23 ноября 2020 г.**

Срок действия исключительного права на изобретение истекает **27 декабря 2039 г.**

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 736 870**(13) **C1**

(51) МПК
H04L 9/08 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 9/08 *(2020.08);* ***H04L 9/0852*** *(2020.08);* ***G06F 21/72*** *(2020.08)*

(21)(22) Заявка: **2019144324, 27.12.2019**

(24) Дата начала отсчета срока действия патента:
27.12.2019

Дата регистрации:
23.11.2020

Приоритет(ы):
(22) Дата подачи заявки: **27.12.2019**

(45) Опубликовано: **23.11.2020** Бюл. № **33**

Адрес для переписки:
127287, Москва, Старый Петровско-Разумовский пр-д, 1/23, стр. 1, Открытое акционерное общество "Информационные технологии и коммуникационные системы"

(72) Автор(ы):
Втюрина Анна Георгиевна (RU),
Жиляев Андрей Евгеньевич (RU)

(73) Патентообладатель(и):
Открытое акционерное общество "Информационные технологии и коммуникационные системы" (RU)

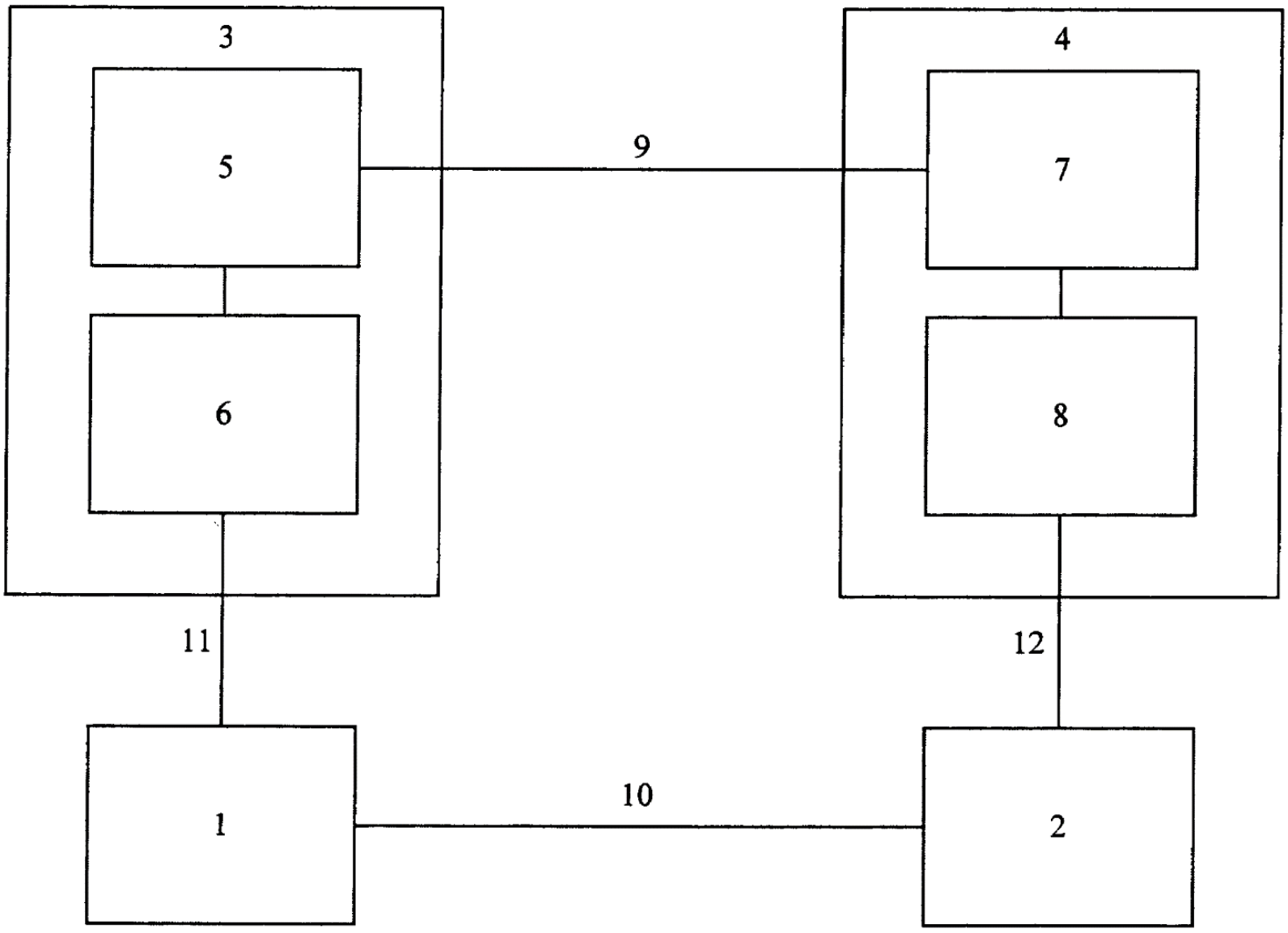
(56) Список документов, цитированных в отчете о поиске: **KZ 27358 A4, 16.09.2013. RU 2708511 C1, 09.12.2019. RU 2621605 C2, 06.06.2017. US 20180191496 A1, 05.07.2018. RU 2454810 C1, 27.06.2012.**

(54) Комплекс для защищенной передачи данных в цифровой сети передачи данных с использованием однопроходной системы квантового распределения ключей и способ согласования ключей при работе комплекса

(57) Реферат:

Изобретение относится к защите информации. Технический результат заключается в повышении защищенности передаваемых пользовательских данных, в повышении надежности комплекса, в повышении стойкости квантовых ключей, вырабатываемых системой квантового распределения ключей (КРК), за счет аутентификации служебных данных системы КРК на ключах аутентификации, сформированных из квантовых ключей, и аутентификации служебных данных системы КРК целиком, до разбиения на блоки, используемые при передаче по цифровой линии связи, и последующего шифрования служебных данных системы КРК. В комплексе используется транспортная линия связи, соединяющая два шифратора и два узла системы КРК. Канал передачи системы КРК состоит из аутентифицированного с использованием квантовых ключей канала передачи служебной информации и квантовых ключей из приемного узла системы КРК в сопряженный шифратор и обратно, аутентифицированного с использованием квантовых ключей канала передачи пользовательских данных между шифраторами, аутентифицированного с использованием квантовых ключей канала передачи служебной информации и квантовых ключей из передающего узла системы КРК в сопряженный шифратор и обратно. 2 н.п. ф-лы, 1 ил.

RU 2736870 C1



RU 2736870 C1

RU 2736870 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 736 870**(13) **C1**

(51) Int. Cl.
H04L 9/08 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 9/08 *(2020.08);* ***H04L 9/0852*** *(2020.08);* ***G06F 21/72*** *(2020.08)*

(21)(22) Application: **2019144324, 27.12.2019**

(24) Effective date for property rights:
27.12.2019

Registration date:
23.11.2020

Priority:
(22) Date of filing: **27.12.2019**

(45) Date of publication: **23.11.2020** Bull. № **33**

Mail address:
127287, Moskva, Staryj Petrovsko-Razumovskij pr-d, 1/23, str. 1, Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy"

(72) Inventor(s):
Vtyurina Anna Georgievna (RU),
Zhilyaev Andrej Evgenevich (RU)

(73) Proprietor(s):
Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy" (RU)

RU 2736870 C1

(54) COMPLEX FOR SECURE DATA TRANSMISSION IN DIGITAL DATA NETWORK USING SINGLE-PASS QUANTUM KEY DISTRIBUTION SYSTEM AND METHOD OF KEYS ADJUSTMENT DURING OPERATION OF SYSTEM

(57) Abstract:

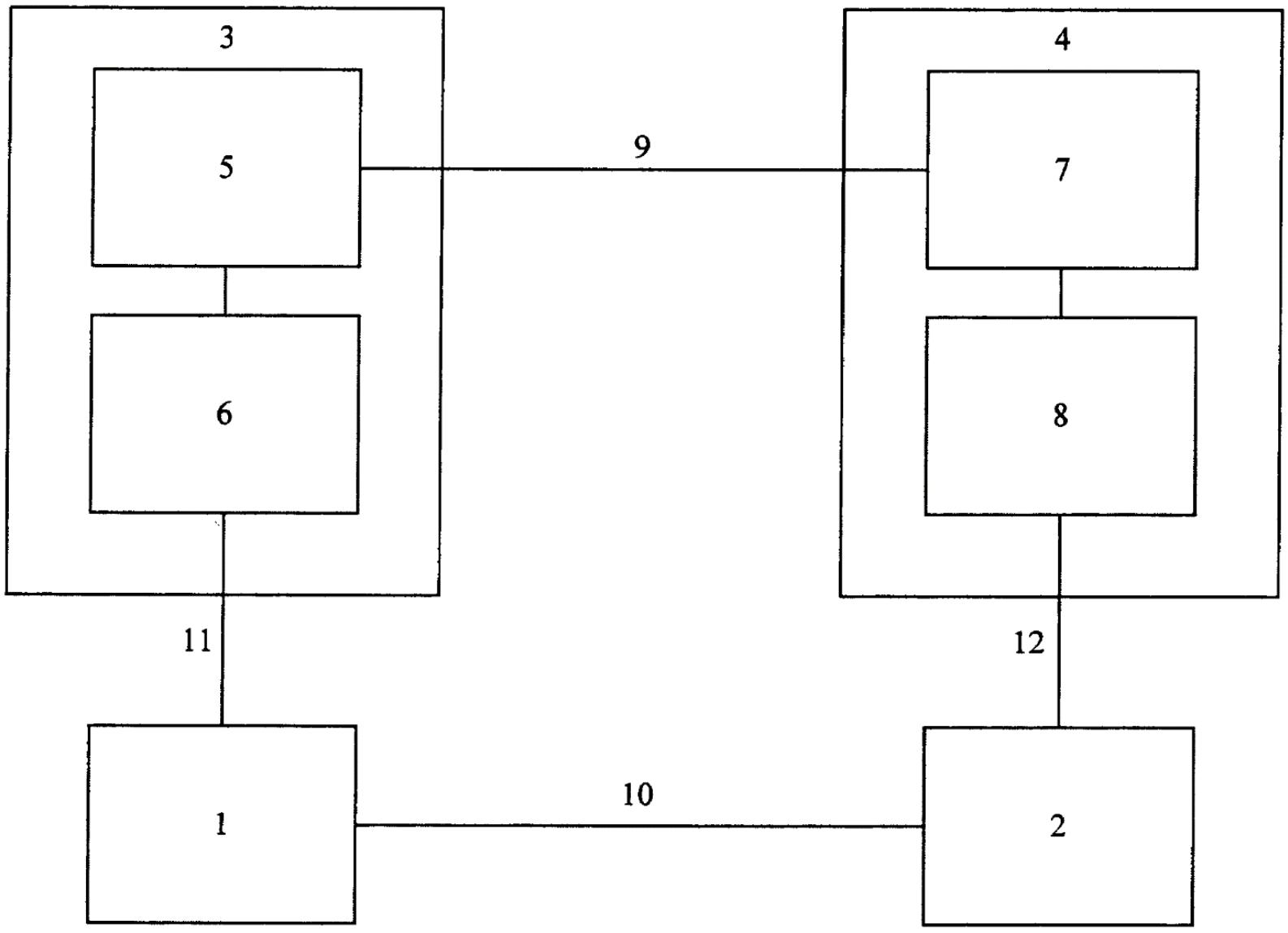
FIELD: physics.

SUBSTANCE: invention relates to information protection. Complex employs a transport communication line connecting two encoders and two QKD system units. Channel for transmitting an QKD system consists of a service information service channel authenticated using quantum keys and quantum keys from the receiving system of the QKD system to the conjugate encoder and back, authenticated using the quantum keys of the user data transmission channel between the encoders, authenticated using quantum keys of channel of service information transmission and quantum keys from transmitting node of QKD system to conjugate encoder and back.

EFFECT: high security of transmitted user data, high reliability of the complex, high durability of quantum keys generated by the quantum key distribution system (QKD), due to authentication of QKD system service data on authentication keys formed from quantum keys, and authentication of service data of the QKD system as a whole, before breaking down into blocks used when transmitting over a digital communication line, and subsequent encryption of service data of the QKD system.

2 cl, 1 dwg

RU 2736870 C1



RU 2736870 C1

RU 2736870 C1

Область техники, к которой относится изобретение

Предполагаемое изобретение относится к области криптографической защиты информации и передачи данных, а более конкретно, системам криптографической защиты информации, использующим для повышения защищенности передаваемой информации ключи, получаемые из квантовых ключей от сопряженной системы квантового распределения ключей.

Уровень техники

Для защиты передаваемой информации в цифровых сетях передачи данных перспективным является использование систем квантового распределения ключей (КРК). Использование квантово-криптографической аппаратуры защиты информации может обеспечить доставку абонентам симметричного ключа для зашифрования и расшифрования передаваемых пользовательских данных, а также оперативную замену ключа в соответствии с требованиями безопасности.

Известен способ и устройство для передачи информации с использованием технологии КРК (заявка США №20180054304, приоритет от 19.08.2016 г.), в котором коммуникационное устройство состоит из модуля загрузки, модуля контроля потока и модуля криптографической обработки, а способ предусматривает передачу и использование ключей в устройстве. Модуль загрузки предоставляет криптографические ключи, полученные с помощью технологии КРК. В случае, если при получении данных коммуникационным устройством отсутствует криптографический ключ, модуль контроля потока выполняет одно из трех действий: отбрасывает (удаляет данные), сохраняет данные в буфер или добавляет к данным метку, что криптографический ключ не был предоставлен, с последующей передачей данных в модуль криптографической обработки. При получении данных от модуля контроля потока модуль криптографической обработки производит криптографическую обработку (зашифрование) данных с использование криптографического ключа.

С помощью данного устройства реализуется система передачи информации, состоящая из устройств генерации, производящих криптографические ключи с помощью технологии КРК, и коммуникационных устройств, описанных выше.

Данное устройство и способ имеют следующие недостатки.

Если в течении продолжительного промежутка времени отсутствует криптографический ключ, то защищенная передача данных прерывается. При этом отбрасывание данных может быть недопустимым в силу характера передаваемых данных, а размер буфера для данных, ожидающих ключа - ограниченным, то есть выполнение первого действия модулем контроля потока может быть запрещено, а выполнение второго невозможно из-за заполненного буфера данных.

Ключи, передаваемые в два коммуникационных устройства системы, в общем случае могут быть различны из-за непредвиденных ошибок. Однако проверка на идентичность загружаемых ключей не производится, как и контроль использования одного и того же ключа для зашифрования и расшифрования данных, что может привести к невозможности расшифрования в одном коммуникационном устройстве данных, зашифрованных на другом ключе в другом коммуникационном устройстве. Таким образом, становится невозможно выполнение устройством своего функционального предназначения по передаче информации.

Известен способ аутентификации и устройство для его осуществления для системы квантовой криптографии (заявка США №20190238326, приоритет от 29.01.2018 г.); способ заключается в сравнении последовательностей, переданных по квантовому каналу передачи в позициях совпадающих базисов.

Этот способ имеет следующий недостаток: аутентифицируются непосредственно устройства квантовой криптографии, но не данные, передаваемые в процессе выработки квантового ключа, а именно: служебные сообщения по согласованию базисов измерений, исправлению ошибок и этапа усиления секретности. Таким образом, не гарантируется целостность и аутентичность этих служебных данных, и нарушитель может осуществить атаку «человек посередине», встроившись в квантовый и классический канал системы КРК и навязывая служебный трафик.

Также известен способ и устройство для шифрования с использованием технологии КРК (заявка США №20050063547, приоритет от 03.05.2004 г.), в котором устройство состоит

• из первого и второго получающего/передающего узла, соединенных соответственно с первым и вторым зашифровывающим/расшифровывающим процессором;

• первой и второй станции КРК, соединенных соответственно с первым и вторым зашифровывающим/расшифровывающим процессором и адаптированных для обмена квантовыми ключами и передачи их в первый и второй зашифровывающий/ расшифровывающий процессоры;

• первым и вторым узлами классического распределения ключей, соединенных соответственно с первым и вторым зашифровывающим/расшифровывающим процессором и адаптированных к обмену классическими ключами и передачи классических ключей в первый и второй зашифровывающий/расшифровывающий процессор.

Зашифровывающий/расшифровывающий процессоры адаптированы для получения сигналов от одной получающей/передающей станции; зашифрования сигналов с использованием сессионного ключа, полученного в зашифровывающем/ расшифровывающем процессоре путем сложения операцией XOR квантового и классического ключа; передачи зашифрованного сигнала на другую получающую/ передающую станцию.

В устройстве реализуется способ передачи зашифрованных сигналов между первой и второй приемной/передающей станциями, включающий:

• передачу первого открытого сигнала с первой приемной/передающей станции на первый зашифровывающий/зашифровывающий процессор классической системы шифрования, содержащей также второй зашифровывающий/расшифровывающий процессор,

• обмен квантовыми ключами между первым и вторым узлом КРК системы КРК и предоставление квантовых ключей первому и второму зашифровывающему/ расшифровывающему процессору,

• обмен классическими ключами между первой и второй классическими станциями и предоставление классических ключей первому и второму зашифровывающему/ расшифровывающему процессору,

• формирование сессионного ключа путем сложения операцией XOR полученных классического и квантового ключа,

• формирование зашифрованного сигнала из первого открытого сигнала на первом зашифровывающем/расшифровывающем процессоре с использованием сессионного ключа, сформированного на первом процессоре,

• формирование расшифрованного сигнала из зашифрованного сигнала, полученного от первого зашифровывающего/расшифровывающего процессора на втором зашифровывающем/расшифровывающем процессоре с использованием сессионного ключа, сформированного на втором процессоре,

• передачу второго открытого сигнала на вторую приемную/передающую станцию.

Известное устройство и способ выбраны в качестве прототипов.

Однако известное техническое решение имеет ряд недостатков.

Контроль идентичности используемых ключей (квантовых и классических) в зашифровывающем/расшифровывающем процессорах производится передачей идентификаторов ключей в открытом виде по линии связи между процессорами, что может вызвать навязывание использования различных сессионных ключей для зашифрования и расшифрования сигнала в процессоре.

Применение в изобретении внешнего источника классических ключей в целях частого распределения ключей требует использования технологий, основанных на ассиметричной криптографии, что приводит к увеличению рисков компрометации распределяемых ключей.

Недостатком изобретения является также наличие отдельных каналов взаимодействия для системы КРК и системы обмена классическими ключами, что повышает затраты на создание и развертывание устройства.

Раскрытие сущности изобретения

Техническим результатом является:

1) повышение защищенности передаваемых пользовательских данных;

2) повышение надежности комплекса, в том числе в случае искажений (случайных или преднамеренных), вносимых локальной линией связи; в случае непредвиденных или преднамеренных кратковременных сбоев системы КРК, выражающихся во временном прекращении генерации квантовых ключей; в случае низкой скорости генерации квантовых ключей и/или генерации квантовых ключей малой длины; а также в случае навязывания ложных идентификаторов ключей;

3) снижение затрат на создание, развертывание и эксплуатацию комплекса за счет уменьшения числа классических линий связи;

4) повышение стойкости квантовых ключей, вырабатываемых системой КРК, за счет аутентификации служебных данных системы КРК на ключах аутентификации, сформированных из квантовых ключей, и аутентификации служебных данных системы КРК целиком, до разбиения на блоки, используемые при передаче по цифровой линии связи, и последующего шифрования служебных данных системы КРК.

Для этого предлагается комплекс для защищенной передачи данных в цифровой сети передачи данных с использованием однопроходной системы квантового распределения ключей, имеющий в составе

• передающий узел системы квантового распределения ключей (КРК), включающий
  ○ передающий модуль выработки квантовых ключей, о модуль согласования ключей передающего узла;
  ○ приемный узел системы КРК, включающий
• приемный модуль выработки квантовых ключей, о модуль согласования ключей приемного узла;
• 1-й шифратор, связанный с модулем согласования ключей передающего узла;
• 2-й шифратор, связанный с модулем согласования ключей приемного узла;

причем

• передающий модуль выработки квантовых ключей связан с приемным модулем выработки квантовых ключей квантовой линией связи, выполненной в виде оптоволоконной линии;
• 1-й шифратор связан со 2-м шифратором транспортной линией связи, выполненной в виде цифровой сети передачи данных;

• 1-й шифратор связан с модулем согласования ключей передающего узла посредством 1-й локальной линии связи (1-я ЛС);

• 2-й шифратор связан с модулем согласования ключей приемного узла посредством 2-й локальной линии связи (2-я ЛС);

• 1-й шифратор связан с внешней цифровой сетью передачи данных;

• 2-й шифратор связан с внешней цифровой сетью передачи данных; при этом

• передающий модуль выработки квантовых ключей выполнен с возможностью

○ генерировать случайные числа,

○ формировать квантовые информационные состояния,

○ отправлять квантовые информационные состояния по квантовой линии связи в приемный модуль выработки квантовых ключей,

○ вырабатывать квантовые ключи совместно с приемным модулем выработки квантовых ключей путем обработки информации, полученной из квантовых информационных состояний;

• модуль согласования ключей передающего узла выполнен с возможностью

○ формировать ключи аутентификации и ключи шифрования на основе квантовых ключей,

○ согласовывать ключи аутентификации и ключи шифрования с ключами аутентификации и ключами шифрования, сформированными модулем согласования ключей приемного узла,

○ принимать данные из 1-го шифратора по 1-й ЛС,

○ передавать данные в 1-й шифратор по 1-й ЛС;

• приемный модуль выработки квантовых ключей выполнен с возможностью

○ генерировать случайные числа,

○ принимать квантовые информационные состояния по квантовой линии связи из передающего модуля выработки квантовых ключей,

○ обрабатывать квантовые информационные состояния,

○ вырабатывать квантовые ключи совместно с передающим модулем выработки квантовых ключей путем обработки информации, полученной из квантовых информационных состояний;

• модуль согласования ключей приемного узла выполнен с возможностью

○ формировать ключи аутентификации и ключи шифрования на основе квантовых ключей,

○ согласовывать ключи аутентификации и ключи шифрования с ключами аутентификации и ключами шифрования, сформированными модулем согласования ключей передающего узла,

○ принимать данные из 2-го шифратора по 2-й ЛС,

○ передавать данные во 2-й шифратор по 2-й ЛС;

• 1-й шифратор выполнен с возможностью

○ принимать ключи шифрования и служебные данные из модуля согласования ключей передающего узла по 1-й ЛС,

○ передавать служебные данные в модуль согласования ключей передающего узла по 1-й ЛС,

○ принимать данные из внешней цифровой сети передачи данных,

○ зашифровывать данные, поступившие в него по внешней цифровой сети передачи данных или по 1-й ЛС, с использованием ключей шифрования,

- передавать данные, зашифрованные с использованием ключей шифрования, по транспортной линии связи,
- расшифровывать данные, поступившие из транспортной линии связи, с использованием ключей шифрования,
- передавать данные во внешнюю цифровую сеть передачи данных;

• 2-й шифратор выполнен с возможностью

- принимать ключи шифрования и служебные данные из модуля согласования ключей приемного узла по 2-й ЛС,
- передавать служебные данные в модуль согласования ключей приемного узла по 2-й ЛС,
- принимать данные из внешней цифровой сети передачи данных,
- зашифровывать данные, поступившие в него по внешней цифровой сети передачи данных или по 2-й ЛС, с использованием ключей шифрования,
- передавать данные, зашифрованные с использованием ключей шифрования, по транспортной линии связи,
- расшифровывать данные, поступившие из транспортной линии связи, с использованием ключей шифрования,
- передавать данные во внешнюю цифровую сеть передачи данных.

Предлагается также способ согласования ключей при работе комплекса, заключающийся в том, что

• выбирают квантовый протокол;

• выбирают размер блока равным b, где b кратно степени целого числа 2;

• выбирают размер ключа шифрования равным n блоков;

• выбирают размер ключа аутентификации равным m блоков;

• выбирают минимальный объем накопленного квантового ключа равным Key=m+n блоков;

• устанавливают значение счетчика ключей аутентификации в модуле согласования ключей передающего узла M1=1;

• устанавливают значение счетчика ключей аутентификации в модуле согласования ключей приемного узла M2=2;

• устанавливают значение счетчика ключей шифрования в модуле согласования ключей передающего узла N1=1;

• устанавливают значение счетчика ключей шифрования в модуле согласования ключей приемного узла N2=2;

• формируют текущий ключ аутентификации размером m блоков, выполняя следующие действия:

- добавляют к ключу аутентификации идентификатор в виде блока данных, содержащий значение счетчика M1 и значение признака ключа аутентификации;
- увеличивают значение счетчика M1 на 1;

• формируют текущий ключ шифрования размером n блоков, выполняя следующие действия:

- добавляют к ключу шифрования идентификатор в виде блока данных, содержащий значение счетчика N1 и значение признака ключа шифрования;
- увеличивают значение счетчика N1 на 1;

• загружают текущий ключ аутентификации в модули согласования ключей приемного и передающего узла;

• загружают текущий ключ шифрования в 1-й и 2-й шифраторы;

• (А) накапливают квантовые ключи в модулях согласования ключей передающего и приемного узлов системы КРК, выполняя следующие действия:

○ (Б) вырабатывают квантовый ключ в передающем и приемном модулях выработки квантовых ключей согласно выбранному квантовому протоколу, причем в ходе выполнения квантового протокола в части передачи служебных данных от передающего к приемному модулю выработки квантового ключа выполняют следующие действия:

■ формируют служебное сообщение из служебных данных в передающем модуле выработки квантовых ключей;

■ передают служебные данные из передающего модуля выработки квантовых ключей в модуль согласования ключей передающего узла;

■ осуществляют аутентификацию служебного сообщения с помощью текущего ключа аутентификации в модуле согласования ключей передающего узла;

■ передают аутентифицированное служебное сообщение по 1-й ЛС в 1-й шифратор;

■ зашифровывают аутентифицированное служебное сообщение с помощью текущего ключа шифрования в 1-м шифраторе;

■ передают зашифрованное аутентифицированное служебное сообщение во 2-й шифратор через транспортную линию связи;

■ расшифровывают зашифрованное аутентифицированное служебное сообщение во 2-м шифраторе с помощью текущего ключа шифрования;

■ передают аутентифицированное служебное сообщение из 2-го шифратора в модуль согласования ключей приемного узла по 2-й ЛС;

■ проверяют аутентичность полученного служебного сообщения с помощью текущего ключа аутентификации в модуле согласования ключей приемного узла, причем если проверка аутентичности успешна, то

➢ передают служебное сообщение из модуля согласования ключей приемного узла в приемный модуль выработки квантовых ключей;

иначе

➢ сигнализируют о неуспешной аутентификации;

➢ переходят к этапу Б;

○ в ходе выполнения квантового протокола в части передачи служебных данных от приемного к передающему модулю выработки квантового ключа выполняют следующие действия:

■ формируют служебное сообщение из служебных данных в приемном модуле выработки квантовых ключей;

■ передают служебные данные из приемного модуля выработки квантовых ключей в модуль согласования ключей приемного узла;

■ осуществляют аутентификацию служебного сообщения с помощью текущего ключа аутентификации в модуле согласования ключей приемного узла;

■ передают аутентифицированное служебное сообщение по 2-й ЛС во 2-й шифратор;

■ зашифровывают аутентифицированное служебное сообщение с помощью текущего ключа шифрования во 2-м шифраторе;

■ передают зашифрованное аутентифицированное служебное сообщение в 1-й шифратор через транспортную линию связи;

■ расшифровывают зашифрованное аутентифицированное служебное сообщение в 1-м шифраторе с помощью текущего ключа шифрования;

■ передают аутентифицированное служебное сообщение из 1-го шифратора в модуль

согласования ключей передающего узла по 1-й ЛС;

■ проверяют аутентичность полученного служебного сообщения с помощью текущего ключа аутентификации в модуле согласования ключей передающего узла, причем если проверка аутентичности успешна, то

➢ передают служебное сообщение из модуля согласования ключей передающего узла в передающий модуль выработки квантовых ключей;

иначе

➢ сигнализируют о неуспешной аутентификации;

➢ переходят к этапу Б;

○ после выработки квантового ключа в приемном и передающем модулях выработки квантовых ключей передают полученный квантовый ключ из приемного модуля выработки квантовых ключей в модуль согласования ключей приемного узла и из передающего модуля выработки квантовых ключей в модуль согласования ключей передающего узла;

○ сохраняют полученный квантовый ключ в модулях согласования ключей приемного и передающего узла;

○ проверяют суммарный размер сохраненных квантовых ключей в модулях согласования квантовых ключей приемного и передающего узлов, причем если суммарный размер сохраненных квантовых ключей меньше Key блоков, то переходят к этапу Б;

• формируют новый ключ аутентификации и новый ключ шифрования из Key блоков сохраненного квантового ключа в модулях согласования квантовых ключей приемного и передающего узлов, выполняя следующие действия:

○ формируют новый ключ аутентификации в модуле согласования квантовых ключей передающего узла путем конкатенации первых m блоков накопленного квантового ключа;

○ добавляют к ключу аутентификации идентификатор в виде блока данных, содержащий значение счетчика ключей аутентификации M1 и значение признака ключа аутентификации;

○ увеличивают значение M1 счетчика ключей аутентификации на единицу;

○ формируют новый ключ шифрования в модуле согласования квантовых ключей передающего узла путем конкатенации последующих n блоков накопленного квантового ключа;

○ добавляют к ключу шифрования идентификатор в виде блока данных, содержащий значение счетчика ключей шифрования N1 и значение признака ключа шифрования;

○ увеличивают значение N1 счетчика ключей шифрования на единицу;

○ формируют новый ключ аутентификации в модуле согласования квантовых ключей приемного узла путем конкатенации первых m блоков накопленного квантового ключа;

○ добавляют к ключу аутентификации идентификатор в виде блока данных, содержащий значение счетчика ключей аутентификации M2 и значение признака ключа аутентификации;

○ увеличивают значение M2 счетчика ключей аутентификации на единицу;

○ формируют новый ключ шифрования в модуле согласования квантовых ключей приемного узла путем конкатенации последующих n блоков накопленного квантового ключа;

○ добавляют к ключу шифрования идентификатор в виде блока данных, содержащий

значение счетчика ключей шифрования N2 и значение признака ключа шифрования;

- увеличивают значение N2 счетчика ключей шифрования на единицу;

- сравнивают идентификаторы полученного нового ключа аутентификации и полученного нового ключа шифрования из модуля согласования ключей приемного узла с идентификаторами нового ключа аутентификации и нового ключа шифрования в модуле согласования ключей передающего узла, причем

- если идентификаторы ключей аутентификации совпали, то

- передают сообщение об успешной проверке идентификаторов ключей аутентификации из модуля согласования ключей передающего узла в модуль согласования ключей приемного узла как служебное зашифрованное аутентифицированное сообщение, зашифрованное на текущем ключе шифрования и аутентифицированное на текущем ключе аутентификации,

- получают в модуле согласования ключей передающего узла служебное сообщение об успешной проверке идентификаторов ключей аутентификации,

- заменяют текущий ключ аутентификации новым ключом аутентификации в модулях согласования ключей приемного и передающего узла;

иначе

- переходят к этапу А;

- если идентификаторы ключей шифрования совпали, то

- передают сообщение об успешной проверке идентификаторов ключей шифрования из модуля согласования ключей передающего узла в модуль согласования ключей приемного узла как служебное зашифрованное аутентифицированное сообщение, зашифрованное на текущем ключе шифрования и аутентифицированное на текущем ключе аутентификации,

- получают в модуле согласования ключей передающего узла служебное сообщение об успешной проверке идентификаторов ключей шифрования,

иначе

- переходят к этапу А;

- передают сформированные новые ключи шифрования из модуля согласования ключей передающего узла в 1-й шифратор по 1-й ЛС и из модуля согласования ключей приемного узла в 2-й шифратор по 2-й ЛС;

- сравнивают идентификатор полученного нового ключа шифрования во 2-м шифраторе с идентификаторами нового ключа шифрования, выполняя следующие действия:

- передают идентификатор нового ключа шифрования из 1-го шифратора во 2-й шифратор как служебное зашифрованное сообщение, зашифрованное на текущем ключе шифрования;

- получают во 2-м шифратор служебное сообщение с идентификатором нового ключа шифрования;

- проводят во 2-м шифраторе сравнение идентификаторов новых ключей шифрования;

- если идентификаторы ключей шифрования не совпали, то

- сигнализируют о неуспешном приеме ключей шифрования шифраторами;

- переходят к этапу А;

иначе

- сохраняют полученные ключи шифрования в шифраторах для дальнейшего

использования.

Назначение комплекса - организация шифрованного канала связи между двумя узлами доверенной сети связи (например, в локальных сетях государственных учреждений и ведомств, корпораций).

Комплекс получает данные, которые необходимо защищенным образом доставить по назначению (например, пользовательские данные), в 1-й шифратор. Полученные 1-м шифратором данные зашифровываются с помощью текущих ключей, созданных с использованием согласованных ключей, полученных с использованием квантовых ключей из системы КРК. Стойкость текущих ключей шифрования обусловлена стойкостью квантовых ключей, из которых получены текущие ключи шифрования, что приводит к повышению защищенности пользовательских данных, передаваемых с защитой на таких ключах.

Затем 1-й шифратор передает зашифрованные данные по транспортной линии связи во 2-й шифратор, который расшифровывает информацию с помощью текущих ключей шифрования, созданных с использованием согласованных ключей, полученных с использованием квантовых ключей из системы КРК, и передает по назначению.

Для обеспечения защищенной передачи информации шифраторам необходимы идентичные ключи шифрования. Применение предлагаемого способа согласования ключей гарантирует использование идентичных ключей как для зашифрования данных, так и для их расшифрования, чем достигается преимущество в защищенности передаваемых пользовательских данных по сравнению с выбранным прототипом, в котором возможно навязывание использования различных сессионных ключей для зашифрования и расшифрования.

В предлагаемом способе квантовые ключи используются не только для создания ключей шифрования, но и для создания ключей аутентификации. Идентичность ключей шифрования и идентичность ключей аутентификации в сопряженных шифраторах по разные стороны транспортной линии связи необходима для корректного выполнения соответствующих операций, а именно, шифрования и расшифрования, а также аутентификации данных и проверки аутентичности данных.

Квантовые ключи, с использованием которых формируются ключи шифрования и ключи аутентификации, идентичны в двух составных частях системы КРК (передающем и приемном узле) в силу особенностей функционирования квантового протокола. При дальнейшем формировании новых ключей из квантовых ключей необходимо убедиться, что в двух шифраторах, соединенных транспортной линией связи (или в двух модулях согласования ключей системы КРК), будут применяться идентичные ключи шифрования (или ключи аутентификации).

Для этого в предлагаемом способе применяется согласование ключей по их идентификаторам путем сравнения идентификаторов ключей. Если идентификаторы не совпадают, то соответствующие им ключи отбрасываются (удаляются), чтобы не нарушать работоспособность комплекса из-за расхождения ключей, которые должны быть идентичными. За счет дополнительного сравнения идентификаторов ключей шифрования в шифраторах (помимо их сравнения в модулях согласования ключей перед передачей ключей шифрования в шифраторы) достигается повышение надежности комплекса в случае искажений (случайных или преднамеренных), вносимых локальной линией связи, связывающей узел системы КРК с шифратором.

Использование части квантового ключа для аутентификации служебных данных системы КРК, в том числе данных квантового протокола по постобработке последовательностей, которые передаются в квантовом канале, повышает стойкость

вырабатываемых квантовых ключей. Как известно, стойкость квантовых ключей зависит от стойкости способа передачи квантовых состояний по квантовому каналу, способа кодирования и детектирования квантовых состояний, от алгоритмов постобработки последовательностей, полученных из квантовых состояний, и от способа защиты данных, которыми обмениваются составные части системы КРК при постобработке последовательностей, полученных из квантового канала. Выбранный квантовый протокол определяет стойкость способа кодирования и детектирования квантовых состояний, а также алгоритма постобработки последовательностей, но не определяет способ защиты служебных данных в процессе постобработки последовательностей. В отсутствии защиты этих служебных данных возможны атаки типа "человек посередине" на системы, КРК. Защита служебных данных достигается их аутентификацией и/или шифрованием.

Аутентификацию передаваемых данных можно обеспечить либо с помощью предварительно распределенных симметричных ключей (предраспределенных ключей), либо с помощью квантовых ключей. В начальный момент функционирования комплекса квантовые ключи для аутентификации еще недоступны, поскольку сама выработка квантовых ключей требует аутентифицированного канала между приемным и передающем узлами системы КРК. Таким образом, первичная аутентификация всех сторон взаимодействия в комплексе основывается на предраспределенных ключах. Для обеспечения аутентификации в дальнейшем используются квантовые ключи согласно предлагаемому способу.

В предлагаемом способе согласования ключей производится аутентификация каждого передаваемого сообщения целиком, что гарантирует его целостность на принимающей стороне. Обычно при аутентификации сообщений, передаваемых по классическим линиям связи, сообщение перед передачей разбивается на части (например, кадры для линии связи, выполненной в виде Ethernet, или IP-пакеты для линии связи, выполненной в виде WAN, LAN) с последующим добавлением ими-товставки к каждой части. Такой способ гарантирует целостность каждой части в отдельности, но не гарантирует целостность полного сообщения, собранного из отдельных частей, так как, например, может быть нарушен порядок частей сообщения. В предлагаемом способе за счет аутентификации целиком каждого сообщения гарантирована его целостность, что повышает стойкость квантовых ключей.

При высоких скоростях шифрования требуется часто заменять текущий ключ шифрования на новый в связи с израсходованием допустимой нагрузки на ключ шифрования. Для этих целей применяется однопроходная система КРК из состава комплекса. С помощью данной системы КРК вырабатываются квантовые ключи, которые затем накапливаются в модулях согласования ключей системы КРК.

Накопление квантовых ключей до требуемого объема с последующим формированием ключей шифрования для передачи в шифраторы позволяет применять комплекс даже при низкой скорости генерации квантовых ключей и/или генерации квантовых ключей длины, меньше требуемой шифратором. Помещение ключей шифрования, переданных в шифратор, в хранилище ключей вместо незамедлительного использования, позволяет полностью использовать допустимую нагрузку на текущий ключ шифрования и осуществлять запланированную смену текущего ключа шифрования.

После накопления достаточного количества квантовых ключей из них формируются ключи шифрования для шифраторов и ключи аутентификации для аутентификации служебных данных системы КРК, передающихся между приемным и передающим

узлами системы КРК в процессе выполнения квантового протокола. Под достаточным количеством накопленных квантовых ключей понимается число квантовых ключей, суммарная длина которых не меньше суммарной длины хотя бы одного ключа шифрования и одного ключа аутентификации. Необходимые длины ключей шифрования и ключей аутентификации определяются применяемыми способом шифрования и способом аутентификации.

За счет накопления квантовых ключей перед дальнейшим формированием ключей шифрования и ключей аутентификации достигается повышение надежности комплекса в случае непредвиденных кратковременных сбоев однопроходной системы КРК, выражающихся во временном прекращении генерации квантовых ключей или вызванных, например, атаками нарушителя на квантовый канал связи. В таком случае уже выработанные квантовые ключи сохраняются, и после восстановления работоспособности системы КРК продолжается накопление квантовых ключей к уже имеющимся накопленным ранее квантовым ключам. Также работоспособность комплекса сохраняется в случае выработки системой КРК квантовых ключей, длина которых недостаточна для формирования новых ключей шифрования и ключей аутентификации. В этом случае происходит накопление квантовых ключей для формирования требуемых ключей шифрования и ключей аутентификации уже из совокупности накопленных квантовых ключей.

Шифрование как служебных данных, так и идентификаторов, используемых при согласовании и вводе в эксплуатацию ключей, повышает защищенность пользовательских данных и надежность комплекса от навязывания ложных идентификаторов ключей. За счет этого гарантируется выполнение устройством своей основной функции по защищенной передаче пользовательских данных с последующим гарантированным расшифрованием.

Также предлагаемый комплекс имеет преимущество по защищенности данных по сравнению с известным прототипом, поскольку не использует дополнительное распределение классических ключей (кроме первично предраспределенных ключей для инициализации комплекса, которые необходимы для любой типовой системы КРК), получая таким образом стойкие к атакам квантовым компьютером ключи шифрования, используемые в шифраторах. Используемая в прототипе система обмена классическими ключами требует построения собственной линии связи, отличной от линии связи между зашифровывающими/расшифровывающими процессорами в прототипе.

В предлагаемом комплексе используется только одна классическая линия связи (транспортная линия связи), соединяющая как два шифратора, так и два узла системы КРК.

Канал передачи служебных сообщений системы КРК состоит из перечисленных ниже каналов передачи информации:

- аутентифицированный с использованием квантовых ключей канал передачи служебной информации и квантовых ключей из приемного узла системы КРК в сопряженный шифратор и обратно,
- аутентифицированный с использованием квантовых ключей канал передачи пользовательских данных между шифраторами,
- аутентифицированный с использованием квантовых ключей канал передачи служебной информации и квантовых ключей из передающего узла системы КРК в сопряженный шифратор и обратно.

Таким образом, по сравнению с прототипом, в предлагаемом техническом решении не требуется отдельный канал для обмена служебными данными узлов системы КРК

при выработке квантовых ключей, вместо этого используется единый канал для передачи служебных сообщений системы КРК и передачи зашифрованных пользовательских данных, что позволяет снизить затраты на создание, развертывание и эксплуатацию комплекса.

Транспортная линия связи может быть доступной для атак возможного нарушителя. При использовании предлагаемого устройства и способа критически важная информация, содержащая сведения о данных в транспортной линии связи, включая служебные данные классического канала системы КРК о квантовом ключе, передается в зашифрованном виде на текущем ключе шифрования. Данное решение повышает защищенность передаваемых пользовательских данных и надежность комплекса.

Краткое описание чертежей

На чертеже показана схема комплекса для защищенной передачи данных с использованием системы КРК.

На чертеже обозначены:

1 - 1-й шифратор,
2 - 2-й шифратор,
3 - передающий узел системы КРК,
4 - приемный узел системы КРК,
5 - модуль выработки квантовых ключей передающего узла системы КРК,
6 - модуль согласования ключей передающего узла системы КРК,
7 - модуль выработки квантовых ключей приемного узла системы КРК,
8 - модуль согласования ключей приемного узла системы КРК,
9 - квантовая линия связи,
10 - транспортная линия связи,
11 - 1-я локальная линия связи,
12 - 2-я локальная линия связи.

Осуществление изобретения

Предлагаемые комплекс и способ могут быть реализованы, например, с использованием известной однопроходной системы КРК (патент РФ №2706175) и двух промышленных шифраторов, например, программно-аппаратных комплексов ViPNet L2 10G (статья по адресу https://infotecs.ru/about/press-centr/news/infoteks-i-eci-telecom-proveli-ispytaniya-na-sovmestimost-svoikh-produktov.html).

Модули согласования ключей 6,8 (на фигуре графического изображения) целесообразно выполнить в виде программных модулей в составе передающего узла 3 и приемного узла 4 однопроходной системы КРК. Возможность принимать ключи шифрования и служебные данные по локальным линиям связи 11, 12 реализуется в шифраторах 1, 2 также программно. Соответствующие программы и модули могут быть сформированы специалистом по программированию (программистом) на основе знания выполняемых функций.

В качестве квантовой линии связи 9 выбирается одномодовое оптоволокно типа SMF-28 допустимой длины. В качестве двух локальных линий связи 11, 12 выбирается два Ethernet патчкорда, которыми соединяются 1-й шифратор 1 с модулем согласования ключей передающего узла 6 системы КРК и 2-й шифратор 2 с модулем согласования ключей приемного узла 8 системы КРК соответственно. В качестве транспортной линии связи 10 может быть выбрано стандартное телекоммуникационное оптоволокно или линия Ethernet.

Для осуществления способа выполняют следующие действия:

Выбирают квантовый протокол, например, протокол на геометрически однородных

когерентных состояниях (Молотков С.Н. О геометрически однородных когерентных квантовых состояниях в квантовой криптографии, Письма в ЖЭТФ, том 95, вып. 6, с. 361-366, 2012).

Выбирают размер блока равным 8 бит.

Выбирают размер ключа шифрования равным 32 блокам, то есть 256 бит, что соответствует, например, размеру ключа шифрования блочного шифра ГОСТ 34.12-2018 "Кузнечик".

Выбирают размер ключа аутентификации равным 32 блокам.

Выбирают минимальный объем накопленного квантового ключа равным Key=32+32=64 блока.

Устанавливают программное значение счетчиков ключей аутентификации и ключей шифрования соответственно M1=1, M2=2, N1=1, N2=2.

Формируют текущий ключ аутентификации длиной 32 блока, например, с помощью квантового генератора случайных чисел (Балыгин К.А. др. Квантовый генератор случайных чисел, основанный на пуассоновской статистике фотоотсчетов, со скоростью около 100 Мбит/с, ЖЭТФ, том 153, вып. 6, с. 879-894, 2018). Присваивают идентификатор ключа аутентификации равным ID=(1, auth).

Формируют текущий ключ шифрования длиной 32 блока, например, с помощью генератора случайных чисел. Присваивают идентификатор ключа шифрования равным ID=(1, cipher).

Увеличивают значение счетчиков M1 и N1 на 1. Новые значения счетчиков M1=2 и N1=2 соответственно.

Загружают сформированный ключ аутентификации в модули согласования ключей приемного и передающего узлов системы КРК, а ключ шифрования - в шифраторы.

Запускают накопление квантовых ключей в модулях согласования. Для этого запускают выполнение выбранного квантового протокола для получения квантового ключа. Служебные данные, генерируемые модулями выработки квантовых ключей 5, 7 системы КРК в процессе выполнения квантового протокола, аутентифицируются с помощью текущего ключа аутентификации, например, путем вычисления имитовставки от аутентифицируемых данных по ГОСТ Р 34.13-2015 и конкатенации ее к служебным данным, в модуле согласования ключей узла системы КРК.

Затем аутентифицированные служебные данные передаются по локальной линии связи в сопряженный шифратор. В шифраторе эти данные зашифровываются с помощью текущего ключа шифрования с помощью алгоритмом шифрования, реализуемого выбранным шифратором. Зашифрованные данные передаются по транспортной линии связи во 2-й шифратор. Во 2-м шифраторе полученные данные расшифровываются и передаются по локальной линии связи в сопряженный модуль согласования ключей второго узла системы КРК. В модуле согласования ключей проверяется аутентичность полученных служебных данных, например, путем вычисления имитовставки по ГОСТ Р 34.13-2015 от служебных данных с помощью текущего ключа аутентификации и сравнения вычисленной имитовставки с полученной по служебной линии связи. В случае совпадения имитовставок служебные данные признаются аутентичными, в противном случае подается сигнал о неуспешной аутентификации служебных данных и прекращение выработки квантового ключа.

Сигнал о неуспешной аутентификации может быть выработан в каком-либо удобном виде, например, в виде звукового сигнала, текстового сообщения и т.п., и выдан администратору или дежурному специалисту из состава персонала, обслуживающего комплекс. Дальнейшие действия при получении сигнала должны определяться принятым

регламентом реагирования на аварийные или нештатные ситуации при эксплуатации комплекса.

После завершения выполнения квантового протокола в модули согласования ключей передаются выработанные квантовые ключи некоторой длины. В силу особенностей квантовых протоколов длина полученного квантового ключа не фиксирована. Поэтому после получения каждого квантового ключа в модуле согласования ключей производят проверку, достаточна ли суммарная длина накопленных квантовых ключей, включая длину только что полученного ключа. Допустим, длина первого полученного квантового ключа оказалась 120 бит. Выбранная минимальная длина накопленных квантовых ключей 64 блока, что составляет 512 бит. Следовательно, полученного квантового ключа недостаточно, его сохраняют в памяти модулей согласования ключей для дальнейшего накопления. Запускают выработку следующего квантового ключа.

Пусть второй квантовый ключ получен длиной 270 бит. Проверяют суммарную длину накопленных квантовых ключей. В данном случае суммарная длина накопленных квантовых ключей, включая полученный, составляет 120+270=390 бит, что снова меньше выбранной минимальной длины. Второй полученный квантовый ключ также сохраняют в памяти модулей согласования ключей и запускают выработку третьего квантового ключа.

Пусть третий квантовый ключ получен длиной 150 бит. Суммарная длина накопленных квантовых ключей после получения третьего квантового ключа 120+270+150=540 бит, что больше выбранного порога в 512 бит. Поэтому сохраняют третий квантовый ключ в памяти модулей согласования ключей и переходят к следующему шагу способа.

Из сохраненных квантовых ключей формируют новый ключ шифрования и новый ключ аутентификации одновременно в обоих модулях согласования ключей узлов системы КРК. Для этого выполняют конкатенацию трех квантовых ключей в одну строку бит. Из первых 32 блоков бит из полученной строки формируют новый ключ аутентификации. К ключу аутентификации добавляют его идентификатор, полученный из значения счетчика и признака использования ключа, то есть ID=(2, auth). Счетчики ключей аутентификации увеличиваются на 1, то есть M1=3, M2=3. Из следующих 32 бит формируют новый ключ шифрования, к которому аналогично добавляют идентификатор ID=(2, cipher), а значения счетчиков ключей шифрования увеличивают N1=3, N2=3.

После формирования новых ключей шифрования и ключей аутентификации проверяют, что полученные ключи согласованы. Для этого производят сравнение их идентификаторов. В частности, идентификаторы ключа шифрования и ключа аутентификации передают как служебные данные из модуля согласования ключей приемного узла системы КРК в передающий узел системы КРК, где производят сравнение идентификаторов. При этом в процессе передачи идентификаторов по транспортной линии связи между шифраторами, идентификаторы аутентифицированы на текущем ключе аутентификации и зашифрованы на текущем ключе шифрования, что защищает от навязывания ложных идентификаторов нарушителем.

При совпадении идентификаторов назначают новый ключ аутентификации текущим, на котором будет производиться аутентификация последующих служебных данных. Новые ключи шифрования вместе с их идентификаторами передают по служебной линии связи в соответствующие шифраторы.

После поступления новых ключей шифрования в шифраторы проверяется согласованность этих ключей аналогичным образом, путем сравнения идентификаторов.

При совпадении идентификаторов новых ключей шифрования, данные ключи вместе с их идентификаторами сохраняют в хранилищах ключей шифраторов для дальнейшего использования.

После этого запускают новую выработку квантовых ключей.

Использование ключей может осуществляться для защиты данных пользователей, при этом пользователи могут подключаться к любому шифратору.

(57) Формула изобретения

1. Комплекс для защищенной передачи данных в цифровой сети передачи данных с использованием однопроходной системы квантового распределения ключей, имеющий в составе

передающий узел системы квантового распределения ключей (КРК), включающий

передающий модуль выработки квантовых ключей,

модуль согласования ключей передающего узла;

приемный узел системы КРК, включающий

приемный модуль выработки квантовых ключей,

модуль согласования ключей приемного узла;

1-й шифратор, связанный с модулем согласования ключей передающего узла;

2-й шифратор, связанный с модулем согласования ключей приемного узла;

причем передающий модуль выработки квантовых ключей связан с приемным модулем выработки квантовых ключей квантовой линией связи, выполненной в виде оптоволоконной линии;

1-й шифратор связан со 2-м шифратором транспортной линией связи, выполненной в виде цифровой сети передачи данных;

1-й шифратор связан с модулем согласования ключей передающего узла посредством 1-й локальной линии связи (1-я ЛС);

2-й шифратор связан с модулем согласования ключей приемного узла посредством 2-й локальной линии связи (2-я ЛС);

1-й шифратор связан с внешней цифровой сетью передачи данных;

2-й шифратор связан с внешней цифровой сетью передачи данных;

при этом передающий модуль выработки квантовых ключей выполнен с возможностью

генерировать случайные числа,

формировать квантовые информационные состояния,

отправлять квантовые информационные состояния по квантовой линии связи в приемный модуль выработки квантовых ключей,

вырабатывать квантовые ключи совместно с приемным модулем выработки квантовых ключей путем обработки информации, полученной из квантовых информационных состояний;

модуль согласования ключей передающего узла выполнен с возможностью

формировать ключи аутентификации и ключи шифрования на основе квантовых ключей,

согласовывать ключи аутентификации и ключи шифрования с ключами аутентификации и ключами шифрования, сформированными модулем согласования ключей приемного узла,

принимать данные из 1-го шифратора по 1-й ЛС,

передавать данные в 1-й шифратор по 1-й ЛС;

приемный модуль выработки квантовых ключей выполнен с возможностью

генерировать случайные числа,

принимать квантовые информационные состояния по квантовой линии связи из передающего модуля выработки квантовых ключей,

обрабатывать квантовые информационные состояния,

вырабатывать квантовые ключи совместно с передающим модулем выработки квантовых ключей путем обработки информации, полученной из квантовых информационных состояний;

модуль согласования ключей приемного узла выполнен с возможностью формировать ключи аутентификации и ключи шифрования на основе квантовых ключей,

согласовывать ключи аутентификации и ключи шифрования с ключами аутентификации и ключами шифрования, сформированными модулем согласования ключей передающего узла,

принимать данные из 2-го шифратора по 2-й ЛС,

передавать данные во 2-й шифратор по 2-й ЛС;

1-й шифратор выполнен с возможностью

принимать ключи шифрования и служебные данные из модуля согласования ключей передающего узла по 1-й ЛС,

передавать служебные данные в модуль согласования ключей передающего узла по 1-й ЛС,

принимать данные из внешней цифровой сети передачи данных,

зашифровывать данные, поступившие в него по внешней цифровой сети передачи данных или по 1-й ЛС, с использованием ключей шифрования,

передавать данные, зашифрованные с использованием ключей шифрования, по транспортной линии связи,

расшифровывать данные, поступившие из транспортной линии связи, с использованием ключей шифрования,

передавать данные во внешнюю цифровую сеть передачи данных;

2-й шифратор выполнен с возможностью

принимать ключи шифрования и служебные данные из модуля согласования ключей приемного узла по 2-й ЛС,

передавать служебные данные в модуль согласования ключей приемного узла по 2-й ЛС,

принимать данные из внешней цифровой сети передачи данных,

зашифровывать данные, поступившие в него по внешней цифровой сети передачи данных или по 2-й ЛС, с использованием ключей шифрования,

передавать данные, зашифрованные с использованием ключей шифрования, по транспортной линии связи,

расшифровывать данные, поступившие из транспортной линии связи, с использованием ключей шифрования,

передавать данные во внешнюю цифровую сеть передачи данных.

2. Способ согласования ключей при работе комплекса, заключающийся в том, что

выбирают квантовый протокол;

выбирают размер блока равным b, где b кратно степени целого числа 2;

выбирают размер ключа шифрования равным n блоков;

выбирают размер ключа аутентификации равным m блоков;

выбирают минимальный объем накопленного квантового ключа равным Key=m+n блоков;

устанавливают значение счетчика ключей аутентификации в модуле согласования

ключей передающего узла M1=1;

устанавливают значение счетчика ключей аутентификации в модуле согласования ключей приемного узла M2=2;

устанавливают значение счетчика ключей шифрования в модуле согласования ключей передающего узла N1=1;

устанавливают значение счетчика ключей шифрования в модуле согласования ключей приемного узла N2=2;

формируют текущий ключ аутентификации размером m блоков, выполняя следующие действия:

добавляют к ключу аутентификации идентификатор в виде блока данных, содержащий значение счетчика M1 и значение признака ключа аутентификации;

увеличивают значение счетчика M1 на 1;

формируют текущий ключ шифрования размером n блоков, выполняя следующие действия:

добавляют к ключу шифрования идентификатор в виде блока данных, содержащий значение счетчика N1 и значение признака ключа шифрования;

увеличивают значение счетчика N1 на 1;

загружают текущий ключ аутентификации в модули согласования ключей приемного и передающего узла;

загружают текущий ключ шифрования в 1-й и 2-й шифраторы;

(А) накапливают квантовые ключи в модулях согласования ключей передающего и приемного узлов системы КРК, выполняя следующие действия:

(Б) вырабатывают квантовый ключ в передающем и приемном модулях выработки квантовых ключей согласно выбранному квантовому протоколу, причем в ходе выполнения квантового протокола в части передачи служебных данных от передающего к приемному модулю выработки квантового ключа выполняют следующие действия:

формируют служебное сообщение из служебных данных в передающем модуле выработки квантовых ключей;

передают служебные данные из передающего модуля выработки квантовых ключей в модуль согласования ключей передающего узла;

осуществляют аутентификацию служебного сообщения с помощью текущего ключа аутентификации в модуле согласования ключей передающего узла;

передают аутентифицированное служебное сообщение по 1-й ЛС в 1-й шифратор;

зашифровывают аутентифицированное служебное сообщение с помощью текущего ключа шифрования в 1-м шифраторе;

передают зашифрованное аутентифицированное служебное сообщение во 2-й шифратор через транспортную линию связи;

расшифровывают зашифрованное аутентифицированное служебное сообщение во 2-м шифраторе с помощью текущего ключа шифрования;

передают аутентифицированное служебное сообщение из 2-го шифратора в модуль согласования ключей приемного узла по 2-й ЛС;

проверяют аутентичность полученного служебного сообщения с помощью текущего ключа аутентификации в модуле согласования ключей приемного узла, причем если проверка аутентичности успешна, то

передают служебное сообщение из модуля согласования ключей приемного узла в приемный модуль выработки квантовых ключей;

иначе сигнализируют о неуспешной аутентификации;

переходят к этапу Б;

в ходе выполнения квантового протокола в части передачи служебных данных от приемного к передающему модулю выработки квантового ключа выполняют следующие действия:

формируют служебное сообщение из служебных данных в приемном модуле выработки квантовых ключей;

передают служебные данные из приемного модуля выработки квантовых ключей в модуль согласования ключей приемного узла;

осуществляют аутентификацию служебного сообщения с помощью текущего ключа аутентификации в модуле согласования ключей приемного узла;

передают аутентифицированное служебное сообщение по 2-й ЛС во 2-й шифратор;

зашифровывают аутентифицированное служебное сообщение с помощью текущего ключа шифрования во 2-м шифраторе;

передают зашифрованное аутентифицированное служебное сообщение в 1-й шифратор через транспортную линию связи;

расшифровывают зашифрованное аутентифицированное служебное сообщение в 1-м шифраторе с помощью текущего ключа шифрования;

передают аутентифицированное служебное сообщение из 1-го шифратора в модуль согласования ключей передающего узла по 1-й ЛС;

проверяют аутентичность полученного служебного сообщения с помощью текущего ключа аутентификации в модуле согласования ключей передающего узла, причем если проверка аутентичности успешна, то

передают служебное сообщение из модуля согласования ключей передающего узла в передающий модуль выработки квантовых ключей;

иначе сигнализируют о неуспешной аутентификации;

переходят к этапу Б;

после выработки квантового ключа в приемном и передающем модулях выработки квантовых ключей передают полученный квантовый ключ из приемного модуля выработки квантовых ключей в модуль согласования ключей приемного узла и из передающего модуля выработки квантовых ключей в модуль согласования ключей передающего узла;

сохраняют полученный квантовый ключ в модулях согласования ключей приемного и передающего узла;

проверяют суммарный размер сохраненных квантовых ключей в модулях согласования квантовых ключей приемного и передающего узлов, причем если суммарный размер сохраненных квантовых ключей меньше Key блоков, то переходят к этапу Б;

формируют новый ключ аутентификации и новый ключ шифрования из Key блоков сохраненного квантового ключа в модулях согласования квантовых ключей приемного и передающего узлов, выполняя следующие действия:

формируют новый ключ аутентификации в модуле согласования квантовых ключей передающего узла путем конкатенации первых m блоков накопленного квантового ключа;

добавляют к ключу аутентификации идентификатор в виде блока данных, содержащий значение счетчика ключей аутентификации M1 и значение признака ключа аутентификации;

увеличивают значение M1 счетчика ключей аутентификации на единицу;

формируют новый ключ шифрования в модуле согласования квантовых ключей передающего узла путем конкатенации последующих n блоков накопленного квантового

ключа;

добавляют к ключу шифрования идентификатор в виде блока данных, содержащий значение счетчика ключей шифрования N1 и значение признака ключа шифрования;

увеличивают значение N1 счетчика ключей шифрования на единицу; формируют новый ключ аутентификации в модуле согласования квантовых ключей приемного узла путем конкатенации первых m блоков накопленного квантового ключа;

добавляют к ключу аутентификации идентификатор в виде блока данных, содержащий значение счетчика ключей аутентификации M2 и значение признака ключа аутентификации;

увеличивают значение M2 счетчика ключей аутентификации на единицу;

формируют новый ключ шифрования в модуле согласования квантовых ключей приемного узла путем конкатенации последующих n блоков накопленного квантового ключа;

добавляют к ключу шифрования идентификатор в виде блока данных, содержащий значение счетчика ключей шифрования N2 и значение признака ключа шифрования;

увеличивают значение N2 счетчика ключей шифрования на единицу; сравнивают идентификаторы полученного нового ключа аутентификации и полученного нового ключа шифрования из модуля согласования ключей приемного узла с идентификаторами нового ключа аутентификации и нового ключа шифрования в модуле согласования ключей передающего узла, причем

если идентификаторы ключей аутентификации совпали, то

передают сообщение об успешной проверке идентификаторов ключей аутентификации из модуля согласования ключей передающего узла в модуль согласования ключей приемного узла как служебное зашифрованное аутентифицированное сообщение, зашифрованное на текущем ключе шифрования и аутентифицированное на текущем ключе аутентификации,

получают в модуле согласования ключей передающего узла служебное сообщение об успешной проверке идентификаторов ключей аутентификации, заменяют текущий ключ аутентификации новым ключом аутентификации в модулях согласования ключей приемного и передающего узла;

иначе переходят к этапу A;

если идентификаторы ключей шифрования совпали, то

передают сообщение об успешной проверке идентификаторов ключей шифрования из модуля согласования ключей передающего узла в модуль согласования ключей приемного узла как служебное зашифрованное аутентифицированное сообщение, зашифрованное на текущем ключе шифрования и аутентифицированное на текущем ключе аутентификации,

получают в модуле согласования ключей передающего узла служебное сообщение об успешной проверке идентификаторов ключей шифрования,

иначе переходят к этапу A;

передают сформированные новые ключи шифрования из модуля согласования ключей передающего узла в 1-й шифратор по 1-й ЛС и из модуля согласования ключей приемного узла в 2-й шифратор по 2-й ЛС;

сравнивают идентификатор полученного нового ключа шифрования во 2-м шифраторе с идентификаторами нового ключа шифрования, выполняя следующие действия:

передают идентификатор нового ключа шифрования из 1-го шифратора во 2-й шифратор как служебное зашифрованное сообщение, зашифрованное на текущем

ключе шифрования;

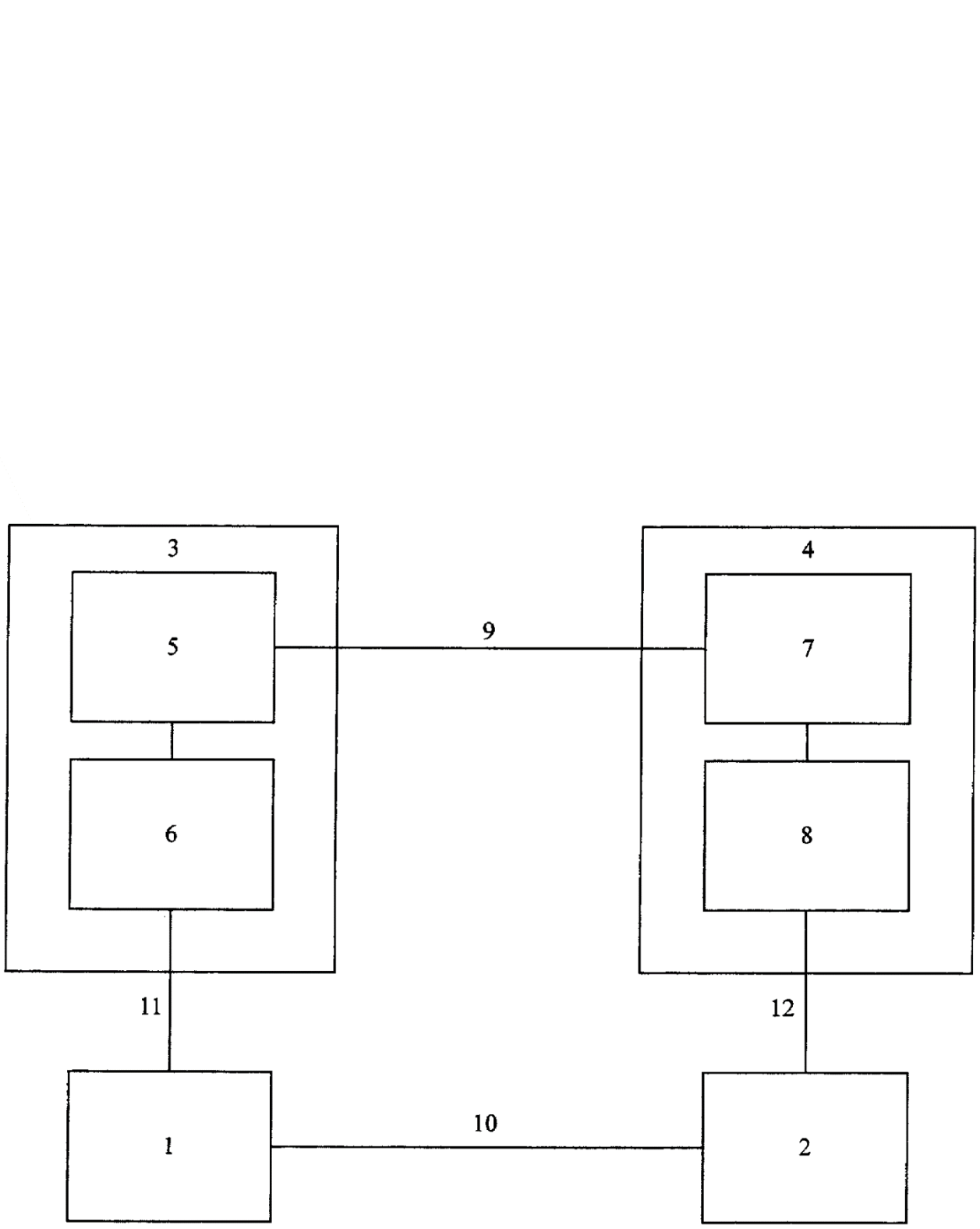
получают во 2-м шифраторе служебное сообщение с идентификатором нового ключа шифрования;

проводят во 2-м шифраторе сравнение идентификаторов новых ключей шифрования;

если идентификаторы ключей шифрования не совпали, тогда сигнализируют о неуспешном приеме ключей шифрования шифраторами;

переходят к этапу А;

иначе сохраняют полученные ключи шифрования в шифраторах для дальнейшего использования.


1
3
4
5
9
7
6
8
11
12
1
10
2

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ

№ 2708511

Способ формирования ключа между узлами вычислительной сети с использованием системы квантового распределения ключей

Патентообладатель: ***Открытое акционерное общество "Информационные технологии и коммуникационные системы" (RU)***

Автор: ***Жиляев Андрей Евгеньевич (RU)***

Заявка № **2019102923**
Приоритет изобретения **04 февраля 2019 г.**
Дата государственной регистрации в Государственном реестре изобретений Российской Федерации **09 декабря 2019 г.**
Срок действия исключительного права на изобретение истекает **04 февраля 2039 г.**

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 708 511** (13) **C1**

(51) МПК
H04L 9/08 (2006.01)
G06F 21/72 (2013.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 9/08 *(2019.05);* ***G06F 21/72*** *(2019.05)*

(21)(22) Заявка: **2019102923, 04.02.2019**

(24) Дата начала отсчета срока действия патента:
04.02.2019

Дата регистрации:
09.12.2019

Приоритет(ы):
(22) Дата подачи заявки: **04.02.2019**

(45) Опубликовано: **09.12.2019** Бюл. № **34**

Адрес для переписки:
127287, Москва, Старый Петровско-Разумовский пр-д, 1/23, стр. 1, Открытое акционерное общество "Информационные технологии и коммуникационные системы"

(72) Автор(ы):
Жиляев Андрей Евгеньевич (RU)

(73) Патентообладатель(и):
Открытое акционерное общество "Информационные технологии и коммуникационные системы" (RU)

(56) Список документов, цитированных в отчете о поиске: **RU 2566335 C1, 20.10.2015. RU 2621605 C2, 06.06.2017. RU 2671620 C1, 02.11.2018. RU 2665249 C1, 28.08.2018. US 2018/0191496 A1, 05.07.2018.**

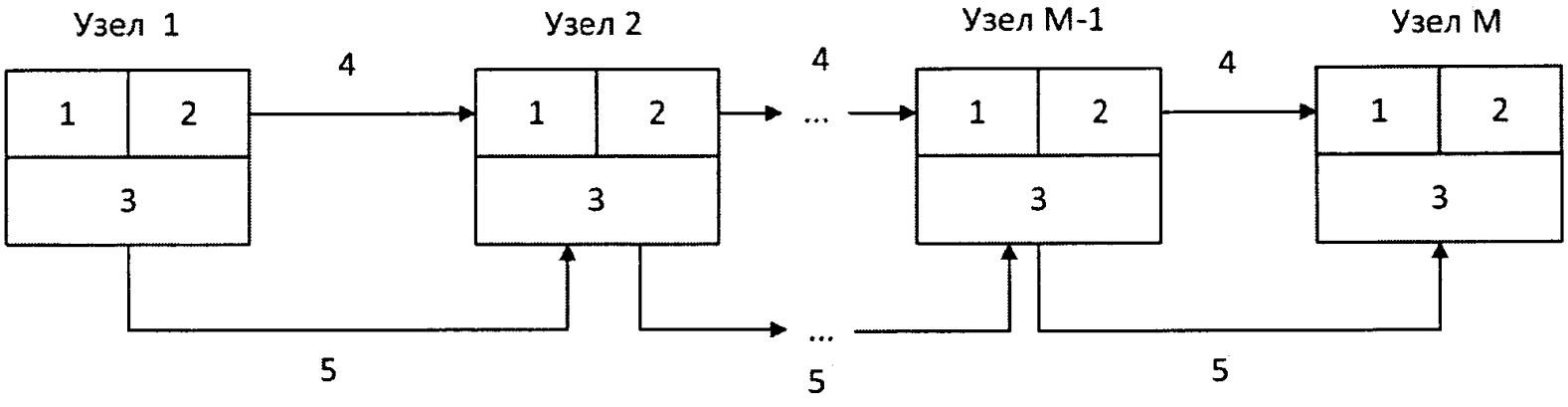
(54) Способ формирования ключа между узлами вычислительной сети с использованием системы квантового распределения ключей

(57) Реферат:

Изобретение относится к области квантовой криптографии. Технический результат заключается в повышении защищенности передаваемого ключа, возможности использования разных алгоритмов шифрования на каждом участке вычислительной сети, снижении возможности проведения атак, основанных на сборе статистики по побочным каналам. Технический результат достигается за счет способа формирования ключа между двумя узлами вычислительной сети с использованием системы квантового распределения ключей, причем в сети установлены последовательно соединенные M узлов, причем каждый узел включает входной и выходной модули аппаратуры квантового распределения ключей, выполненные с возможностью формирования квантовых ключей в результате выполнения установленного протокола квантового распределения ключей, модуль обработки информации; входной модуль одного узла и выходной модуль предыдущего узла связаны квантовым каналом связи, выполненным в виде оптоволоконной линии; модуль обработки информации связан с входным и выходным модулями цифровой сетью передачи данных и выполнен с возможностью принимать данные, генерировать случайные числа, зашифровывать данные, расшифровывать данные и передавать данные. 5 з.п. ф-лы, 1 ил.

RU 2708511 C1

RU 2708511 C1



RU 2708511 C1

RU 2708511 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 708 511** (13) **C1**

(51) Int. Cl.
H04L 9/08 (2006.01)
G06F 21/72 (2013.01)

(12) **ABSTRACT OF INVENTION**

(52) CPC
H04L 9/08 *(2019.05);* ***G06F 21/72*** *(2019.05)*

(21)(22) Application: **2019102923, 04.02.2019**

(24) Effective date for property rights:
04.02.2019

Registration date:
09.12.2019

Priority:
(22) Date of filing: **04.02.2019**

(45) Date of publication: **09.12.2019** Bull. № **34**

Mail address:
127287, Moskva, Staryj Petrovsko-Razumovskij pr-d, 1/23, str. 1, Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy"

(72) Inventor(s):
Zhilyaev Andrej Evgenevich (RU)

(73) Proprietor(s):
Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy" (RU)

RU 2708511 C1

(54) **METHOD OF GENERATING A KEY BETWEEN NODES OF A COMPUTER NETWORK USING A QUANTUM KEY DISTRIBUTION SYSTEM**

(57) Abstract:

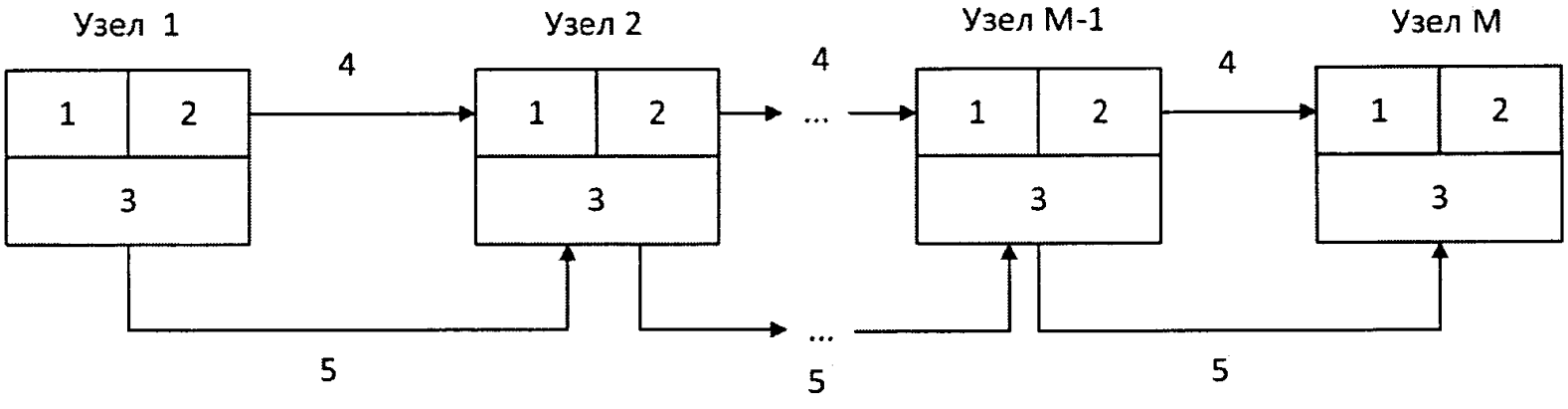
FIELD: quantum cryptography.

SUBSTANCE: technical result is achieved by a method of generating a key between two nodes of a computer network using a quantum key distribution system, wherein the network has M nodes connected in series, wherein each node includes input and output modules of quantum key distribution hardware, configured to generate quantum keys as a result of executing a set protocol of quantum key distribution, an information processing module; input module of one node and output module of the previous node are connected by a quantum communication channel made in form of a fiber-optic line; information processing module is connected to input and output modules with a digital data transmission network and is configured to receive data, generate random numbers, encrypt data, decrypt data, and transmit data.

EFFECT: technical result consists in improvement of security of transmitted key, possibility of using different encryption algorithms on each section of computer network, reduced possibility of attacks based on collection of statistics on by channels.

6 cl, 1 dwg

RU 2708511 C1



RU 2708511 C1

RU 2708511 C1

Область техники, к которой относится изобретение

Предполагаемое изобретение относится к области квантовой криптографии, а именно к формированию симметричного ключа между двумя узлами вычислительной сети с системой квантового распределения ключей.

Уровень техники

Системы квантовой криптографии - вычислительные системы, используемые для генерации идентичной последовательно нулей и единиц на двух концах квантового канала. Получаемая последовательность используется для формирования секретного симметричного ключа, называемого квантовым ключом, обладающего теоретико-информационной стойкостью и неизвестного потенциальному нарушителю.

Однако, истинный квантовый ключ возможно получить только на концах одного квантового канала, имеющего ограниченную длину. Одним из способов увеличения расстояния между узлами, для которых надо сформировать симметричный ключ, является последовательное соединение систем квантовой криптографии в вычислительную сеть. При таком удлинении на каждом участке сети генерируется истинный квантовый ключ с последующей генерацией симметричного квантового ключа между требуемыми удаленными узлами вычислительной сети.

Известен способ формирования симметричного ключа между двумя узлами сети с использованием квантового распределения ключей (патент РФ №2621605, приоритет от 02.10.2015 г.). Сеть квантового распределения ключей (КРК), включает в себя, по меньшей мере, две локальные сети с КРК, соединенные волоконно-оптическим каналом связи, причем каждая вышеупомянутая локальная сеть содержит, по меньшей мере, один сервер и, по меньшей мере, одну клиентскую часть, причем сервер включает, по меньшей мере, одну передающую серверную часть и, по меньшей мере, одну вспомогательную клиентскую часть, логически связанную с серверной передающей частью на узле.

При этом способ синхронизации ключей между клиентами, расположенными в разных локальных сетях с квантовым распределением ключей, включает в себя:

• осуществление процесса квантового распределения общего секретного ключа между первым клиентом и первым сервером, которые соединены между собой волоконно-оптическим каналом связи и расположены в первой локальной сети, при этом формируется общий ключ K1;

• осуществление процесса квантового распределения общего секретного ключа между вторым клиентом и вторым сервером, которые соединены между собой волоконно-оптическим каналом связи и расположены во второй локальной сети, при этом формируется общий ключ K3;

• осуществление процесса квантового распределения общего секретного ключа между первым сервером и вспомогательным клиентом второго сервера, которые соединены между собой волоконно-оптическим каналом связи, при этом формируется ключ K2;

После чего первый сервер просматривает позиции ключей K1 и K2 и отправляет первому клиенту номера позиций в ключе K1, значения которых не совпали со значениями в ключе K2.

Первый клиент получает номера несовпавших позиций и формирует ключ K21 путем инвертирования в ключе K1 вышеуказанных несовпавших позиций.

После чего второй сервер просматривает позиции ключей K3 и K2 и отправляет второму клиенту номера позиций в ключе K3, значения которых не совпали со значениями в ключе K2.

Второй клиент получает номера несовпавших позиций и формирует ключ K22 путем

инвертирования в ключе K3 вышеуказанных несовпавших позиций.

Данный способ имеет следующие недостатки.

Формирование симметричного ключа между крайними узлами (клиентами из локальных подсетей) происходит с передачей существенного объема информации о квантовых ключах, что позволяет проводить атаки, которые основаны на сборе статистики по побочным каналам.

Также процесс формирования симметричного ключа основан на сравнении с опорным ключом K2, что затрудняет масштабируемость сети и позволяет формировать симметричный ключ только между узлами из разных подсетей.

Известен также способ формирования симметричного ключа с использованием системы КРК (Tajima A. et al. Quantum key distribution network for multiple applications, Quantum Science and Technology, 2017, v. 2, №3, статья по адресу: http://iopscience.iop.org/article/10.1088/2058-9565/aa7154/meta).

Для формирования квантового ключа между двумя удаленными узлами используется цепь последовательно соединенных узлов, имеющими в составе входной и выходной модули аппаратуры КРК. Сначала генерируются квантовые ключи между всеми последовательно соединенными узлами в цепочке. Затем в качестве требуемого квантового ключа принимается полученный квантовый ключ между первым и вторым узлом цепочки.

После этого осуществляется передача квантового ключа до последнего узла цепочки следующим способом:

Начиная со второго узла цепочки передаваемый ключ смешивается с квантовым ключом между текущим и следующим узлом цепочки с помощью операции XOR (исключающее ИЛИ) с использованием шифра типа одноразовый блокнот. Полученное зашифрованное сообщение посылается в следующий узел цепочки. Далее зашифрованное сообщение расшифровывается с помощью шифра типа одноразовый блокнот на квантовом ключе между текущим и предыдущим узлом цепочки. В результате, на промежуточном узле цепочки получается передаваемый квантовый ключ в явном виде.

Такая передача повторяется до тех пор, пока передаваемый квантовый ключ не окажется на последнем узле цепочки. В результате, на первом и последнем узле получается идентичный симметричный квантовый ключ.

Известный способ принят за прототип.

Однако, известный способ имеет недостатки.

Перед очередной пересылкой на каждом узле сети КРК необходимо расшифровывать и зашифровывать один и тот же квантовый ключ, в результате чего ключ появляется в открытом виде на каждом узле, что делает возможным случайное или преднамеренное получение передаваемого ключа злоумышленником при получении им доступа к любому узлу, в связи с чем передаваемый ключ может оказаться скомпрометированным.

При этом в качестве квантового ключа выбирается один из сформированных квантовых ключей, что снижает защищенность передаваемого ключа за счет возможности проведение атак, которые основаны на сборе статистики по побочным каналам, и утечки дополнительной информации о передаваемом ключе злоумышленнику во время непосредственно выработки квантового ключа между первым и вторым узлом.

Помимо этого, не обеспечивается возможность использования разных алгоритмов шифрования на каждом промежуточном звене.

Раскрытие изобретения

Техническим результатом является

1) повышение защищенности передаваемого ключа,

2) возможность использования разных алгоритмов шифрования на каждом участке вычислительной сети,

3) снижение возможности проведения атак, основанных на сборе статистики по побочным каналам.

Для этого предлагается способ формирования ключа между узлами вычислительной сети с использованием системы квантового распределения ключей, причем в сети установлены

- последовательно соединенные M узлов, причем
  - - каждый узел включает
  - входной и выходной модули аппаратуры квантового распределения ключей, выполненные с возможностью формирования квантовых ключей в результате выполнения установленного протокола квантового распределения ключей,
  - модуль обработки информации;
  - входной модуль одного узла и выходной модуль предыдущего узла связаны квантовым каналом связи, выполненным в виде оптоволоконной линии;
  - модуль обработки информации связан с входным и выходным модулями, цифровой сетью передачи данных и выполнен с возможностью
    - принимать данные,
    - генерировать случайные числа,
    - зашифровывать данные,
    - расшифровывать данные,
    - передавать данные;

способ заключается в том, что

- формируют ключ K в модуле обработки первого узла на основе случайного числа;
- генерируют квантовые ключи между всеми узлами в последовательности узлов;
- зашифровывают ключ K с помощью выбранного алгоритма шифрования в модуле обработки первого узла на квантовом ключе между первым и вторым узлом, получая исходное сообщение;
- передают исходное сообщение из первого узла во второй узел через цифровую сеть передачи данных;
- вычисляют n=2;
- (A) если n=2, то
  - принимают исходное сообщение на узле n;
  - зашифровывают исходное сообщение с помощью выбранного алгоритма шифрования в модуле обработки на узле n на квантовом ключе между узлами n и n+1, получая промежуточное сообщение,

иначе

  - принимают выходное сообщение на узле n;
  - зашифровывают выходное сообщение с помощью выбранного алгоритма шифрования в модуле обработки на узле n на квантовом ключе между узлами n и n+1, получая промежуточное сообщение,
- расшифровывают промежуточное сообщение с помощью выбранного алгоритма шифрования в модуле обработки на узле n на квантовом ключе между узлами n и n-1, получая выходное сообщение;
- передают выходное сообщение из узла n в узел n+1 через цифровую сеть передачи данных;
- вычисляют n=n+1;
- если n≠M, то переходят к этапу A;

• принимают выходное сообщение на узле М;

• расшифровывают выходное сообщение с помощью выбранного алгоритма шифрования в модуле обработки на узле М на квантовом ключе между узлом М - 1 и узлом М, получая ключ К.

Для повышения защищенности передаваемого квантового ключа К на промежуточных узлах используются коммутативные шифры, позволяющие осуществлять специальный порядок преобразований, в результате которого промежуточное сообщение оказывается отличным от передаваемого ключа К.

Коммутативный шифр - шифр для которого выполняется свойство:

$$D_{K1}(E_{K2}(E_{K1}(X))) = E_{K2}(X), \quad (1)$$

где D_{Ki} - функция расшифрования на ключе Ki,

E_{Ki} - функция зашифрования на ключе Ki,

Ki - используемый ключ шифрования,

X - сообщение.

В качестве таких шифров могут использоваться, по меньшей мере следующие: шифр типа одноразовый блокнот, поточный алгоритм шифрования (кроме само синхронизирующихся поточных алгоритмов шифрования), блочный алгоритм шифрования (любой) в режиме гаммирования, блочный алгоритм шифрования (любой) в режиме связи по выходу (OFB).

В результате, согласно предложенному способу, на промежуточный узел, допустим, без ограничения общности, узел 2, поступает зашифрованное сообщение

$$C_1 = E_{k_{1,2}}(K)$$

Здесь и далее $k_{i,j}$ - это квантовый ключ между узлами i и j.

В результате первого преобразования получают промежуточное сообщение

$$C' = E_{k_{2,3}}(C_1) = E_{k_{2,3}}(E_{k_{1,2}}(K))$$

Нетрудно показать, что, в общем случае, $C' \neq K$.

Затем в результате второго преобразования получают для передачи на следующий узел выходное зашифрованное сообщение

$$C_2 = D_{k_{1,2}}(C')$$

В силу свойства (1) для применяемых алгоритмов шифрования, можно показать, что

$$C_2 = E_{k_{2,3}}(K)$$

Таким образом, на рассматриваемом узле 2 никогда не появляется в незашифрованном виде ключ К, следовательно, повышается защищенность передаваемого ключа.

Более того, за счет формирования квантового ключа К непосредственно на первом узле и отсутствия взаимной информации между этим ключом К и квантовыми ключами между соседними узлами сети достигается снижение информации, доступной злоумышленнику для проведения атак по побочным каналам.

На различных участках вычислительной сети можно использовать различные алгоритмы шифрования, удовлетворяющие свойству (1). Выбор алгоритма шифрования для конкретного участка может производиться исходя из скорости генерации квантовых ключей на данном участке, а также требуемой стойкости шифрования. Выбор алгоритма

шифрования производится до начала формирования симметричного ключа.

Краткое описание чертежей

На фигуре графического изображения показана схема вычислительной сети с использованием системы квантового распределения ключей.

Использованы следующие обозначения:

1 - входной модуль аппаратуры КРК,

2 - выходной модуль аппаратуры КРК,

3 - модуль обработки информации,

4 - квантовый канал связи на основе оптоволокна,

5 - канал цифрой сети передачи данных.

Осуществление изобретения

Для реализации предложенного способа надо сначала сформировать вычислительную сеть с узлами, содержащими входной, выходной модули аппаратуры КРК, соединенные последовательно квантовым каналом, и модули обработки информации, связанные последовательно через цифровую сеть передачи данных.

В качестве входного и выходного модулей аппаратуры КРК можно, например, использовать известную однопроходную систему КРК (патент РФ №2665249).

Входной модуль аппаратуры КРК должен быть связан с выходным модулем аппаратуры КРК предыдущего узла оптоволоконной линией.

На каждом узле необходимо установить модуль обработки информации с возможностью принимать, передавать, обрабатывать данные и генерировать случайное число. Для модуля обработки информации используем процессор общего назначения Intel Core i7 с операционной системой Linux. Для обеспечения связи через цифровую сеть передачи данных используется, например, ПО ОС Linux.

В качестве протокола КРК может применяться любой протокол с фазовым кодированием, например, протокол ГОКС (Молотков С.Н. О стойкости волоконной квантовой криптографии при произвольных потерях в канале связи: запрет измерений с определенным исходом // Письма в Журнал экспериментальной и теоретической физики, т. 106, 2014).

Для простоты описания осуществления изобретения в качестве алгоритма шифрования выберем одноразовый блокнот. Тогда функции зашифрования и расшифрования сообщения X на ключе k будут иметь вид:

$$E_K(X) = X \oplus k,$$

$$D_K(X) = X \oplus k$$

Схематичное изображение используемой сети представлено на фигуре графического изображения.

После сформирования программно-аппаратной части можно выполнить предложенный способ.

Используя генератор случайных чисел первого узла, находящийся, например, в выходном модуле аппаратуры КРК, формируют ключ К, например, длиной 256 бит.

Затем генерируются квантовые ключи $k_{i,(i+1)}$ длиной 256 бит для i от 1 до M - 1, при условии, что в сети последовательно соединены M узлов.

Осуществляется формирование зашифрованного сообщения

$$C_1 = K \oplus k_{1,2}$$

и передача данного сообщения на второй узел сети.

Начиная со второго узла, производится вычисление промежуточного сообщения

$$C' = C_{i-1} \oplus k_{i,i+1}$$

и дальнейшее вычисление выходного сообщения

$$C_{i+1} = C' \oplus k_{i-1,i}$$

Затем сформированное сообщение C_i передают на следующий узел i+1. Вычисление и передача выполняется для i от 2 до M - 1, т.е. до передачи сообщения C_{M-1} на последний узел M. На данном узле производится расшифрование полученного сообщения C_{M-1}, т.е. операция

$$C_{M-1} \oplus k_{M-1,M} = K$$

и на узле M получают ключ K, сформированный на первом узле.

(57) Формула изобретения

1. Способ формирования ключа между узлами вычислительной сети с использованием системы квантового распределения ключей, причем в сети установлены последовательно соединенные M узлов, причем

каждый узел включает

входной и выходной модули аппаратуры квантового распределения ключей, выполненные с возможностью формирования квантовых ключей в результате выполнения установленного протокола квантового распределения ключей,

модуль обработки информации;

входной модуль одного узла и выходной модуль предыдущего узла связаны квантовым каналом связи, выполненным в виде оптоволоконной линии;

модуль обработки информации связан с входным и выходным модулями цифровой сетью передачи данных и выполнен с возможностью

принимать данные,

генерировать случайные числа,

зашифровывать данные,

расшифровывать данные,

передавать данные;

способ заключается в том, что

формируют ключ K в модуле обработки первого узла на основе случайного числа;

генерируют квантовые ключи между всеми узлами в последовательности узлов;

зашифровывают ключ K с помощью выбранного алгоритма шифрования в модуле обработки первого узла на квантовом ключе между первым и вторым узлом, получая исходное сообщение;

передают исходное сообщение из первого узла во второй узел через цифровую сеть передачи данных;

вычисляют n=2;

(A) если n=2, то

принимают исходное сообщение на узле n;

зашифровывают исходное сообщение с помощью выбранного алгоритма шифрования в модуле обработки на узле n на квантовом ключе между узлами n и n+1, получая промежуточное сообщение;

иначе

принимают выходное сообщение на узле n;

зашифровывают выходное сообщение с помощью выбранного алгоритма

шифрования в модуле обработки на узле n на квантовом ключе между узлами n и n+1, получая промежуточное сообщение,

расшифровывают промежуточное сообщение с помощью выбранного алгоритма шифрования в модуле обработки на узле n на квантовом ключе между узлами n и n-1, получая выходное сообщение;

передают выходное сообщение из узла n в узел n+1 через цифровую сеть передачи данных;

вычисляют n=n+1;

если n≠M, то переходят к этапу A;

принимают выходное сообщение на узле M;

расшифровывают выходное сообщение с помощью выбранного алгоритма шифрования в модуле обработки на узле M на квантовом ключе между узлом M-1 и узлом M, получая ключ K.

2. Способ по п. 1, в котором для шифрования выбирается шифр, для которого выполняется свойство

$$D_{K1}(E_{K2}(E_{K1}(X))) = E_{K2}(X),$$

где D_{Ki} - функция расшифрования на ключе Ki,

E_{Ki} - функция зашифрования на ключе Ki,

Ki - используемый ключ шифрования,

X - сообщение.

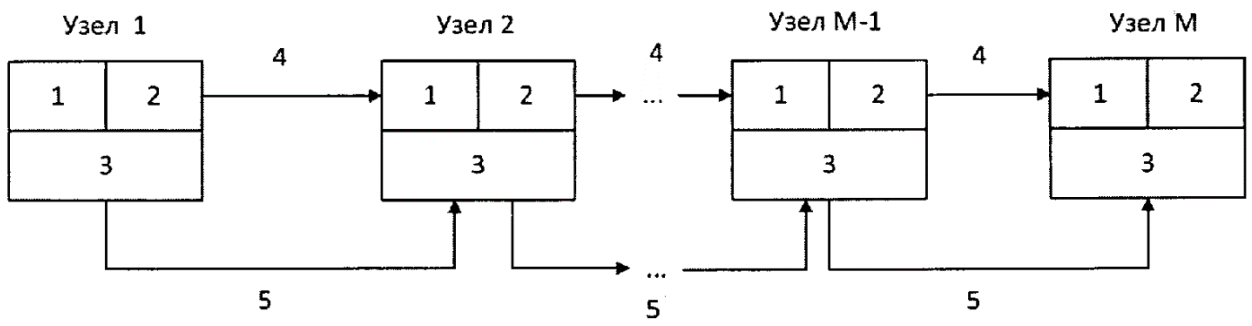
3. Способ по п. 2, в котором для шифрования выбирается шифр типа одноразовый блокнот.

4. Способ по п. 2, в котором для шифрования выбирается поточный алгоритм шифрования (кроме самосинхронизирующихся поточных алгоритмов шифрования).

5. Способ по п. 2, в котором для шифрования выбирается блочный алгоритм шифрования в режиме гаммирования.

6. Способ по п. 2, в котором для шифрования выбирается блочный алгоритм шифрования в режиме связи по выходу (OFB).

1



РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ

№ 2752844

Система выработки и распределения ключей и способ распределенной выработки ключей с использованием квантового распределения ключей (варианты)

Патентообладатель: ***Акционерное общество "Информационные технологии и коммуникационные системы" (RU)***

Автор(ы): ***Жиляев Андрей Евгеньевич (RU)***

Заявка № **2020140774**

Приоритет изобретения **10 декабря 2020 г.**

Дата государственной регистрации в Государственном реестре изобретений Российской Федерации **11 августа 2021 г.**

Срок действия исключительного права на изобретение истекает **10 декабря 2040 г.**

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 752 844**(13) **C1**

(51) МПК
H04L 9/08 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 9/0855 (2021.02)

(21)(22) Заявка: **2020140774, 10.12.2020**

(24) Дата начала отсчета срока действия патента:
10.12.2020

Дата регистрации:
11.08.2021

Приоритет(ы):
(22) Дата подачи заявки: **10.12.2020**

(45) Опубликовано: **11.08.2021** Бюл. № **23**

Адрес для переписки:
127287, Москва, ул. Мишина, 56, стр. 2, пом. IX, комн. 29, Акционерное общество "Информационные технологии и коммуникационные системы"

(72) Автор(ы):
Жиляев Андрей Евгеньевич (RU)

(73) Патентообладатель(и):
Акционерное общество "Информационные технологии и коммуникационные системы" (RU)

(56) Список документов, цитированных в отчете о поиске: **US 10348493 B2, 09.07.2019. US 2016/013936 A1, 14.01.2016. US 8041039 B2, 18.10.2018. RU 2736870 C1, 23.11.2020.**

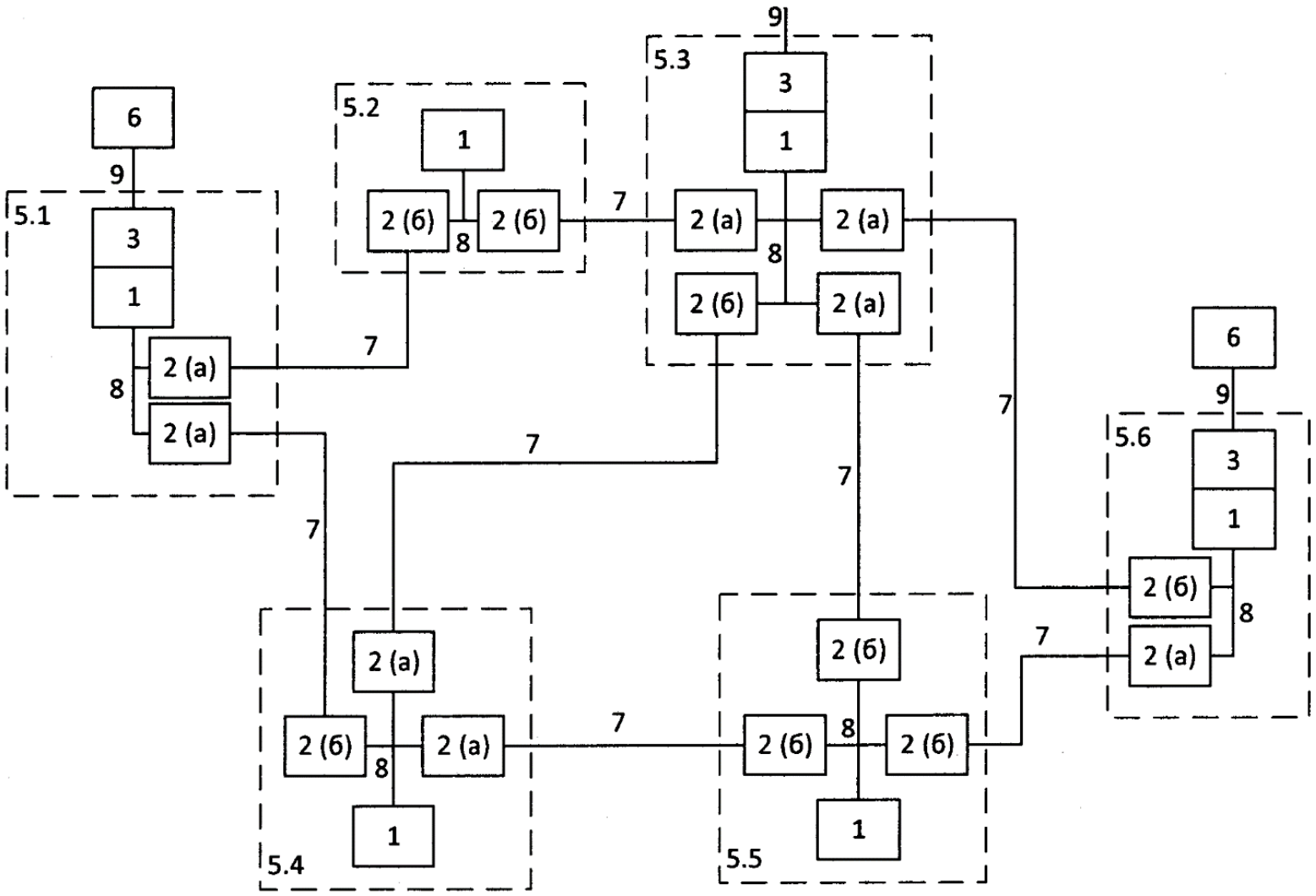
(54) Система выработки и распределения ключей и способ распределенной выработки ключей с использованием квантового распределения ключей (варианты)

(57) Реферат:

Изобретение относится к системам генерации ключей с использованием технологии квантового распределения ключей (КРК) для криптографических средств защиты информации. Техническим результатом является повышение отказоустойчивости системы за счет децентрализованной обработки запросов пользовательских ключей и расчета квантовых маршрутов. Вырабатывают классический пользовательский ключ в первом и последнем узле сети КРК зарезервированного квантового маршрута в модулях выработки пользовательских ключей с использованием предварительных ключей согласно выбранному порядку выработки классического пользовательского ключа. Вырабатывают в модулях выработки пользовательских ключей первого и последнего узлов сети КРК зарезервированного квантового маршрута пользовательский ключ с использованием квантового пользовательского ключа и классического пользовательского ключа согласно выбранному порядку объединения квантового пользовательского ключа и классического пользовательского ключа. Передают выработанный пользовательский ключ из модуля выработки пользовательского ключа первого и последнего узлов сети КРК зарезервированного квантового маршрута в модули управления пользовательскими ключами первого и последнего узлов сети КРК зарезервированного квантового маршрута. Сохраняют в хранилище пользовательских ключей модуля управления пользовательскими ключами узла сети КРК полученный пользовательский ключ. Передают пользовательский ключ из хранилища пользовательских ключей модуля управления пользовательскими ключами узла сети КРК в шифратор пользователя, запросивший пользовательский ключ. 4 н. и 6 з.п. ф-лы, 2 ил., 2 табл.

RU 2752844 C1

RU 2752844 C1



Фиг. 1

RU 2752844 C1

RU 2752844 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 752 844**(13) **C1**

(51) Int. Cl.
H04L 9/08 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 9/0855 (2021.02)

(21)(22) Application: **2020140774, 10.12.2020**

(24) Effective date for property rights:
10.12.2020

Registration date:
11.08.2021

Priority:
(22) Date of filing: **10.12.2020**

(45) Date of publication: **11.08.2021** Bull. № **23**

Mail address:
127287, Moskva, ul. Mishina, 56, str. 2, pom. IX, komn. 29, Aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy"

(72) Inventor(s):
Zhilyaev Andrej Evgenevich (RU)

(73) Proprietor(s):
Aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy" (RU)

RU 2752844 C1

(54) KEY GENERATION AND DISTRIBUTION SYSTEM AND METHOD FOR DISTRIBUTED KEY GENERATION USING QUANTUM KEY DISTRIBUTION (OPTIONS)

(57) Abstract:

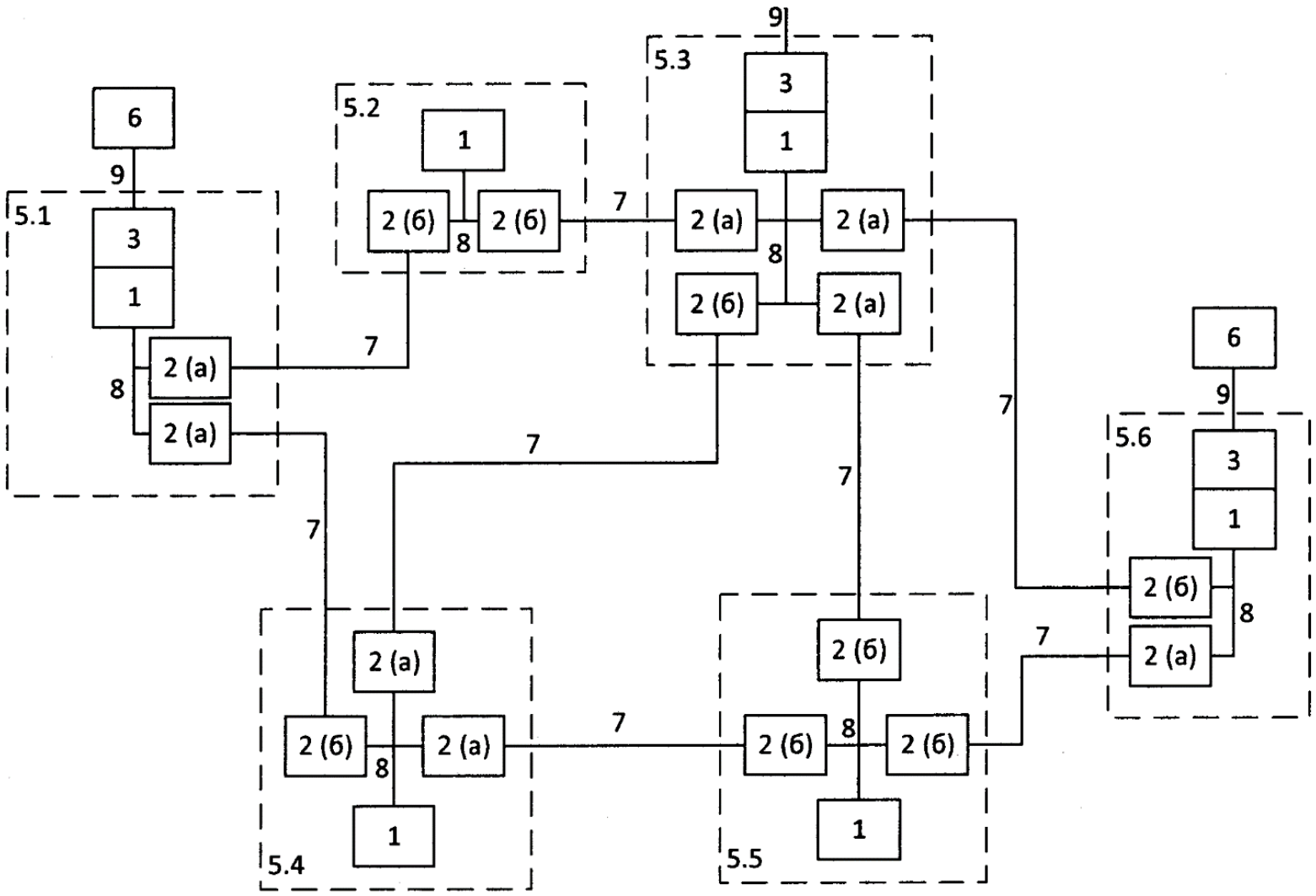
FIELD: information protection.

SUBSTANCE: invention relates to key generation systems using quantum key distribution (hereinafter – QKD) technology for cryptographic information protection tools. A classic user key is generated in the first and last node of the QKD network of the reserved quantum route in the modules for generating user keys using preliminary keys according to the selected order of generating the classical user key. In the modules for generating user keys of the first and last nodes of the QKD network of the reserved quantum route, a user key is generated using the quantum user key and the classical user key according to the selected order of combining the quantum user key and the classical user key. The generated user key is transmitted from the module for generating user keys of the first and last nodes of the QKD network of the reserved quantum route to the modules for managing user keys of the first and last nodes of the QKD network of the reserved quantum route. The received user key is stored in the user key storage of the module for managing user keys of the QKD network node. The user key is transmitted from the user key storage of the module for managing user keys of the QKD network node to the user's encoder that requested the user key.

EFFECT: technical result is an increase in the fault tolerance of the system due to the decentralized processing of user key requests and the calculation of quantum routes.

10 cl, 2 tbl, 2 dwg

RU 2752844 C1



Фиг. 1

RU 2752844 C1

RU 2752844 C1

Область техники, к которой относится изобретение

Предлагаемое изобретение относится к области криптографической защиты информации, и, в частности, к системам генерации ключей с использованием технологии квантового распределения ключей (КРК) для криптографических средств защиты информации.

Уровень техники

Технология КРК позволяет получить идентичные ключи одновременно на двух устройствах, соединенных квантовым каналом. При этом для любого известного протокола КРК существует предельная длина квантового канала, то есть предельное удаление друг от друга двух устройств, между которыми вырабатывается квантовый ключ. Для увеличения предельной длины между двумя устройствами, на которых необходимо получить идентичный ключ, применяется подход на основе построения сетей КРК с доверенными узлами. Такие узлы последовательно соединяются квантовыми каналами, используемыми для генерации или передачи ключа между крайними устройствами.

Известна система КРК, способ и устройство на основе доверенных передатчиков (патент США №10348493, приоритет от 06.01.2016 г.). Система состоит из нескольких маршрутизирующих устройств, используемых для передачи ключей, устройства КРК, соединенного с маршрутизирующими устройствами и настроенного для построения двух или более маршрутов до другого устройства КРК с целью согласования квантового ключа и получения общего ключа. Два и более различных маршрутов между устройствами КРК могут включать одно или более маршрутизирующих устройств. Устройства КРК системы также могут объединять согласованные квантовые ключи, полученные с различных маршрутов для создания нового общего ключа. Устройства КРК системы также могут рассылать информацию о выбранном маршруте на устройства маршрутизации до начала процесса согласования квантовых ключей. Система также может иметь устройства квантового шлюза, через которые устройства КРК соединяются с устройствами передачи данных. Устройства квантового шлюза могут зашифровывать и расшифровывать данные от устройств передачи данных на квантовых ключах, полученных от устройств КРК.

В данной системе реализуется способ КРК, состоящий из выбора двух или более маршрутов между двумя устройствами квантового распределения ключей. Каждый маршрут включает одно или более устройств маршрутизации. После выбора маршрута осуществляется согласование квантовых ключей на выбранных маршрутах.

Известные система, устройство и способ имеют ряд недостатков.

Так, используется строгое разделение устройств на два типа, что не позволяет использовать устройства КРК в качестве промежуточных устройств выбранного маршрута.

Для организации сетей КРК, в которых предполагается множество устройств передачи данных, в известной системе могут возникать участки с избыточным набором устройств. Быстродействие и отказоустойчивость системы зависят от числа маршрутизирующих устройств и связей между ними. При этом система не предполагает использование устройств КРК в качестве маршрутизирующих устройств. В связи с этим может возникнуть ситуация, при которой в одной определенной точке сети (маршрута) потребуется размещать устройства обоих типов с дублированием квантовых каналов. Такая ситуация возникает, если в некотором месте сети необходимо подключать потребителей к устройству КРК, и это же место сети оптимально для построения через него маршрутов, т.е. оптимально для размещения маршрутизирующего устройства.

Также данная система использует только согласование квантовых ключей при выработке общего ключа, вследствие чего стойкость общего ключа основывается только на стойкости способов выработки квантовых ключей. Более того, стойкость итогового ключа, полученного объединением квантовых ключей с нескольких маршрутов, при пересечении этих маршрутов не превышает стойкости ключа с одного из маршрутов, т.е. использование нескольких пересекающихся маршрутов излишне.

Также в данной системе отсутствует хранилище ключей как квантовых, так и общих. Частота запросов общего ключа может меняться с течением времени и существенно превышать возможности системы по генерации общих ключей в периоды пиковой нагрузки, что приведет к длительному ожиданию новых общих ключей.

Известна централизованная сеть мониторинга и управления и способ передачи квантового ключа в сети (заявка США №20190260581, приоритет от 03.05.2019 г.).

Централизованная сеть содержит

• централизованный контроллер,

• N узлов обслуживания, сконфигурированных для обеспечения связи друг с другом,

• M ключевых узлов, сконфигурированных для предоставления квантовых ключей N узлам обслуживания,

при этом

• каждый из N узлов обслуживания соответствует одному из M ключевых узлов, и как N, так и M являются целыми числами, большими или равными 2.

Централизованный контроллер содержит

• процессор,

• блок памяти, сконфигурированный для хранения программ и команд,

• приемопередатчик.

Каждый ключевой узел содержит

• приемопередатчик,

• хранилище ключей, сконфигурированное для хранения квантовых ключей,

• процессор ретрансляции ключей.

Приемопередатчик сконфигурирован с возможностью

• сообщения информации о топологии ключевого узла централизованному контроллеру,

• приема команды ретрансляции ключа, доставляемой централизованным контроллером.

Процессор ретрансляции ключей выполнен с возможностью выполнения квантовой ретрансляции ключей на основе команды ретрансляции ключей, доставленной централизованным контроллером.

Способ заключается в том, что

• получают централизованным контроллером централизованной сети управления и контроля Z запросов на обслуживание, каждый из которых запрашивает передачу услуги, которая должна быть выполнена между двумя узлами обслуживания, где Z является целым числом, большим или равным 1;

• определяют централизованным контроллером на основе каждого из Z запросов на обслуживание, исходный узел обслуживания и целевой узел обслуживания, соответствующие каждому запросу на обслуживания, и параметр потребления квантового ключа соответствующего запроса на обслуживания, при этом исходный узел обслуживания соответствует исходному ключевому узлу в M ключевых узлах, а целевой узел обслуживания соответствует целевому ключевому узлу в M ключевых узлах;

• определяют централизованным контроллером команды ретрансляции ключей, соответствующие запросам на обслуживание G в запросах на обслуживание Z, на основе

○ идентификатора исходного узла обслуживания и идентификатора целевого узла обслуживания, соответствующего каждому из Z запросов на обслуживание,

○ параметра потребления квантового ключа каждого из Z запросов на обслуживание, и

○ топологической информации M ключевых узлов в централизованной сети управления и контроля, где G является целым числом, меньшим или равным Z и большим или равным 1, и при этом каждая команда ретрансляции ключа задает путь для ретрансляции квантового ключа между исходным ключевым узлом и целевому ключевому узлом соответствующего запроса на обслуживание;

• доставляют централизованным контроллером команды ретрансляции ключей, соответствующие запросам на обслуживание G, в ключевые узлы, соответствующие командам ретрансляции ключей, так что ключевые узлы выполняют ретрансляцию квантовых ключей на основе команд ретрансляции ключей, чтобы генерировать соответствующие совместно используемые квантовые ключи между соответствующим исходным узлом обслуживания и целевыми ключевыми узлами. Топологическая информация M ключевых узлов в централизованной сети управления и контроля может содержать:

• идентификатор каждого ключевого узла,

• состояние квантовой линии связи между каждым ключевым узлом и одним или несколькими другими ключевыми узлами, и

• вес ребра, соединяющего два соседних ключевых узла, на каждом пути от исходного ключевого узла до ключевого узла назначения соответствующего запроса на обслуживание.

Известные способ и устройство имеют ряд недостатков.

Так, централизованный контроллер является точкой отказа всей сети и узким местом в вычислении инструкций по передаче ключа при наличии большого числа сервисных запросов.

Наличие единственное ключевое хранилище в каждом ключевом узле, при получении злоумышленником доступа к нему, может привести к компрометации как квантовых ключей, используемых для защиты при передаче ключей согласно инструкциям централизованного контроллера, так и квантовых ключей, переданных согласно инструкции.

Ретрансляция ключей в способе предполагает передачу одного выработанного квантового ключа на целевой ключевой узел. Таким образом, стойкость итогового квантового ключа основывается только на стойкости протокола КРК, причем о самом квантовом ключе у злоумышленника имеется некоторая, пусть малая, информация, полученная во время выполнения протокола КРК.

Обработка запросов на обслуживание производится в централизованном контроллере, что не позволит одновременно обрабатывать запросы, поступившие на разные узлы сети, а потребует ожидать каждому запросу своей очереди в централизованном контролере.

Известные способ и устройство выбраны в качестве прототипа для первого варианта системы и способа.

Для расширения возможностей систем с КРК применяются оптические коммутаторы, позволяющие оптимизировать использование квантовых линий связи при построении систем.

Так, известна квантовая коммуникационная сеть (заявка США №2019/03794636, приоритет от 06.06.2019 г.), состоящая из узлов сети, каждый из которых оснащается оптическим коммутатором, имеющим n входов и m выходов, причем каждый узел сети содержит как устройство с источником одиночных фотонов, так и устройство с приемников одиночных фотонов. В этой коммуникационной сети реализуется способ управлений сетью, заключающийся в соединении с помощью оптических коммутаторов двух узлов сети квантовыми линиями связи, в том числе проходящие транзитом через другие узлы сети.

Известные способ и сеть имеют ряд недостатков.

Каждый узел сети имеет избыточное оборудование для обеспечения возможности подключения любого узла к любому - в каждом узле имеется как источник одиночных фотонов, так и приемник. Размещение только одного из устройств с незначительным усложнением работы коммутаторов позволит снизить стоимость одного узла.

Узлы сети с обоих концов квантового канала имеют оптический коммутатор. Согласованная работа двух коммутаторов без единого центра управления является нетривиальной задачей. Два коммутатора должны переключиться в корректное положение для соединения двух узлов сети и при этом не разрывать полученную квантовую линию из-за попыток организовать другие квантовые линии через эти коммутаторы или попыток начать выработку квантового ключа с одним из этих двух узлов. С учетом возможности организации транзитных квантовых линий количество коммутаторов, которые должны работать согласованно и не прерывать квантовую линию связи во время выработки квантовых ключей, увеличивается.

Предлагаемая сеть позволяет соединить множество пар узлов одновременно, но при этом сохраняется проблема максимальной длины квантового канала, т.е. сохраняется принципиальная проблема максимальной удаленности узлов сети, между которыми возможно выработать квантовый ключ. Способ не позволяет выработать общий ключ между узлами, расстояние между которыми превышает максимальную длину квантового канала.

Также известна защищенная система связи и способ управления каналом (патент США №8041039, приоритет от 19.04.2007 г.), содержащая центральный узел и множество удаленных узлов, соединенных с центральным квантовыми линиями связи через оптический коммутатор и каналами передачи данных через другой оптический коммутатор.

Защищенная система связи содержит

- центральный узел;
- множество удаленных узлов, каждый из которых соединен с центральным узлом через оптическую линию передачи;

причем множество каналов установлено между центральным узлом и каждым удаленным узлом;

при этом множество каналов включает в себя

- первый канал, используемый для передачи квантового сигнала,
- второй канал, используемый для передачи данных,
- причем центральный узел содержит
  - первый коммутатор для переключения первого канала для соединения с выбранным одним из удаленных узлов;
  - второй коммутатор для переключения второго канала для соединения с выбранным одним из удаленных узлов;
  - контроллер для независимого управления первым коммутатором и вторым

коммутатором таким образом, что они соединены с различными удаленными узлами, выбранными из множества удаленных узлов, для осуществления

- передачи квантового сигнала,
- формирования общего случайного числа через второй канал на основе данных, полученных путем обнаружения квантового сигнала через первый канал и/или криптографической связи с использованием криптографического ключа, извлеченного из общего случайного числа.

Используется способ управления каналом для защищенного устройства связи, соединенного с каждым из множества удаленных узлов через оптическую линию передачи,

причем множество каналов устанавливается с каждым удаленным узлом, при этом множество каналов включает в себя

• первый канал, используемый для передачи квантового сигнала, и

• второй канал, используемый для передачи данных, причем защищенное устройство связи включает в себя:

• первый переключатель для переключения первого канала для соединения с выбранным одним из удаленных узлов и

• второй переключатель для переключения второго канала для соединения с выбранным одним из удаленных узлов, причем способ управления каналом содержит:

• независимо управляют первым коммутатором и вторым коммутатором так, что они соединяются с различными удаленными узлами, выбранными из множества удаленных узлов

- для выполнения передачи квантового сигнала,
- для формирования общего случайного числа через второй канал на основе данных, полученных путем обнаружения квантового сигнала через первый канал и/или {из канала} криптографической связи с использованием криптографического ключа, извлеченного из общего случайного числа. В способе реализуется синхронное включение канала передачи данных и квантовой линии связи. Переключение каналов производится в зависимости от скорости выработки квантовых ключей на каждой линии.

Также в способе предлагается вырабатывать общий ключ для всех узлов в сети путем передачи одного квантового ключа из центрального узла на все удаленные узлы с защитой передачи с помощью шифрования типа одноразового шифр-блокнота.

Известные система и способ приняты за прототипы для второго варианта системы и способа.

Однако известная система и способ имеют следующие недостатки.

Применение двух независимых коммутаторов для коммутации квантового сигнала и передаваемых данных совместно с применением одного физического канала к каждому узлу (оптоволокна) создает повышенный риск ошибок при коммутации и передачи, более того, передача квантового сигнала требует темного волокна, т.е. необходимо прерывать передачу данных при передаче квантового сигнала в том же оптоволокне.

Также не решается проблема максимальной длины квантового канала. Максимальное расстояние между центральным и удаленным узлом не превышает длину квантового канала, расстояние между двумя удаленными узлами не превышает двух максимальных длин квантового канала, а генерация ключа строго между парой удаленных узлов оказывается невозможной.

Создание единого ключа для взаимодействия всех узлов является спорным с точки зрения безопасности, так как позволяет получить доступ третьему узлу к информации, передаваемой между двумя узлами.

Управление переключением каналов не оптимально и не учитывает потребности в квантовых ключах между удаленным и центральным узлом.

Раскрытие изобретения

Техническим результатом является

1) повышение отказоустойчивости системы за счет децентрализованной обработки запросов пользовательских ключей и расчета квантовых маршрутов,

2) повышение защищенности системы за счет двух независимых ключевых хранилищ на каждом узле,

3) повышение быстродействия за счет параллельной обработки запросов пользовательских ключей,

4) повышение стойкости пользовательских ключей за счет объединения квантового пользовательского ключа и классического пользовательского ключа,

5) устранение ограничений на максимальную удаленность двух узлов системы, между которыми вырабатывается общий ключ.

Для этого предлагается, согласно первому варианту, система выработки и распределения ключей, включающая

- множество узлов сети выработки и квантового распределения ключей (узлы сети КРК), причем
  - узлы сети КРК соединены квантовыми линиями связи так, что граф, отображающий связи квантовыми линиями, является связным;
  - узлы сети КРК соединены классической линией связи с цифровой сетью передачи данных; причем к каждому узлу сети КРК присоединено, по крайней мере, две квантовые линии связи;

при этом каждый узел сети КРК, включает

- модуль выработки пользовательских ключей,
- модуль управления пользовательскими ключами,
- по крайней мере, два модуля выработки квантовых ключей; причем
- каждый модуль выработки квантовых ключей связан с модулем выработки пользовательских ключей локальной цифровой линией передачи данных;
- модуль выработки пользовательских ключей соединен с модулем управления пользовательскими ключами локальной цифровой линией передачи данных;

при этом каждый модуль выработки квантовых ключей выполнен с возможностью

- вырабатывать квантовые ключи совместно с другим модулем выработки квантовых ключей, соединенным с данным квантовой линией связи;
- генерировать случайные числа;
- получать запросы на выработку квантового ключа от модуля выработки пользовательских ключей;
- передавать вырабатываемые квантовые ключи в модули выработки пользовательских ключей;
- передавать/получать служебные данные протокола КРК от модуля выработки пользовательских ключей;

при этом модуль выработки пользовательских ключей выполнен с возможностью

- создавать запросы на выработку квантового ключа в модули выработки квантовых ключей;
- получать квантовые ключи от модулей выработки квантовых ключей согласно переданным запросам;
- хранить квантовые ключи в хранилище квантовых ключей;
- зашифровывать данные;

• расшифровывать данные;
• аутентифицировать данные;
• проверять аутентификацию данных;
• определять топологию сети КРК;
• определять квантовый маршрут для выработки пользовательских ключей;
• вырабатывать пользовательские ключи совместно с модулями выработки пользовательских ключей других узлов сети КРК на квантовом маршруте;
• получать запросы на выработку пользовательских ключей от модулей управления пользовательскими ключами;
• передавать пользовательские ключи в модули управления пользовательскими ключами;

при этом модуль управления пользовательскими ключами выполнен с возможностью
• подключать шифраторы пользователей с помощью цифровой сети передачи данных;
• хранить пользовательские ключи в хранилище пользовательских ключей;
• определять совместно с модулями управления пользовательскими ключами других узлов сети КРК соответствие узла сети КРК и подключенных к ним шифраторов пользователей;
• формировать общую базу данных подключенных шифраторов пользователей, содержащую соответствие узлов сети КРК и подключенных к ним шифраторов пользователей;
• формировать запросы на выработку пользовательского ключа в модули выработки пользовательских ключей;
• получать пользовательские ключи от модулей выработки пользовательских ключей согласно переданным запросам.

Для работы системы предлагается способ выработки и распределения пользовательских ключей в системе заключающийся в том, что
• выбирают порядок выработки квантового пользовательского ключа;
• выбирают порядок выработки классического пользовательского ключа;
• выбирают порядок объединения квантового пользовательского ключа и классического пользовательского ключа;
• загружают предварительные ключи в модули выработки пользовательских ключей узлов сети КРК, причем в каждый модуль выработки пользовательских ключей загружается N-1 ключ, где N - число узлов сети КРК;
• загружают в модуль выработки пользовательских ключей каждого узла сети КРК идентификационную информацию для связи с другими узлами сети КРК, которые соединены квантовой линией связи с данным узлом сети КРК;
• загружают в каждый модуль управления пользовательскими ключами идентификационную информацию подключенных к ним шифраторов пользователей;
• передают из модуля управления пользовательскими ключами каждого узла сети КРК в модули управления пользовательскими ключами всех остальных узлов сети КРК данные о подключенных шифраторах пользователей;
• получают в модуле управления пользовательскими ключами каждого узла сети КРК переданную информацию о подключенных шифраторах пользователей и записывают ее в общую базу данных подключенных шифраторов пользователей;
• передают из модуля выработки пользовательских ключей каждого узла сети КРК в модули выработки пользовательских ключей остальных узлов сети КРК идентификационную информацию всех соседних с ним узлов сети КРК,
• получают в модуле выработки пользовательских ключей каждого узла сети КРК

переданную ему идентификационную информацию соседних узлов и на ее основе формируют топологию сети КРК,

• получают запрос пользовательского ключа от шифратора пользователя, подключенного к модулю управления пользовательскими ключами узла сети КРК, причем запрос включает идентификационную информацию шифратора пользователя, для связи с которым необходим пользовательский ключ;

• определяют из общей базы данных подключенных шифраторов пользователей узел сети КРК, к которому подключен шифратор пользователя, для связи с которым необходим пользовательский ключ;

• формируют в модуле управления пользовательскими ключами узла сети КРК запрос пользовательского ключа с указанием идентификационной информации текущего узла сети КРК и узла сети КРК, определенного по общей базе данных подключенных шифраторов пользователей;

• передают сформированный запрос пользовательского ключа из модуля управления пользовательскими ключами в модуль выработки пользовательских ключей узла сети КРК;

• принимают в модуле выработки пользовательских ключей запрос пользовательского ключа от модуля управления пользовательскими ключами;

• определяют последовательность узлов сети КРК (квантовый маршрут) и количество k узлов в квантовом маршруте от узла сети КРК, получившего запрос пользовательского ключа, до узла сети КРК, указанного в запросе пользовательского ключа, с помощью топологии сети КРК;

• резервируют квантовый маршрут, передавая из модуля выработки пользовательских ключей узла сети КРК, получившего запрос пользовательского ключа, в модули выработки пользовательских ключей узлов сети КРК, с идентификаторами, соответствующими остальным идентификаторам узлов сети КРК в квантовом маршруте, сообщения о резервировании квантового маршрута;

• вычисляют i=1;

• (A) посылают запрос выработки квантового ключа из модуля выработки пользовательских ключей в модуль выработки квантовых ключей i-го узла зарезервированного квантового маршрута и из модуля выработки пользовательских ключей в модуль выработки квантовых ключей (i+1)-го узла зарезервированного квантового маршрута, причем

○ если i-й узел сети КРК имеет несколько модулей выработки квантового ключа, то посылают запрос в модуль выработки квантовых ключей, соединенный квантовой линией связи с (i+1)-м узлом сети КРК;

○ если (i+1)-й узел сети КРК имеет несколько модулей выработки квантового ключа, то посылают запрос в модуль выработки квантовых ключей, соединенный квантовой линией связи с i-м узлом сети КРК;

• вырабатывают квантовый ключ в модулях выработки квантового ключа i-го и (i+1)-го узлов сети КРК;

• передают полученный квантовый ключ из модуля выработки квантового ключа в модуль выработки пользовательских ключей на i-м и (i+1)-м узле сети КРК;

• помещают полученный квантовый ключ в хранилища квантовых ключей модулей выработки пользовательских ключей i-го и (i+1)-го узлов сети КРК;

• если i<k-1, то

○ вычисляют i=i+1;

○ переходят к этапу A;

• запрашивают случайное число в модуле выработки пользовательских ключей от модуля выработки квантовых ключей узла сети КРК с идентификатором, соответствующему первому узлу сети КРК зарезервированного квантового маршрута;

• вырабатывают запрошенное случайное число с помощью генератора случайных чисел модуля выработки квантовых ключей;

• передают выработанное случайное число из модуля выработки квантовых ключей в модуль выработки пользовательских ключей узла сети КРК с идентификатором, соответствующему первому узлу зарезервированного квантового маршрута;

• вырабатывают на первом и последнем узле сети КРК зарезервированного квантового маршрута квантовый пользовательский ключ с помощью случайного числа в модуле выработки пользовательских ключей первого узла сети КРК и квантовых ключей в хранилищах квантовых ключей узлов сети КРК, входящих в зарезервированный квантовый маршрут, согласно выбранному порядку выработки квантового пользовательского ключа;

• вырабатывают классический пользовательский ключ в первом и последнем узле сети КРК зарезервированного квантового маршрута в модулях выработки пользовательских ключей с использованием предварительных ключей согласно выбранному порядку выработки классического пользовательского ключа;

• вырабатывают в модулях выработки пользовательских ключей первого и последнего узлов сети КРК зарезервированного квантового маршрута пользовательский ключ с использованием квантового пользовательского ключа и классического пользовательского ключа согласно выбранному порядку объединения квантового пользовательского ключа и классического пользовательского ключа;

• передают выработанный пользовательский ключ из модуля выработки пользовательского ключа первого и последнего узлов сети КРК зарезервированного квантового маршрута в модули управления пользовательскими ключами первого и последнего узлов сети КРК зарезервированного квантового маршрута;

• сохраняют в хранилище пользовательских ключей модуля управления пользовательскими ключами узла сети КРК полученный пользовательский ключ;

• передают пользовательский ключ из хранилища пользовательских ключей модуля управления пользовательскими ключами узла сети КРК в шифратор пользователя, запросивший пользовательский ключ.

В предложенном способе может быть предусмотрено, что

• определяют в модулях выработки пользовательских ключей и передают другим модулям выработки пользовательских ключей топологические метрики сети КРК, которыми дополняют топологию сети КРК, причем топологические метрики включают

○ количество квантовых ключей в хранилище квантовых ключей;

○ скорость выработки квантовых ключей с соседними узлами сети КРК;

○ скорость расходования и количество квантовых ключей на зарезервированных квантовых маршрутах;

• при определении квантового маршрута модули выработки пользовательских ключей учитывают топологические метрики, которыми дополнена топология сети КРК;

• при резервировании квантового маршрута сообщение о резервировании дополняется информацией о количестве необходимых квантовых ключей для резервирования.

В предложенном способе также может быть предусмотрено, что запрос квантового ключа к модулю выработки квантовых ключей содержит характеристики запрашиваемого квантового ключа: длину, максимальное время готовности квантового ключа, режим выработки ключа.

Кроме этого, в предложенном способе может быть предусмотрено, что запрос пользовательского ключа к модулю управления пользовательскими ключами содержит характеристики запрашиваемого квантового ключа: длину, максимальное время готовности пользовательского ключа, необходимость применения классического пользовательского ключа при вычислении пользовательского ключа.

Также предлагается, согласно второму варианту, система выработки и распределения ключей, включающая

• множество узлов сети выработки и квантового распределения ключей (узлы сети КРК), причем

○ узлы сети КРК соединены квантовыми линиями связи, так, что граф, отображающий связи квантовыми линиями, является связным;

○ узлы сети КРК соединены классической цифровой сетью передачи данных;

причем к каждому узлу сети КРК присоединено, по крайней мере, две квантовые линии связи;

при этом узел сети КРК включает

• модуль выработки пользовательских ключей,

• модуль управления пользовательскими ключами,

• по крайней мере, два модуля выработки квантовых ключей;

причем соединение с квантовыми линиями связи узлов сети КРК может быть выполнено как напрямую, так и через оптический коммутатор; причем

• количество оптических коммутаторов не превышает количество узлов сети КРК;

• каждый оптический коммутатор имеет один оптический вход и т оптических выходов, позволяющих подключать до т квантовых линий связи к одному узлу сети КРК;

• каждый оптический коммутатор соединен локальной цифровой линией передачи данных с модулем выработки пользовательских ключей, подключенным квантовой линией связи к оптическому входу оптического коммутатора;

при этом каждый модуль управления пользовательскими ключами соединен с модулем выработки пользовательских ключей локальной цифровой линией передачи данных и выполненный с возможностью

• получать и передавать данные в шифраторы пользователей через цифровую сеть передачи данных;

• хранить пользовательские ключи в хранилище пользовательских ключей;

• определять совместно с модулями управления пользовательскими ключами других узлов сети КРК соответствие узла сети КРК и подключенных к ним шифраторов пользователей;

• формировать общую базу данных подключенных шифраторов пользователей, содержащую соответствие узлов сети КРК и подключенных к ним шифраторов пользователей;

• создавать запросы на выработку пользовательского ключа в модули выработки пользовательских ключей;

• получать пользовательские ключи от модулей выработки пользовательских ключей согласно переданным запросам;

при этом каждый модуль выработки квантовых ключей связан с модулем выработки пользовательских ключей локальной цифровой линией передачи данных и выполнен с возможностью

• вырабатывать квантовые ключи совместно с другим модулем выработки квантовых ключей, соединенным квантовой линией связи;

• генерировать случайные числа;

• получать запросы на выработку квантового ключа от модуля выработки пользовательских ключей;

• передавать вырабатываемые квантовые ключи в модули выработки пользовательских ключей;

• передавать и получать служебные данные протокола КРК из модуля выработки пользовательских ключей;

при этом модуль выработки пользовательских ключей выполнен с возможностью

• создавать запросы на выработку квантового ключа в модули выработки квантовых ключей;

• получать квантовые ключи от модулей выработки квантовых ключей согласно переданным запросам;

• хранить квантовые ключи в хранилище квантовых ключей;

• зашифровывать данные;

• расшифровывать данные;

• осуществлять аутентификацию данных;

• проверять аутентификацию данных;

• определять топологию сети КРК;

• определять квантовый маршрут для выработки пользовательских ключей;

• управлять коммутацией каналов внутри оптического коммутатора;

• вырабатывать пользовательские ключи совместно с модулями выработки пользовательских ключей других узлов сети КРК на квантовом маршруте,

• получать запросы на выработку пользовательских ключей от модулей управления пользовательскими ключами;

• передавать пользовательские ключи в модули управления пользовательскими ключами.

Для работы системы, согласно второму варианту, предлагается способ выработки и распределения пользовательских ключей в системе, заключающийся в том, что

• выбирают порядок выработки квантового пользовательского ключа;

• выбирают порядок выработки классического пользовательского ключа;

• выбирают порядок объединения квантового пользовательского ключа и классического пользовательского ключа;

• загружают предварительные ключи в модули выработки пользовательских ключей узлов сети КРК, причем в каждый модуль выработки пользовательских ключей загружается N-1 ключ, где N - число узлов сети КРК;

• загружают в модуль выработки пользовательских ключей каждого узла сети КРК идентификационную информацию для связи с другими узлами сети КРК, которые соединены квантовой линией связи с данным узлом сети ККР;

• загружают в каждый модуль управления пользовательскими ключами идентификационную информацию подключенных к ним шифраторов пользователей;

• передают из модуля управления пользовательскими ключами каждого узла сети КРК в модули управления пользовательскими ключами всех остальных узлов сети КРК данные о подключенных шифраторах пользователей;

• получают в модуле управления пользовательскими ключами каждого узла сети КРК переданную информацию о подключенных шифраторах пользователей и собирают ее в общую базу данных подключенных шифраторов пользователей;

• передают из модуля выработки пользовательских ключей каждого узла сети КРК в модули выработки пользовательских ключей всех остальных узлов сети КРК

идентификационную информацию всех соседних с ним узлов сети КРК;

• получают в модуле выработки пользовательских ключей каждого узла сети КРК переданную ему идентификационную информацию соседних узлов и на ее основе формируют топологию сети КРК;

• получают запрос пользовательского ключа от шифратора пользователя, подключенного к модулю управления пользовательскими ключами узла сети КРК, причем запрос включает идентификационную информацию шифратора пользователя, для связи с которым необходим пользовательский ключ;

• определяют по общей базе данных подключенных шифраторов пользователей узел сети КРК, к которому подключен шифратор пользователя, для связи с которым необходим пользовательский ключ;

• формируют в модуле управления пользовательскими ключами узла сети КРК запрос пользовательского ключа с указанием идентификационной информации узла сети КРК, получившего запрос пользовательского ключа, и узла сети КРК, определенного по общей базе данных подключенных шифраторов пользователей;

• передают сформированный запрос пользовательского ключа из модуля управления пользовательскими ключами в модуль выработки пользовательских ключей узла сети КРК;

• принимают в модуле выработки пользовательских ключей запрос пользовательского ключа от модуля управления пользовательскими ключами;

• определяют последовательность узлов сети КРК (квантовый маршрут) и количество k узлов в квантовом маршруте от узла сети КРК, получившего запрос пользовательского ключа, до узла сети КРК, указанного в запросе пользовательского ключа, с помощью топологии сети КРК;

• резервируют квантовый маршрут, передавая из модуля выработки пользовательских ключей узла сети КРК, получившего запрос пользовательского ключа, в модули выработки пользовательских ключей узлов сети КРК, с идентификаторами, соответствующими остальным идентификаторам узлов сети КРК в зарезервированном квантовом маршруте сообщения о резервировании квантового маршрута;

• вычисляют i=1;

• (A) посылают запрос выработки квантового ключа из модуля выработки пользовательских ключей в модуль выработки квантовых ключей i-го узла зарезервированного квантового маршрута и из модуля выработки пользовательских ключей в модуль выработки квантовых ключей (i+1)-го узла зарезервированного квантового маршрута, причем

○ если i-й узел сети КРК имеет несколько модулей выработки квантового ключа, то посылают запрос в модуль выработки квантовых ключей, соединенный квантовой линией связи с (i+1)-М узлом сети КРК;

○ если (i+1)-й узел сети КРК имеет несколько модулей выработки квантового ключа, то посылают запрос в модуль выработки квантовых ключей, соединенный квантовой линией связи с i-м узлом сети КРК;

• если модули выработки квантовых ключей i-го и (i+1)-го узла сети КРК связаны квантовым каналом связи через оптический коммутатор, то

○ если модуль выработки квантовых ключей (i+1)-го узла сети КРК подключен к j-му выходу оптического коммутатора, то задают коммутацию квантовых каналов в оптическом коммутаторе из модуля выработки пользовательских ключей i-го узла сети КРК со входа оптического коммутатора на j-й выход;

○ если модуль выработки квантовых ключей i-го узла сети КРК подключен к j-му

выходу оптического коммутатора, то задают коммутацию квантовых каналов в оптическом коммутатор из модуля выработки пользовательских ключей (i+1)-го узла сети КРК со входа оптического коммутатора на j-й выход;

• вырабатывают квантовый ключ в модулях выработки квантового ключа i-го и (i+1)-го узлов сети КРК;

• передают полученный квантовый ключ из модуля выработки квантового ключа в модуль выработки пользовательских ключей на i-м и (i+1)-м узле сети КРК;

• помещают полученный квантовый ключ в хранилища квантовых ключей модулей выработки пользовательских ключей i-го и (i+1)-го узлов сети КРК;

• если i<k-1, то

- вычисляют i=i+1;
- переходят к этапу А;

• запрашивают случайное число в модуле выработки пользовательских ключей из модуля выработки квантовых ключей узла сети КРК с идентификатором, соответствующему первому узлу зарезервированного квантового маршрута;

• вырабатывают запрошенное случайное число с помощью генератора случайных чисел модуля выработки квантовых ключей;

• передают выработанное случайное число из модуля выработки квантовых ключей в модуль выработки пользовательских ключей узла сети КРК с идентификатором, соответствующему первому узлу зарезервированного квантового маршрута;

• вырабатывают на первом и последнем узлах сети КРК зарезервированного квантового маршрута квантовый пользовательский ключ с помощью случайного числа в модуле выработки пользовательских ключей первого узла сети КРК и квантовых ключей в хранилищах квантовых ключей узлов сети КРК зарезервированного квантового маршрута, согласно выбранному порядку выработки квантового пользовательского ключа;

• вырабатывают классический пользовательский ключ на первом и последнем узле сети КРК зарезервированного квантового маршрута в модулях выработки пользовательских ключей с использованием предварительных ключей согласно выбранному порядку выработки классического пользовательского ключа;

• вырабатывают в модулях выработки пользовательских ключей первого и последнего узлов сети КРК зарезервированного квантового маршрута пользовательский ключ с использованием квантового пользовательского ключа и классического пользовательского ключа согласно выбранному порядку объединения квантового пользовательского ключа и классического пользовательского ключа;

• передают выработанный пользовательский ключ из модуля выработки пользовательского ключа первого и последнего узлов сети КРК зарезервированного квантового маршрута в модули управления пользовательскими ключами первого и последнего узлов сети КРК зарезервированного квантового маршрута;

• сохраняют в хранилище пользовательских ключей модуля управления пользовательскими ключами узла сети КРК полученный пользовательский ключ;

• передают пользовательский ключ из хранилища пользовательских ключей модуля управления пользовательскими ключами узла сети КРК в шифратор пользователя, запросивший пользовательский ключ.

В предложенном способе может быть предусмотрено, что

• определяют в модулях выработки пользовательских ключей и передают другим модулям выработки пользовательских ключей топологические метрики сети КРК, которыми дополняют топологию сети КРК, причем топологические метрики включают

- количество квантовых ключей в хранилище квантовых ключей;
- скорость выработки квантовых ключей с соседними узлами сети КРК;
- скорость расходования и количество квантовых ключей на зарезервированных квантовых маршрутах;

• учитывают топологические метрики при определении квантового маршрута в модуле выработки пользовательских ключей;

• при резервировании квантового маршрута сообщение о резервировании дополняют информацией о количестве необходимых квантовых ключей для резервирования.

В предложенном способе также может быть предусмотрено, что запрос квантового ключа в модуль выработки квантовых ключей содержит характеристики запрашиваемого квантового ключа: длину, максимальное время готовности квантового ключа, режим выработки ключа.

Кроме этого, в предложенном способе может быть предусмотрено, что запрос пользовательского ключа в модуль управления пользовательскими ключами содержит характеристики запрашиваемого квантового ключа: длину, максимальное время готовности пользовательского ключа, необходимость применения классического пользовательского ключа при вычислении пользовательского ключа.

Предлагаемая система (далее - сеть КРК) в целом предназначена для выработки и распределения ключей между любой парой входящих в ее состав узлов. Вырабатываемые ключи могут применяться как узлами самой системы, так и передаваться во внешние устройства, подключаемые к узлам. Способ выработки и распределения ключей реализуется в первом варианте узла (узла сети КРК). Система позволяет вырабатывать ключи, стойкость которых основана на стойкости как квантовых ключей, получаемых с помощью протоколов КРК с доказанной секретностью, так и классических ключей. Объединение двух ключей, имеющих разную природу, позволяет получить стойкий ключ даже в случае, если проведена успешная атака на один из составных ключей. Таким образом, достигается повышение стойкости пользовательских ключей.

Узлы сети КРК соединяются квантовыми линиями связи. Причем на каждую квантовую линию связи в узле сети КРК выделяется обособленный модуль выработки квантовых ключей. За счет этого достигается высокая скорость выработки квантовых ключей на сегментах сети КРК, т.е. на паре модулей выработки квантовых ключей, соединенных квантовыми линиями связи. Множество модулей выработки квантовых ключей в одном узле сети КРК позволяет строить сети КРК произвольной топологии. При этом может осуществляться параллельная выработка квантовых ключей на всех сегментах сети КРК, в которые входит данный узел сети КРК, повышая итоговую скорость выработки пользовательских ключей.

Отметим, что модули выработки квантовых ключей в общем случае бывают двух видов: одни содержат источник одиночных фотонов, другие - приемник одиночных фотонов. Узел сети КРК может содержать модули выработки квантовых ключей как одного, так и другого вида. Единственное требование, которое накладывается на эти модули, - с одного конца квантовой линии связи должен находиться источник одиночных фотонов, а с другого конца этой же квантовой линии связи должен находиться приемник одиночных фотонов.

Для подключения внешних устройств, которым необходимо передавать пользовательский ключ, например, шифраторов, узел сети КРК оборудуется модулем управления пользовательских ключей.

Данный модуль служит для трех целей.

Первая - унификация идентификационной информации узлов сети КРК, за счет

перевода запросов пользовательского ключа с указанием идентификационной информации шифраторов в запросы пользовательского ключа внутри сети КРК с указанием идентификационной информации узлов сети КРК. Таким образом, идентификационная информация пар шифраторов может иметь различный вид.

Вторая - хранение пользовательских ключей в выделенном ключевом хранилище. Таким образом, уменьшается вероятность случайного или преднамеренного использования выработанного пользовательского ключа после передачи в модули управления пользовательскими ключами. Также за счет этого хранилища возможна отложенная выдача пользовательского ключа внешнему устройству, если оно было не подключено в момент выработки пользовательского ключа.

Третья - невозможность на физическом уровне подключить внешнее устройство к узлу, с которого не предполагается выдача пользовательских ключей.

Отметим, что подключенные шифраторы пользователей (или иные внешние устройства, предназначенные для получения пользовательского ключа от сети КРК) инициируют выполнение способа выработки и распределения пользовательских ключей путем передачи запроса пользовательского ключа в модуль управления пользовательскими ключами. Для корректной обработки запросов пользовательского ключа на узле сети КРК необходимо, чтобы каждый узел сети КРК мог определить узел сети КРК, к которому подключен другой шифратор пользователя, с которым запрошен пользовательский ключ.

Для этих целей каждым модулем управления пользовательскими ключами формируется общая база данных подключенных шифраторов пользователей, которая содержит информацию о том, какие шифраторы пользователей подключены к сети КРК и к какому именно узлу сети КРК. Эта база данных позволяет переводить идентификационную информацию шифраторов в идентификационную информацию узлов сети КРК, к которым подключены эти шифраторы. Общая база данных представляет собой определенную структуру, хранящуюся в памяти модуля во время работы системы.

Модули управления пользовательскими ключами служат для взаимодействия с внешними по отношению к системе шифраторами пользователей. В том случае, если к конкретному узлу сети КРК не планируется в принципе подключать шифраторы пользователей и с этого узла сети КРК не будут выдаваться пользовательские ключи, то возможна упрощенная реализация узла сети КРК, при которой исключается модуль управления пользовательскими ключами. В этом случае также исключается возможность взаимодействия с данным узлом извне системы, что позволяет создать более защищенную реализацию узла сети КРК. Необходимость в такой защищенной реализации может возникнуть при реализации системы, соединяющий, например, удаленные географические объекты, между которыми расстояние существенно больше 100 км (предельное расстояние для известных систем КРК), а между ними находятся малонаселенные труднодоступные территории. Тогда безопасная реализация узла сети КРК позволит упростить организацию места размещения такого узла и уменьшить частоту регламентного очного контроля узла сети КРК.

Способ выработки и распределения пользовательских ключей предполагает децентрализованное управление выработкой пользовательских ключей. Тот узел сети КРК, к которому подключено запросившее ключ устройство, может самостоятельно определить необходимую цепочку узлов сети КРК (квантовый маршрут), которая позволит выработать пользовательский ключ. Для определения квантового маршрута каждый узел сети КРК, выполняющий расчет маршрута, должен обладать полной

информацией о существующих квантовых линиях связи в сети КРК, а также об эффективности их использования

Квантовым маршрутом назовем упорядоченную последовательность узлов сети КРК, в которой каждый последующий узел связан с предыдущим квантовым каналом связи.

Первый узел сети КРК в этой последовательности - это узел сети КРК, в модуле выработки пользовательских ключей которого получен запрос пользовательского ключа. Последний узел сети КРК в квантовом маршруте - узел сети КРК, с которым необходимо выработать пользовательский ключ в соответствии с запросом пользовательского ключа. Последовательность узлов сети КРК может задаваться, например, упорядоченным массивом идентификаторов этих узлов.

В общем случае, существуют различные способы выбора квантового маршрута. Квантовый маршрут для каждой пары узлов сети КРК может быть заранее предопределенным и зафиксированным. Но в таком случае он может оказаться неработоспособным в случае нарушения выработки квантовых ключей (например, падение скорости выработки ключей, нерегулярность выработки ключей) между какой-либо парой узлов сети КРК квантового маршрута и, тем более, в случае невозможности выработки квантовых ключей.

Динамические способы определения квантового маршрута позволяют строить маршрут, оптимальный по некоторому признаку в конкретный момент времени.

Предлагается при определении квантового маршрута минимизировать время, необходимое для выработки квантовых ключей на всех последовательных парах узлов сети КРК для повышения скорость выработки пользовательского ключа.

Для этого предлагается использовать следующие параметры квантового канала связи и узлов сети КРК, характеризующие эффективность выработки пользовательского ключа на некотором маршруте (показатели эффективности квантовой линии связи):

- количество накопленных квантовых ключей в хранилище квантовых ключей в узлах сети КРК на предполагаемом квантовом маршруте,
- скорость выработки квантовых ключей на узле сети КРК с соседними узлами сети КРК,
- скорость расходования квантовых ключей,
- количество квантовых ключей на зарезервированных квантовых маршрутах для выработки квантовых пользовательских ключей,
- размеры квантовых ключей и размер запрошенного пользовательского ключа,
- выбранный способ передачи квантовой составляющей пользовательского ключа и способ объединения квантовой и пользовательской составляющих пользовательского ключа.

Информация о показателях эффективности квантовых линиях связи всей сети КРК передается на каждый узел сети КРК с помощью служебных сообщений. Каждый узел сети КРК раскрывает всем прочим узлам сети КРК в системе информацию о соседних с ним узлах сети КРК и эффективности квантовых линий связи, подключенных к данному узлу. Объединив свою раскрытую информацию с аналогичной информацией от прочих узлов сети КРК, каждый узел сети КРК может сформировать топологию сети КРК, представив ее, например, в виде графа, где вершинами будут узлы сети КРК, а ребрами - квантовые линии связи. Тогда каждому ребру графа можно сопоставить вес, показывающий эффективность квантовой линии связи, рассчитанную на основании показателей эффективности. Таким образом, на каждом узле сети КРК хранится взвешенный граф, по которому узел сети КРК определяет квантовый маршрут. Значения

показателей эффективности могут определяться модулями выработки пользовательских ключей на основе анализа статистики выработки квантовых ключей в процессе работы системы или заранее зафиксированных производителем. В первом случае при изменении значений показателей эффективности необходимо обновить топологию сети (взвешенный граф) на узле сети КРК, на котором обновились значения показателей эффективности, и разослать обновленную топологию на все остальные узлы сети КРК. Во втором случае значения показателей эффективности не изменяются во время работы сети КРК.

На фиг. 1 приведен пример сети КРК, состоящей из 6 узлов сети КРК. Линиями обозначены квантовые каналы связи. Тогда квантовый маршрут от узла 1 до узла 6 может принимать следующие значения:

- 1, 2, 3, 6;
- 1, 2, 3, 4, 5, 6;
- 1,2,3,5,6;
- 1, 4, 5, 6;
- 1, 4, 3, 6;
- 1, 4, 3, 5, 6;
- 1, 4, 5, 3, 6.

После расчета квантового маршрута модуль выработки пользовательских ключей резервирует этот маршрут, чтобы модули выработки пользовательских ключей прочих узлов сети КРК могли учитывать рассчитанный зарезервированный маршрут, на котором будут расходоваться квантовые ключи, при расчете следующих квантовых маршрутов.

Хранение вырабатываемых квантовых ключей, как и управление выработкой квантовых ключей, производится в модулях выработки пользовательских ключей. Таким образом, упрощается управление выработкой квантовых ключей, в том числе при необходимости переключения оптических коммутаторов, так как квантовый маршрут и его резервирование на узлах сети КРК выполняется в модулях выработки пользовательских ключей, что позволяет этим модулям собирать информацию о необходимых квантовых ключах и сформировать последовательность выработки квантовых ключей с соседними узлами сети. Более того, вычисление маршрутов и последующая выработка пользовательских ключей непосредственно в модулях выработки пользовательских ключей позволяет проводить параллельные вычисление этих маршрутов для запросов, полученных на разных узлах в отличие, например, от прототипа, в котором запросы поступают в единый центр управления, который рассчитывает их последовательно.

Децентрализованная система управления выработкой квантовых и пользовательских ключей повышает отказоустойчивость системы в целом, так как отказ одного узла сети КРК ведет только к невозможности реализации таких маршрутов, которые задействуют отказавший узел, не влияя на прочие маршруты. При достаточной избыточности связей отказ одного узла не повлияет на способность системы выполнять свои функции по созданию пользовательских ключей, а повлияет только на скорость выполнения этих функций.

Примером достаточной избыточности связей может служить такая топология связей квантовыми линиями связи, при которой любую пару узлов сети КРК можно соединить двумя независимыми маршрутами, такими, что у них совпадают только начальный и конечный узел, а все промежуточные узлы различны.

Второй вариант системы позволяет оптимизировать некоторые сегменты сети КРК. Для этого применяются оптические коммутаторы, с помощью которых можно

уменьшить количество модулей выработки квантовых ключей в одном узле сети КРК. Несколько модулей выработки квантовых ключей в узле сети КРК заменяются одним модулем выработки квантовых ключей. Этот модуль выработки квантовых ключей подключается дополнительной квантовой линией связи ко входу оптического коммутатор, а квантовые линии связи, которые соединяли данный узел сети КРК с сопряженными узлами, подключаются к выходам оптического коммутатора. То есть фактически оптический коммутатор помещается в разрыв квантовой линии связи.

Управление оптическим коммутатором производится с того узла сети КРК, в котором была произведена замена модулей выработки квантовых ключей один модулем. Для этого оптический коммутатор соединяется служебной линией связи с модулем выработки пользовательских ключей этого узла сети КРК.

На добавление оптических коммутаторов накладывается следующее ограничение. Не должно быть двух узлов сети КРК, подключенных к двум оптическим коммутаторам, встроенных в разрыв одной и той же квантовой линии связи. Данное ограничение необходимо для того, чтобы одной квантовой линией связи не управляли два узла сети КРК, а следовательно, включение конкретной квантовой линии связи определялось строго одним узлом сети КРК и было однозначно.

Во втором варианте системы, как и в первом, возможна упрощенная реализация узла сети КРК, выполненная без модулей управления пользовательскими ключами.

Добавление оптических коммутаторов модифицирует способ выработки и распределения пользовательских ключей с учетом характеристик оптических коммутаторов.

В таком случае выработка квантовых ключей по сегментам производится последовательно по принципу разделения времени с последовательным переключением оптического коммутатора согласно полученной информации о резервировании квантового маршрута. Сначала оптический коммутатор включается в положение, организовывающее непрерывную квантовую линию связи с узлом сети КРК, предшествующим данному в зарезервированном квантовом маршруте, а после успешной выработки квантового ключа на этом сегменте оптический коммутатор включается в положение для организации квантовой линии связи с о следующим узлом в зарезервированном квантовом маршруте для выработки квантового ключа на этом сегменте квантового маршрута. Общая скорость выработки пользовательских ключей снижается, но также снижается стоимость узла сети КРК, его масса и габариты, а также суммарная длина оптоволокна, использованного для квантовых линий связи сети КРК.

Краткое описание чертежей

На фиг. 1 показана схема системы из 6 узлов сети КРК по первому варианту.

На фиг. 2 показана схема системы из 6 узлов сети КРК по второму варианту с добавлением оптического коммутатора.

Обозначения на фигурах

1 - модуль выработки пользовательских ключей

2 - модуль выработки квантовых ключей

2 (а) - модуль выработки квантовых ключей типа источник

2 (б) - модуль выработки квантовых ключей типа приемник

3 - модуль управления пользовательскими ключами

4 - оптический коммутатор

5 - узел сети КРК

5.x, где x от 1 до 6 - узел сети КРК с номером x

6 - шифратор пользователя

7 - квантовая линия связи

8 - локальная линия связи между модулем выработки квантовых ключей и модулем выработки пользовательских ключей

9 - служебная цифровая линия связи между модулем управления пользовательскими ключами узла сети КРК и шифратором пользователя.

Осуществление изобретения

Предлагаемая система, устройство и способ могут быть реализованы, например, с использованием известной однопроходной системы КРК (патент РФ №2706175) и программно-аппаратных комплексов ViPNet Coordinator HW 100 (статья по адресу https://infotecs.ru/upload/iblock/60a/ViPNet_Coordinator_HW100_web_apri_2018.pdf).

В качестве квантовой линии связи 7 выбирается одномодовое оптоволокно типа SMF-28 допустимой длины. В качестве локальных линий связи 8, соединяющих модули выработки квантовых ключей и модули выработки пользовательских ключей, выбирается Ethernet патчкорд.

Модули выработки квантовых ключей реализуются с помощью данной однопроходной системы КРК, причем с одного конца квантовой линии связи устанавливается модуль, содержащий источник одиночных фотонов (далее - модуль типа источник, 2(а)), а с другого конца - модуль, содержащий приемник одиночных фотонов (далее - модуль типа приемник, 2(б)). Модули выработки пользовательских ключей 1 реализуются с помощью программно-аппаратного комплекса ViPNet Coordinator HW100 с модифицированным ПО. Модифицированное ПО может быть составлено специалистом по программированию (программистом). Модуль управления пользовательскими ключами 3 может быть выполнен в виде дополнительного ПО, запускаемого на ViPNet Coordinator HW100.

Приведем пример системы, состоящей из 6 узлов, соединенных квантовыми линиями связи, как показано на фиг. 1. Узел 1 состоит из модуля управления пользовательскими ключами, модуля выработки пользовательских ключей, двух модулей выработки квантовых ключей типа источник. Узел 2 состоит из модуля выработки пользовательских ключей и двух модулей выработки квантовых ключей типа приемник. Узел 3 состоит из модуля управления пользовательскими ключами, модуля выработки пользовательских ключей, трех модулей выработки квантовых ключей типа источник, одного модуля выработки квантовых ключей типа приемник. Узел 4 состоит из модуля выработки пользовательских ключей, двух модулей выработки квантовых ключей типа источник и одного модуля выработки квантовых ключей типа приемник. Узел 5 состоит из одного модуля выработки пользовательских ключей, трех модулей выработки квантовых ключей типа приемник. Узел 6 состоит из модуля управления пользовательскими ключами, модуля выработки пользовательских ключей, модуля выработки квантовых ключей типа источник и модуля выработки квантовых ключей типа приемник.

Для осуществления способа выполняют следующие действия:

Выбирают порядок передачи квантового пользовательского ключа, например, согласно известному способу по патенту РФ №2708511.

Выбирают порядок передачи классического пользовательского ключа, например, путем предварительной загрузки классических пользовательских ключей доверенным курьером без дальнейшей передачи.

Выбирают порядок объединения квантового пользовательского ключа и классического пользовательского ключа, например, путем побитового сложения (с использованием операции исключающее ИЛИ (XOR)) квантового пользовательского ключа и классического пользовательского ключа.

Загружают предварительные ключи K1_2, K1_3, K1_4, K1_5, K1_6 в модуль выработки пользовательских ключей узла 1, ключи K1_2, K2_3, K2_4, K2_5, K2_6 в модуль выработки пользовательских ключей узла 2, ключи K1_3, K2_3, K3_4, K3_5, K3_6 в модуль выработки пользовательских ключей узла 3, ключи K1_4, K2_4, K3_4, K4_5, K4_6 в модуль выработки пользовательских ключей узла 4, ключи K1_5, K2_5, K3_5, K4_5, K5_6 в модуль выработки пользовательских ключей узла 5, ключи K1_6, K2_6, K3_6, K4_6, K5_6 в модуль выработки пользовательских ключей узла 6.

Загружают в модули выработки пользовательских ключей идентификационную информацию. Например, в качестве такой информации может использоваться идентификатор узла системы и его IP адрес. Пусть идентификатора узла принимает значение ID_i для i-го узла, где i - номер узла. В узел 1 загружают ID_1, ID_2, ID_4. В узел 2 загружают ID_1, ID_2, ID_3. В узел 3 загружают ID_2, ID_3, ID_4, ID_5, ID_6. В узел 4 загружают ID_1, ID_3, ID_4, ID_5. В узел 5 загружают ID_3, ID_4, ID_5, ID_6. В узел 6 загружают ID_3, ID_5, ID_6.

Загружают в модуль управления пользовательскими ключами информацию о подключенных шифраторах пользователей системы. Например, к узлу 1 подключают шифратор с идентификатором ID_E_1, а к узлу 6 подключают шифратор с идентификатором ID_E_2. В качестве шифратора пользователя может использоваться, например, программно-аппаратный комплекс ViPNet L2 10G (статья по адресу https://infotecs.ru/about/press-centr/news/infoteks-i-eci-telecom-proveli-ispytaniya-na-sovmestimost-svoikh-produktov.html).

Модуль управления пользовательскими ключами передает модулям управления пользовательскими ключами других узлов информации о подключенных шифраторах пользователей 6. Тогда модуль управления пользовательскими ключами узла 1 отправляет в модуль управления пользовательскими ключами узлов 3 и 6 информацию вида {ID_1, ID_E_1}. Аналогично модуль управления пользовательскими ключами узла 6 отправляет в адрес модулей управления пользовательскими ключами узлов 1 и 3 информацию вида {ID_6, ID_E_2}.

Модули управления пользовательскими ключами принимают переданную информацию. После этого каждый модуль управления пользовательскими ключами объединяет ее в общую базу данных подключенных шифраторов, которая может быть представлена в виде упорядоченной структуры, например, таблицы. Общая база данных подключенных шифраторов пользователей на каждом узле будет иметь вид, представленный ниже в табл. 1.

Таблица 1

ID_1	ID_E_1
ID_2	-
ID_3	ID_E_2

Модули выработки пользовательских ключей каждого узла передают в модули выработки пользовательских ключей всех других узлов информацию о соседних узлах. Для узла 1 соседними являются узлы 2 и 4. Для узла 2 - узлы 1 и 3. Для узла 3 - узлы 2, 4, 5, 6. Для узла 4 - узлы 1, 3,5. Для узла 5 - узлы 3, 4, 6. Для узла 6 - узлы 3, 5. В качестве информации о соседних узлах может использоваться, например, идентификаторы соседних узлов. Тогда Узел 1 рассылает информацию вида {ID_1; ID_2, ID_4}, Узел 2 - {ID_2; ID_1, ID_3}, Узел 3 - {ID_3; ID_2, ID_4, ID_5, ID_6} и т.д.

Модули выработки пользовательских ключей принимают переданную информацию

и формируют на основе нее топологию сети КРК. Такая топология сети КРК может быть представлена, например, в виде табл. 2.

Таблица 2

ID_1	ID_2
ID_1	ID_4
ID_2	ID_1
ID_2	ID_3
ID_3	ID_2
ID_3	ID_4
ID_3	ID_5
ID_3	ID_6
ID_4	ID_1
ID_4	ID_3
ID_4	ID_5
ID_5	ID_3
ID_5	ID_4
ID_5	ID_6
ID_6	ID_3
ID_6	ID_5

Пусть пользовательский ключ запрошен шифратором с идентификатором ID_E_1 для связи с шифратором с идентификатором ID_E_2.

Шифратор с идентификатором ID_E_1 отправляет запрос пользовательского ключа в модуль управления пользовательскими ключами узла 1, указывая в запросе идентификатор целевого шифратора ID_E_2.

Модуль управления пользовательскими ключами узла 1 по общей базе данных подключенных шифраторов пользователей (таблице 1) определяет узел сети, соответствующий шифратору с идентификатором ID_E_2, т.е. узел 6 с идентификатором ID_6.

Модуль управления пользовательскими ключами формирует запрос пользовательского ключа к модулю выработки пользовательских ключей с указанием текущего и целевого узла сети {ID_1, ID_6}. Сформированный запрос передается в модуль выработки пользовательских ключей узла 1.

Модуль выработки пользовательских ключей принимает запрос от модуля управления пользовательскими ключами и начинает определение квантового маршрута. Первым идентификатором в квантовом маршруте становится ID_1, последним - ID_6. Далее по таблице топологии сети КРК (таблице 2) определяются остальные идентификаторы маршрута. Квантовый маршрут получается, например, {ID_1, ID_4, ID_3, ID_6}. Этому квантовому маршруту соответствуют узлы 1, 4, 3, 6.

Модуль выработки пользовательских ключей узла 1 передает сообщение о

резервировании маршрута для выработки пользовательского ключа между узлами 1 и 6 в модули выработки пользовательских ключей узлов 4, 3, 6.

Модуль выработки пользовательских ключей узла 1 передает запрос выработки квантового ключа в модуль выработки квантового ключа, соединенного квантового линией связи с модулем выработки квантового ключа узла 4. Модуль выработки пользовательских ключей узла 4 передает запрос выработки квантового ключа в модуль выработки квантового ключа, соединенного квантового линией связи с модулем выработки квантового ключа узла 1, и в модуль выработки квантового ключа, соединенного квантового линией связи с модулем выработки квантового ключа узла 3. Модуль выработки пользовательских ключей узла 3 передает запрос выработки квантового ключа в модуль выработки квантового ключа, соединенного квантового линией связи с модулем выработки квантового ключа узла 4, и в модуль выработки квантового ключа, соединенного квантового линией связи с модулем выработки квантового ключа узла 6. Модуль выработки пользовательских ключей узла 6 передает запрос выработки квантового ключа в модуль выработки квантового ключа, соединенного квантового линией связи с модулем выработки квантового ключа узла 3.

Модули выработки квантового ключа, получившие запрос выработки квантового ключа, с помощью выбранного протокола КРК формируют квантовые ключи: ключ QK1 в модулях выработки квантовых ключей узлов 1 и 4, соединенных квантовой линией связи, ключ QK2 в модулях выработки квантовых ключей узлов 4 и 3, соединенных квантовой линией связи, ключ QK3 в модулях выработки квантовых ключей узлов 3 и 6.

Выработанные квантовые ключи передаются в модули выработки пользовательских ключей соответствующих узлов и помещаются в хранилище квантовых ключей, т.е. ключ QK1 помещается в хранилище квантовых ключей модулей выработки пользовательских ключей узлов 1 и 4, ключ QK2 в хранилище узлов 4 и 3, ключ QK3 в хранилище узлов 3 и 6.

Запрашивают случайное число в модуле выработки пользовательских ключей от модуля выработки квантовых ключей узла 1.

Вырабатывают запрошенное случайное число с помощью генератора случайных чисел модуля выработки квантовых ключей.

Передают выработанное случайное число от модуля выработки квантовых ключей в модуль выработки пользовательских ключей узла 1.

С помощью ключей QK1, QK2, QK3 передают полученное случайное число в узел 6 с помощью выбранного способа.

Назначают в узлах 1 и 6 данное случайное число квантовым пользовательским ключом KQ.

Назначают, согласно выбранному способу выработки классического пользовательского ключа, предраспределенный ключ K1_6 классическим пользовательским ключом KC.

Вырабатывают в узле 1 и в узле 6 пользовательский ключ K согласно выбранному способу объединения квантового пользовательского ключа и классического пользовательского ключа, т.е. $K=KQ \oplus KC$, где $\oplus$ - операция XOR (исключающее ИЛИ).

Передают выработанный пользовательский ключ K из модулей выработки пользовательских ключей узлов 1 и 6 в модули управления пользовательскими ключами узлов 1 и 6 и сохраняют в хранилище пользовательских ключей узлов 1 и 6 соответственно.

Передают пользовательский ключ K из хранилища пользовательских ключей узла 1 в шифратор с идентификатором ID_E_1 и из хранилища пользовательских ключей узла 6 в шифратор с идентификатором ID_E_2.

Реализовать действия предложенного способа в составе программы или функции может специалист в области программирования (программист).

Для реализации второго варианта системы дополнительно устанавливают оптический коммутатор, например, реализованный на базе оптического переключателя Sercalo sw1x4 (статья по адресу http://www.shs-systems.ru/catalog/ sercalo/SW/).

Приведем пример системы, состоящей из 6 узлов и соединенной квантовыми линиями связи, как показано на фиг. 2. Состав узлов 1, 2, 3, 4, 6 соответствует составу узлов системы по первому варианту. Узел 5 в составе содержит только один модуль выработки квантовых ключей типа приемник, соединенный квантовой линий связи со входом оптического коммутатора. Выходы оптического коммутатора соединены квантовыми линиями связи с модулями выработки квантовых ключей типа источник узлов 3, 4, 6.

Осуществление способа по второму варианту совпадает с осуществлением способа по первому варианту до шага определения квантового маршрута.

Пусть был определен квантовый маршрут {ID_1, ID_4, ID_5, ID_6}. Этому квантовому маршруту соответствуют узлы 1, 4, 5, 6.

Модуль выработки пользовательских ключей узла 1 передает сообщение о резервировании маршрута для выработки пользовательского ключа между узлами 1 и 6 в модули выработки пользовательских ключей узлов 4, 5, 6.

Модуль выработки пользовательских ключей узла 1 передает запрос выработки квантового ключа в модуль выработки квантового ключа, соединенного квантового линией связи с модулем выработки квантового ключа узла 4. Модуль выработки пользовательских ключей узла 4 передает запрос выработки квантового ключа в модуль выработки квантового ключа, соединенного квантового линией связи с модулем выработки квантового ключа узла 1, и в модуль выработки квантового ключа, соединенного квантового линией связи с модулем выработки квантового ключа узла 5. Модуль выработки пользовательских ключей узла 5 переключает коммутацию оптического коммутатора со входа на выход, соответствующий квантовой линией связи к узлу 4, затем передает запрос выработки квантового ключа в модуль выработки квантового ключа, соединенного квантового линией связи с модулем выработки квантового ключа узла 4. Модули выработки квантового ключа, получившие запрос выработки квантового ключа, с помощью выбранного протокола КРК формируют квантовые ключи: ключ QK1 в модулях выработки квантовых ключей узлов 1 и 4, соединенных квантовой линией связи, ключ QK2 в модулях выработки квантовых ключей узлов 4 и 5. Модуль выработки пользовательских ключей переключает коммутацию оптического коммутатора со входа на выход, соответствующий квантовой линией связи к узлу 6, затем передает запрос выработки квантового ключа в модуль выработки квантового ключа, соединенного квантового линией связи с модулем выработки квантового ключа узла 6. Модуль выработки пользовательских ключей узла 6 передает запрос выработки квантового ключа в модуль выработки квантового ключа, соединенного квантового линией связи с модулем выработки квантового ключа узла 5.

Модули выработки квантового ключа, получившие запрос выработки квантового ключа, с помощью выбранного протокола КРК формируют квантовые ключи: ключ QK3 в модулях выработки квантовых ключей узлов 5 и 6.

Выработанные квантовые ключи передаются в модули выработки пользовательских

ключей соответствующих узлов и помещаются в хранилище квантовых ключей, т.е. ключ QK1 помещается в хранилище квантовых ключей модулей выработки пользовательских ключей узлов 1 и 4, ключ QK2 в хранилище узлов 4 и 5, ключ QK3 в хранилище узлов 5 и 6.

Затем формируют пользовательский ключ и завершают выполнение способа аналогично способу по первому варианту.

(57) Формула изобретения

1. Система выработки и распределения ключей, включающая

множество узлов сети выработки и квантового распределения ключей (узлы сети КРК), причем

узлы сети КРК соединены квантовыми линиями связи так, что граф, отображающий связи квантовыми линиями, является связным;

узлы сети КРК соединены классической линией связи с цифровой сетью передачи данных;

причем к каждому узлу сети КРК присоединено, по крайней мере, две квантовые линии связи;

при этом каждый узел сети КРК включает

модуль выработки пользовательских ключей,

модуль управления пользовательскими ключами,

по крайней мере, два модуля выработки квантовых ключей;

причем

каждый модуль выработки квантовых ключей связан с модулем выработки пользовательских ключей локальной цифровой линией передачи данных;

модуль выработки пользовательских ключей соединен с модулем управления пользовательскими ключами локальной цифровой линией передачи данных;

при этом каждый модуль выработки квантовых ключей выполнен с возможностью вырабатывать квантовые ключи совместно с другим модулем выработки квантовых ключей, соединенным с данным квантовой линией связи; генерировать случайные числа;

получать запросы на выработку квантового ключа от модуля выработки пользовательских ключей;

передавать вырабатываемые квантовые ключи в модули выработки пользовательских ключей;

передавать/получать служебные данные протокола КРК от модуля выработки пользовательских ключей; при этом модуль выработки пользовательских ключей выполнен с возможностью создавать запросы на выработку квантового ключа в модули выработки квантовых ключей;

получать квантовые ключи от модулей выработки квантовых ключей согласно переданным запросам;

хранить квантовые ключи в хранилище квантовых ключей;

зашифровывать данные;

расшифровывать данные;

аутентифицировать данные;

проверять аутентификацию данных;

определять топологию сети КРК;

определять квантовый маршрут для выработки пользовательских ключей; вырабатывать пользовательские ключи совместно с модулями выработки пользовательских ключей других узлов сети КРК на квантовом маршруте; получать

запросы на выработку пользовательских ключей от модулей управления пользовательскими ключами;

передавать пользовательские ключи в модули управления пользовательскими ключами;

при этом модуль управления пользовательскими ключами выполнен с возможностью подключать шифраторы пользователей с помощью цифровой сети передачи данных;

хранить пользовательские ключи в хранилище пользовательских ключей;

определять совместно с модулями управления пользовательскими ключами других узлов сети КРК соответствие узла сети КРК и подключенных к ним шифраторов пользователей;

формировать общую базу данных подключенных шифраторов пользователей, содержащую соответствие узлов сети КРК и подключенных к ним шифраторов пользователей;

формировать запросы на выработку пользовательского ключа в модули выработки пользовательских ключей;

получать пользовательские ключи от модулей выработки пользовательских ключей согласно переданным запросам.

2. Способ выработки и распределения пользовательских ключей в системе заключающийся в том, что

выбирают порядок выработки квантового пользовательского ключа;

выбирают порядок выработки классического пользовательского ключа;

выбирают порядок объединения квантового пользовательского ключа и классического пользовательского ключа;

загружают предварительные ключи в модули выработки пользовательских ключей узлов сети КРК, причем в каждый модуль выработки пользовательских ключей загружается N-1 ключ, где N - число узлов сети КРК;

загружают в модуль выработки пользовательских ключей каждого узла сети КРК идентификационную информацию для связи с другими узлами сети КРК, которые соединены квантовой линией связи с данным узлом сети КРК;

загружают в каждый модуль управления пользовательскими ключами идентификационную информацию подключенных к ним шифраторов пользователей;

передают из модуля управления пользовательскими ключами каждого узла сети КРК в модули управления пользовательскими ключами всех остальных узлов сети КРК данные о подключенных шифраторах пользователей;

получают в модуле управления пользовательскими ключами каждого узла сети КРК переданную информацию о подключенных шифраторах пользователей и записывают ее в общую базу данных подключенных шифраторов пользователей;

передают из модуля выработки пользовательских ключей каждого узла сети КРК в модули выработки пользовательских ключей остальных узлов сети КРК идентификационную информацию всех соседних с ним узлов сети КРК, получают в модуле выработки пользовательских ключей каждого узла сети КРК переданную ему идентификационную информацию соседних узлов и на ее основе формируют топологию сети КРК;

получают запрос пользовательского ключа от шифратора пользователя, подключенного к модулю управления пользовательскими ключами узла сети КРК, причем запрос включает идентификационную информацию шифратора пользователя, для связи с которым необходим пользовательский ключ;

определяют из общей базы данных подключенных шифраторов пользователей узел

сети КРК, к которому подключен шифратор пользователя, для связи с которым необходим пользовательский ключ;

формируют в модуле управления пользовательскими ключами узла сети КРК запрос пользовательского ключа с указанием идентификационной информации текущего узла сети КРК и узла сети КРК, определенного по общей базе данных подключенных шифраторов пользователей;

передают сформированный запрос пользовательского ключа из модуля управления пользовательскими ключами в модуль выработки пользовательских ключей узла сети КРК;

принимают в модуле выработки пользовательских ключей запрос пользовательского ключа от модуля управления пользовательскими ключами; определяют последовательность узлов сети КРК (квантовый маршрут) и количество k узлов в квантовом маршруте от узла сети КРК, получившего запрос пользовательского ключа, до узла сети КРК, указанного в запросе пользовательского ключа, с помощью топологии сети КРК;

резервируют квантовый маршрут, передавая из модуля выработки пользовательских ключей узла сети КРК, получившего запрос пользовательского ключа, в модули выработки пользовательских ключей узлов сети КРК, с идентификаторами, соответствующими остальным идентификаторам узлов сети КРК в квантовом маршруте, сообщения о резервировании квантового маршрута; вычисляют i=1;

(A) посылают запрос выработки квантового ключа из модуля выработки пользовательских ключей в модуль выработки квантовых ключей i-го узла зарезервированного квантового маршрута и из модуля выработки пользовательских ключей в модуль выработки квантовых ключей (i+1)-го узла зарезервированного квантового маршрута, причем если i-й узел сети КРК имеет несколько модулей выработки квантового ключа, то посылают запрос в модуль выработки квантовых ключей, соединенный квантовой линией связи с (i+1)-м узлом сети КРК; если (i+1)-й узел сети КРК имеет несколько модулей выработки квантового ключа, то посылают запрос в модуль выработки квантовых ключей, соединенный квантовой линией связи с i-м узлом сети КРК;

вырабатывают квантовый ключ в модулях выработки квантового ключа i-го и (i+1)-го узлов сети КРК;

передают полученный квантовый ключ из модуля выработки квантового ключа в модуль выработки пользовательских ключей на i-м и (i+1)-м узле сети КРК;

помещают полученный квантовый ключ в хранилища квантовых ключей модулей выработки пользовательских ключей i-го и (i+1)-го узлов сети КРК;

если i<k-1, то

вычисляют i=i+1,

переходят к этапу A; запрашивают случайное число в модуле выработки пользовательских ключей от модуля выработки квантовых ключей узла сети КРК с идентификатором, соответствующим первому узлу сети КРК зарезервированного квантового маршрута;

вырабатывают запрошенное случайное число с помощью генератора случайных чисел модуля выработки квантовых ключей;

передают выработанное случайное число из модуля выработки квантовых ключей в модуль выработки пользовательских ключей узла сети КРК с идентификатором, соответствующим первому узлу зарезервированного квантового маршрута;

вырабатывают на первом и последнем узле сети КРК зарезервированного квантового

маршрута квантовый пользовательский ключ с помощью случайного числа в модуле выработки пользовательских ключей первого узла сети КРК и квантовых ключей в хранилищах квантовых ключей узлов сети КРК, входящих в зарезервированный квантовый маршрут, согласно выбранному порядку выработки квантового пользовательского ключа;

вырабатывают классический пользовательский ключ в первом и последнем узле сети КРК зарезервированного квантового маршрута в модулях выработки пользовательских ключей с использованием предварительных ключей согласно выбранному порядку выработки классического пользовательского ключа;

вырабатывают в модулях выработки пользовательских ключей первого и последнего узлов сети КРК зарезервированного квантового маршрута пользовательский ключ с использованием квантового пользовательского ключа и классического пользовательского ключа согласно выбранному порядку объединения квантового пользовательского ключа и классического пользовательского ключа;

передают выработанный пользовательский ключ из модуля выработки пользовательского ключа первого и последнего узлов сети КРК зарезервированного квантового маршрута в модули управления пользовательскими ключами первого и последнего узлов сети КРК зарезервированного квантового маршрута;

сохраняют в хранилище пользовательских ключей модуля управления пользовательскими ключами узла сети КРК полученный пользовательский ключ;

передают пользовательский ключ из хранилища пользовательских ключей модуля управления пользовательскими ключами узла сети КРК в шифратор пользователя, запросивший пользовательский ключ.

3. Способ выработки и распределения пользовательских ключей по п. 2, в котором определяют в модулях выработки пользовательских ключей и передают другим модулям выработки пользовательских ключей топологические метрики сети КРК, которыми дополняют топологию сети КРК, причем топологические метрики включают

количество квантовых ключей в хранилище квантовых ключей; скорость выработки квантовых ключей с соседними узлами сети КРК; скорость расходования и количество квантовых ключей на зарезервированных квантовых маршрутах;

при определении квантового маршрута модули выработки пользовательских ключей учитывают топологические метрики, которыми дополнена топология сети КРК;

при резервировании квантового маршрута сообщение о резервировании дополняется информацией о количестве необходимых квантовых ключей для резервирования.

4. Способ выработки и распределения пользовательских ключей по п. 2, в котором запрос квантового ключа к модулю выработки квантовых ключей содержит характеристики запрашиваемого квантового ключа: длину, максимальное время готовности квантового ключа, режим выработки ключа.

5. Способ выработки и распределения пользовательских ключей по п. 2, в котором запрос пользовательского ключа к модулю управления пользовательскими ключами содержит характеристики запрашиваемого квантового ключа: длину, максимальное время готовности пользовательского ключа, необходимость применения классического пользовательского ключа при вычислении пользовательского ключа.

6. Система выработки и распределения ключей, включающая

множество узлов сети выработки и квантового распределения ключей (узлы сети КРК), причем

узлы сети КРК соединены квантовыми линиями связи так, что граф, отображающий связи квантовыми линиями, является связным;

узлы сети КРК соединены классической цифровой сетью передачи данных;

причем к каждому узлу сети КРК присоединено, по крайней мере, две квантовые линии связи;

при этом узел сети КРК включает

модуль выработки пользовательских ключей,

модуль управления пользовательскими ключами,

по крайней мере, два модуля выработки квантовых ключей;

причем соединение с квантовыми линиями связи узлов сети КРК может быть выполнено как напрямую, так и через оптический коммутатор; причем

количество оптических коммутаторов не превышает количество узлов сети КРК;

каждый оптический коммутатор имеет один оптический вход и m оптических выходов, позволяющих подключать до m квантовых линий связи к одному узлу сети КРК;

каждый оптический коммутатор соединен локальной цифровой линией передачи данных с модулем выработки пользовательских ключей, подключенным квантовой линией связи к оптическому входу оптического коммутатора; при этом каждый модуль управления пользовательскими ключами соединен с модулем выработки пользовательских ключей локальной цифровой линией передачи данных и выполнен с возможностью получать и передавать данные в шифраторы пользователей через цифровую сеть передачи данных;

хранить пользовательские ключи в хранилище пользовательских ключей; определять совместно с модулями управления пользовательскими ключами других узлов сети КРК соответствие узла сети КРК и подключенных к ним шифраторов пользователей;

формировать общую базу данных подключенных шифраторов пользователей, содержащую соответствие узлов сети КРК и подключенных к ним шифраторов пользователей;

создавать запросы на выработку пользовательского ключа в модули выработки пользовательских ключей;

получать пользовательские ключи от модулей выработки пользовательских ключей согласно переданным запросам;

при этом каждый модуль выработки квантовых ключей связан с модулем выработки пользовательских ключей локальной цифровой линией передачи данных и выполнен с возможностью вырабатывать квантовые ключи совместно с другим модулем выработки квантовых ключей, соединенным квантовой линией связи;

генерировать случайные числа;

получать запросы на выработку квантового ключа от модуля выработки пользовательских ключей;

передавать вырабатываемые квантовые ключи в модули выработки пользовательских ключей;

передавать и получать служебные данные протокола КРК из модуля выработки пользовательских ключей; при этом модуль выработки пользовательских ключей выполнен с возможностью создавать запросы на выработку квантового ключа в модули выработки квантовых ключей;

получать квантовые ключи от модулей выработки квантовых ключей согласно переданным запросам;

хранить квантовые ключи в хранилище квантовых ключей;

зашифровывать данные;

расшифровывать данные;

осуществлять аутентификацию данных;

проверять аутентификацию данных;

определять топологию сети КРК;

определять квантовый маршрут для выработки пользовательских ключей; управлять коммутацией каналов внутри оптического коммутатора; вырабатывать пользовательские ключи совместно с модулями выработки пользовательских ключей других узлов сети КРК на квантовом маршруте, получать запросы на выработку пользовательских ключей от модулей управления пользовательскими ключами;

передавать пользовательские ключи в модули управления пользовательскими ключами.

7. Способ выработки и распределения пользовательских ключей в системе, заключающийся в том, что

выбирают порядок выработки квантового пользовательского ключа;

выбирают порядок выработки классического пользовательского ключа;

выбирают порядок объединения квантового пользовательского ключа и классического пользовательского ключа;

загружают предварительные ключи в модули выработки пользовательских ключей узлов сети КРК, причем в каждый модуль выработки пользовательских ключей загружается N-1 ключ, где N - число узлов сети КРК;

загружают в модуль выработки пользовательских ключей каждого узла сети КРК идентификационную информацию для связи с другими узлами сети КРК, которые соединены квантовой линией связи с данным узлом сети КРК;

загружают в каждый модуль управления пользовательскими ключами идентификационную информацию подключенных к ним шифраторов пользователей;

передают из модуля управления пользовательскими ключами каждого узла сети КРК в модули управления пользовательскими ключами всех остальных узлов сети КРК данные о подключенных шифраторах пользователей;

получают в модуле управления пользовательскими ключами каждого узла сети КРК переданную информацию о подключенных шифраторах пользователей и собирают ее в общую базу данных подключенных шифраторов пользователей;

передают из модуля выработки пользовательских ключей каждого узла сети КРК в модули выработки пользовательских ключей всех остальных узлов сети КРК идентификационную информацию всех соседних с ним узлов сети КРК;

получают в модуле выработки пользовательских ключей каждого узла сети КРК переданную ему идентификационную информацию соседних узлов и на ее основе формируют топологию сети КРК;

получают запрос пользовательского ключа от шифратора пользователя, подключенного к модулю управления пользовательскими ключами узла сети КРК, причем запрос включает идентификационную информацию шифратора пользователя, для связи с которым необходим пользовательский ключ;

определяют по общей базе данных подключенных шифраторов пользователей узел сети КРК, к которому подключен шифратор пользователя, для связи с которым необходим пользовательский ключ;

формируют в модуле управления пользовательскими ключами узла сети КРК запрос пользовательского ключа с указанием идентификационной информации узла сети КРК, получившего запрос пользовательского ключа, и узла сети КРК, определенного по общей базе данных подключенных шифраторов пользователей;

передают сформированный запрос пользовательского ключа из модуля управления пользовательскими ключами в модуль выработки пользовательских ключей узла сети

КРК;

принимают в модуле выработки пользовательских ключей запрос пользовательского ключа от модуля управления пользовательскими ключами; определяют последовательность узлов сети КРК (квантовый маршрут) и количество k узлов в квантовом маршруте от узла сети КРК, получившего запрос пользовательского ключа, до узла сети КРК, указанного в запросе пользовательского ключа, с помощью топологии сети КРК;

резервируют квантовый маршрут, передавая из модуля выработки пользовательских ключей узла сети КРК, получившего запрос пользовательского ключа, в модули выработки пользовательских ключей узлов сети КРК, с идентификаторами, соответствующими остальным идентификаторам узлов сети КРК в зарезервированном квантовом маршруте сообщения о резервировании квантового маршрута; вычисляют i=1,

(А) посылают запрос выработки квантового ключа из модуля выработки пользовательских ключей в модуль выработки квантовых ключей i-го узла зарезервированного квантового маршрута и из модуля выработки пользовательских ключей в модуль выработки квантовых ключей (i+1)-го узла зарезервированного квантового маршрута, причем

если i-й узел сети КРК имеет несколько модулей выработки квантового ключа, то посылают запрос в модуль выработки квантовых ключей, соединенный квантовой линией связи с (i+1)-м узлом сети КРК; если (i+1)-й узел сети КРК имеет несколько модулей выработки квантового ключа, то посылают запрос в модуль выработки квантовых ключей, соединенный квантовой линией связи с i-м узлом сети КРК;

если модули выработки квантовых ключей i-го и (i+1)-го узла сети КРК связаны квантовым каналом связи через оптический коммутатор, то

если модуль выработки квантовых ключей (i+1)-го узла сети КРК подключен к j-му выходу оптического коммутатора, то задают коммутацию квантовых каналов в оптическом коммутаторе из модуля выработки пользовательских ключей i-го узла сети КРК со входа оптического коммутатора на j-й выход;

если модуль выработки квантовых ключей i-го узла сети КРК подключен к j-му выходу оптического коммутатора, то задают коммутацию квантовых каналов в оптическом коммутаторе из модуля выработки пользовательских ключей (i+1)-го узла сети КРК со входа оптического коммутатора на j-й выход;

вырабатывают квантовый ключ в модулях выработки квантового ключа i-го и (i+1)-го узлов сети КРК;

передают полученный квантовый ключ из модуля выработки квантового ключа в модуль выработки пользовательских ключей на i-м и (i+1)-м узле сети КРК;

помещают полученный квантовый ключ в хранилища квантовых ключей модулей выработки пользовательских ключей i-го и (i+1)-го узлов сети КРК;

если i<k-1, то

вычисляют i=i+1;

переходят к этапу А; запрашивают случайное число в модуле выработки пользовательских ключей из модуля выработки квантовых ключей узла сети КРК с идентификатором соответствующему первому узлу зарезервированного квантового маршрута;

вырабатывают запрошенное случайное число с помощью генератора случайных чисел модуля выработки квантовых ключей;

передают выработанное случайное число из модуля выработки квантовых ключей

в модуль выработки пользовательских ключей узла сети КРК с идентификатором соответствующему первому узлу зарезервированного квантового маршрута;

вырабатывают на первом и последнем узлах сети КРК зарезервированного квантового маршрута квантовый пользовательский ключ с помощью случайного числа в модуле выработки пользовательских ключей первого узла сети КРК и квантовых ключей в хранилищах квантовых ключей узлов сети КРК зарезервированного квантового маршрута, согласно выбранному порядку выработки квантового пользовательского ключа;

вырабатывают классический пользовательский ключ на первом и последнем узле сети КРК зарезервированного квантового маршрута в модулях выработки пользовательских ключей с использованием предварительных ключей согласно выбранному порядку выработки классического пользовательского ключа;

вырабатывают в модулях выработки пользовательских ключей первого и последнего узлов сети КРК зарезервированного квантового маршрута пользовательский ключ с использованием квантового пользовательского ключа и классического пользовательского ключа согласно выбранному порядку объединения квантового пользовательского ключа и классического пользовательского ключа;

передают выработанный пользовательский ключ из модуля выработки пользовательского ключа первого и последнего узлов сети КРК зарезервированного квантового маршрута в модули управления пользовательскими ключами первого и последнего узлов сети КРК зарезервированного квантового маршрута;

сохраняют в хранилище пользовательских ключей модуля управления пользовательскими ключами узла сети КРК полученный пользовательский ключ;

передают пользовательский ключ из хранилища пользовательских ключей модуля управления пользовательскими ключами узла сети КРК в шифратор пользователя, запросивший пользовательский ключ.

8. Способ выработки и распределения пользовательских ключей по п. 7, в котором определяют в модулях выработки пользовательских ключей и передают другим модулям выработки пользовательских ключей топологические метрики сети КРК, которыми дополняют топологию сети КРК, причем топологические метрики включают

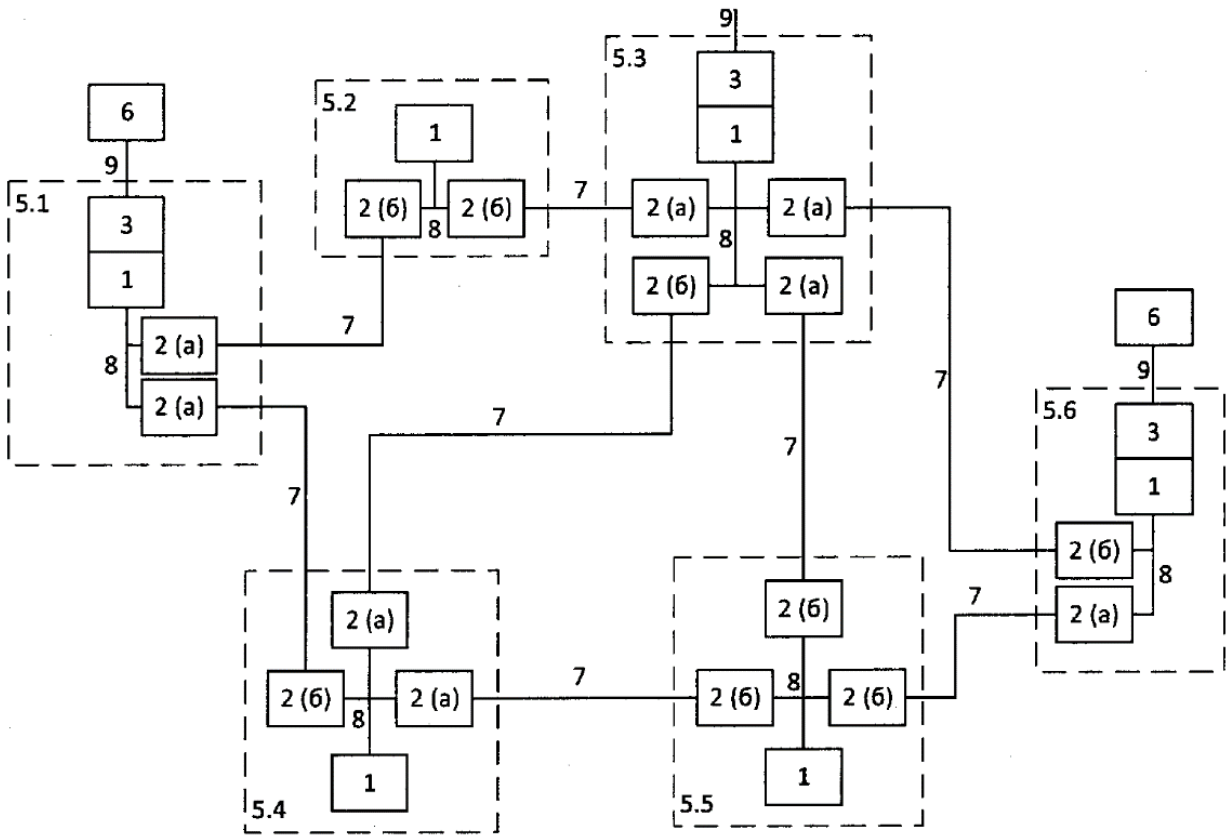
количество квантовых ключей в хранилище квантовых ключей; скорость выработки квантовых ключей с соседними узлами сети КРК; скорость расходования и количество квантовых ключей на зарезервированных квантовых маршрутах; учитывают топологические метрики при определении квантового маршрута в модуле выработки пользовательских ключей;

при резервировании квантового маршрута сообщение о резервировании дополняют информацией о количестве необходимых квантовых ключей для резервирования.

9. Способ выработки и распределения пользовательских ключей по п. 7, в котором запрос квантового ключа в модуль выработки квантовых ключей содержит характеристики запрашиваемого квантового ключа: длину, максимальное время готовности квантового ключа, режим выработки ключа.

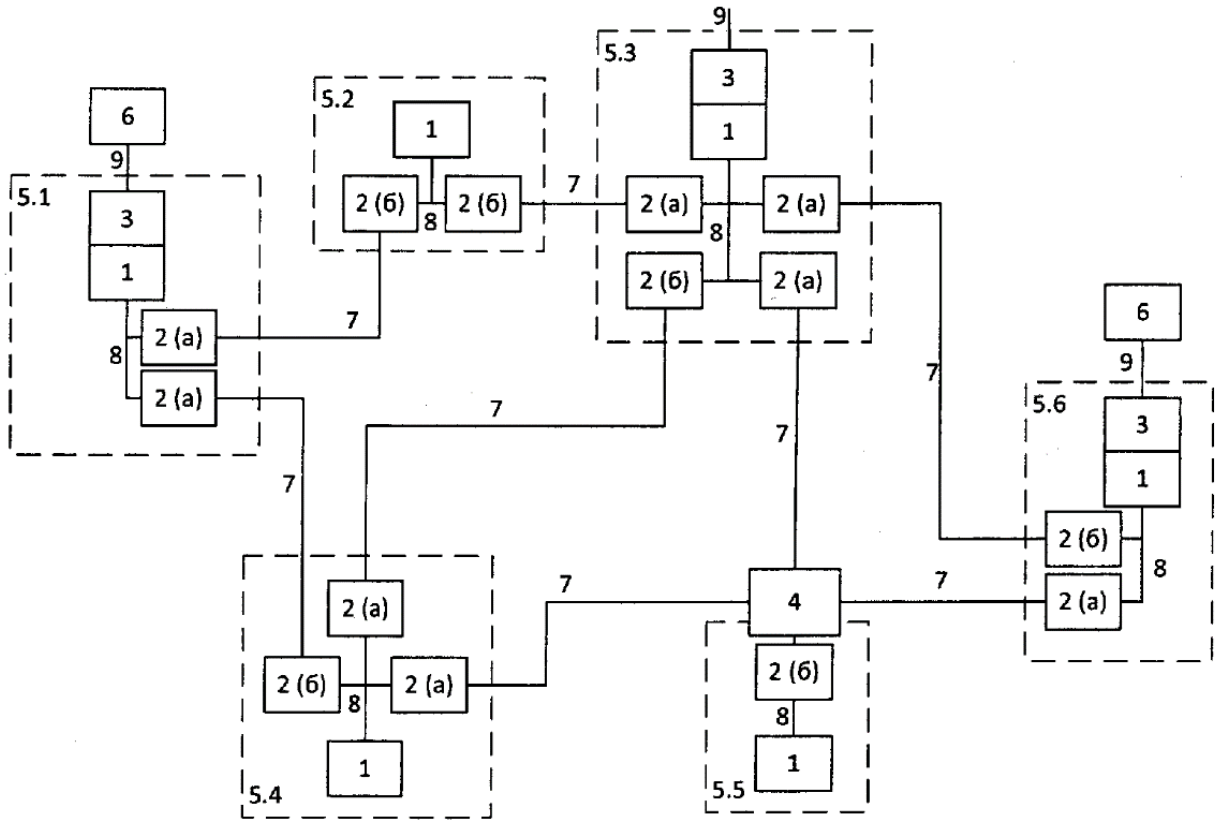
10. Способ выработки и распределения пользовательских ключей по п. 7, в котором запрос пользовательского ключа в модуль управления пользовательскими ключами содержит характеристики запрашиваемого квантового ключа: длину, максимальное время готовности пользовательского ключа, необходимость применения классического пользовательского ключа при вычислении пользовательского ключа.

1


9
5.3
3
1
5.2
1
2 (б)
2 (б)
7
2 (а)
2 (а)
8
2 (б)
2 (а)
6
9
5.1
3
1
2 (а)
2 (а)
8
7
7
7
7
6
9
5.6
3
1
2 (б)
8
2 (а)
7
2 (а)
2 (б)
2 (а)
8
7
2 (б)
2 (б)
8
2 (б)
1
1
5.4
5.5

Фиг. 1

2


5.1
6
9
3
1
2 (а)
2 (а)
8
7
5.2
1
2 (б)
2 (б)
8
7
5.3
9
3
1
2 (а)
2 (а)
8
2 (б)
2 (а)
7
7
7
5.4
2 (а)
2 (б)
2 (а)
8
1
7
4
7
5.5
2 (б)
8
1
5.6
6
9
3
1
2 (б)
2 (а)
8

Фиг. 2