ОТЗЫВ

Официального оппонента, д.ф.-м.н. Молоткова Сергея Николаевича, на диссертацию Жиляева Андрея Евгеньевича «Методика построения сетей квантового распределения ключей смешанной топологии», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Актуальность работы

Квантовые технологии стремительно развиваются и в настоящее время переходят из теоретической концепции в лабораторные и промышленные образцы систем квантовых коммуникаций и квантовых вычислений. Создание эффективного квантового компьютера позволит проводить успешные атаки на существующие алгоритмы, основанные на сложности задач дискретного логарифмирования и разложения больших чисел на простые множители.

В условиях изменения возможностей потенциального злоумышленника актуальной становится задача пересмотра стойкости существующих используемых механизмов и поиск новых способов защиты информации. Для функционирования средств и систем защиты информации необходимо регулярно снабжать их общими секретами для защищенного взаимодействия. Квантовые коммуникации и квантовое распределение ключей (КРК) в частности позволяет достичь регулярного формирования и доставки в пользовательские устройства общих секретов, чья стойкость обусловлена фундаментальными физическими законами и построена на новых принципах.

Для создания и широкого использования систем КРК необходимо решить принципиальную проблему данной технологии, а именно преодоление максимально допустимой длины квантового канала при формировании квантовых ключей для пользовательских устройств. До создания квантовой памяти и, соответственно, квантовых повторителей, единственным универсальным решением этой проблемы является создание так называемых сетей КРК на основе доверенных промежуточных узлов. Определение порядка функционирования таких сетей, их рекомендованной архитектуры и способов использования истинной квантовых ключей при формировании секретов для произвольно удаленных друг от друга пользовательских устройств несомненно является актуальной задачей для создания протяженных сетей КРК различной топологии.

По этой причине, разработка методов создания защищенных коммуникационных сетей, использующих квантовое распределение ключей

является *актуальной* и злободневной научной задачей. Исследованию данной проблемы и посвящена диссертационная работа Андрея Евгеньевича Жиляева.

Структура диссертации

Диссертационная работа Жиляева А.Е. состоит из Введения, четырех глав, Заключения и трех приложений.

Во введении автор обосновывает актуальность темы диссертации, обозначает цель и задачи исследования, приводит научную новизну, практическую и теоретическую значимость полученных в работе результатов, положения, выносимые на защиту.

В первой главе описывается обобщенная структура системы КРК, необходимая для реализации типового протокола КРК на дискретных переменных. Выделены основные этапы протокола КРК.

Сделан подробный анализ существующих подходов увеличения длины линий связи с КРК. Проведенный анализ показал, что наиболее проработанным и реализуемым на сегодняшнем технологическом уровне является подход использующий распределение общего секрета через доверенные узлы.

Комплексный анализ систем квантовой криптографии с учетом атак на квантовый канал и классический каналы связи, атак активного и пассивного зондирования аппаратуры, атак с учетом побочных каналов утечки информации активно начат только в последние годы. Такой всеобъемлющий анализ криптографической стойкости систем КРК и сетей на их основе представляет сложную научную задачу, которая в полной мере до сих пор не решена.

Исторически сложилось, что слова, о необходимости вспомогательного классического аутентичного канала связи в системах КРК, произносились, начиная с первых работ по квантовой криптографии, детальное исследование данного вопроса откладывалось “на потом”, и основное внимание уделялось исследованию различных атак на квантовый канал связи.

Автором уделено особое внимание анализу недостаточной проработанности задачи обеспечения аутентичности служебного канала в различных существующих системах КРК.

В представленном исследовании проанализированы различные методы преодоления фундаментального ограничения систем КРК (предельной длины квантового канала). Обоснованно сделан вывод о необходимости построения сетей КРК на основе доверенных промежуточных узлов. Жиляевым А.Е. подробно изучены наиболее проработанные концепции протяженных сетей КРК, описанные в зарубежных стандартизующих документах, и выявлены их недостатки. По

результатам анализа систем и сетей КРК сформированы основные проблемы и задачи проводимого исследования.

Во второй главе решаются выявленные проблемы для систем КРК топологии точка-точка. Достаточно подробно описаны класс и семейства функций универсального хэширования, а также способы их использования для решения задачи построения аутентифицированного канала системы КРК. Рекомендована функция универсального хэширования, обладающая минимальным расходом ключа аутентификации при фиксированном параметре стойкости. Дополнительно оценена возможность применения рекомендованной функции хэширования в имеющейся системе КРК ViPNet Quandor.

Также в данной главе представлен способ функционирования системы КРК совместно с подключенной парой средств защиты информации (СЗИ), учитывающий неоднородность квантовой гаммы, генерируемой в результате выполнения протокола КРК.

В третьей главе автором разработаны способы распределения общего секрета в магистральных сетях КРК и сетях топологии “звезда”. Для этого подробно проанализирован основной известный способ, называемый в исследовании базовым. Каждый из предлагаемых способов устраняет один из сформулированных недостатков базового. Важным является разделение истинно квантовых ключей, которые возможны только в результате реализации протокола КРК при наличии непрерывного квантового канала, и нового объекта, который возникает в протяженных сетях КРК с использованием истинной квантовых ключей. Такой новый объект в диссертационном исследовании имеет мнемоническое наименование “квантовозащищенный ключ”, КЗК, что отражает его природу как объекта, переданного с защитой на квантовых ключах.

Для разработанных способов предложены критерии классификации, учитывающие как свойства безопасности, достигаемые применением конкретного способа, так и практические, эксплуатационные характеристики способов. В результате синтезируется методика распределения общих секретов в магистральных сетях КРК, позволяющая путем использования ключевых подсистем разной природы получать КЗК, стойкие даже в случае компрометации одной из подсистем.

Четвертая глава посвящена построению сетей КРК смешанной топологии. По результатам анализа европейских аналогов предлагается новая многоуровневая архитектура сети КРК и структура узла такой сети. Для каждого уровня сети подробно обоснованы требования к функциям каждого уровня. Для сети КРК,

реализуемой с предложенными узлами, разработана методика построения сети КРК смешанной топологии и основные этапы функционирования сети. Разработанная методика опирается на ранее синтезированную методику формирования КЗК в магистральной сети КРК.

В заключении приведены основные выводы и результаты диссертационного исследования.

В Приложениях приведены патенты автора и краткие презентации докладов автора на двух престижных международных конференциях, что, не является обязательным для диссертации, и конечно, увеличивает почти вдвое объем текста, но дает удобство читателю и избавляет его от поиска материалов в Интернете.

Новизна полученных результатов.

Выделю, наиболее интересные, с моей точки зрения, новые научные результатами, полученные в диссертации:

1. 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;
2. 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. методика построения сети КРК смешанной топологии, включающая требования к структуре сети КРК, способу ее функционирования, методику распределения квантовозащищенных ключей, 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.

Практическая и теоретическая ценность и внедрение результатов

Результаты данной работы представляют развитие теории защиты информации в части применения технологии КРК для регулярной доставки общих

секретов, предлагая решение, позволяющее распределять общие секреты на расстояния, превышающие предельные длины квантовых каналов.

Введенное Жиляевым А.Е 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 проектирования развертывания протяженных квантовых сетей. Разработанная методика распределения общего секрета в магистральной сети КРК существенно ускорила процесс разработки стандартов в области квантовых коммуникаций.

Достоверность и обоснованность основных результатов и выводов

Достоверность и обоснованность результатов и выводов работы подкрепляется глубоким анализом современного состояния исследований в предметной области, непротиворечивым обоснованием предложенных методик, апробацией полученных результатов в научных публикациях и докладах на различных международных и российских конференциях, а также внедрением результатов в реально работающие экспериментальные сети КРК (Университетская квантовая сеть, ViPNet QTS), комплексы систем КРК (ViPNet Quandor, ViPNet QSS, Квазар-СКР), а также использованием результатов диссертационного исследования в методических рекомендациях Технического комитета 26.

Рекомендации по использованию результатов работы

Результаты диссертационной работы Жиляева А.Е. *уже используются* в экспериментальных сетях, и могут быть также применены при проектировании протяженных сетей квантового распределения ключей, а также комплексов защиты информации с использованием систем квантового распределения ключей.

Публикации по теме диссертации

Результаты, полученные в диссертации, своевременно опубликованы и доложены на научных конференциях по данной тематике.

По материалам диссертации Жиляевым А.Е. опубликовано 8 научных работ, в том числе 4 работы в изданиях, рекомендованных ВАК РФ, 2 работы в изданиях, индексируемых в базах Scopus и WoS, получены 3 патента на изобретения. Результаты представлены на различных российских и международных конференциях. Отмечу, что автором представлены доклады на двух престижных международных конференциях

9-th International Conference on Quantum Cryptography (QCrypt-2019), (Монреаль, Канада, 2019);
10-th International Conference on Quantum Cryptography (QCrypt-2020), (Амстердам, Нидерланды, 2020);

Замечания по работе

1. Целесообразно было бы подробнее описать процессы построения карты сети КРК и подходов к определению последовательности узлов сети, необходимых для непосредственно формирования КЗК.
2. Предложение использования общего ключа между целевыми УКС не позволяет применять квантовые технологии для этой подсистемы при распределении КЗК. В то же время возможность применения постквантовых алгоритмов для этих целей требует дальнейших исследований. Вместе с тем следует дополнительно рассмотреть возможность распределения КЗК с использованием только защиты на квантовых ключах, например, по различным маршрутам между целевыми УКС.
3. В описании разработанных способов распределения КЗК обозначение n используется и для обозначения числа узлов в цепочке УКС и для обозначения числа квантовых ключей.

Соответствие темы диссертации заявленной научной специальности

Тема и положения, выносимые на защиту, соответствуют паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» по пунктам:

- 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 (п. 6);

- модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем (п. 8);

- принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности (п. 13).

Оформление диссертации и автореферата соответствует требованиям ГОСТ Р 7.0.11-2011. Автореферат правильно отражает содержание диссертации.

Говоря более неформально, работа оформлена аккуратно, при внимательном прочтении текста мне не удалось обнаружить в тексте ни одной опечатки.

Оценка диссертации

Диссертация Жиляева А.Е. является завершенной научно-квалификационной работой, в которой даны научно обоснованные решения по построению протяженных сетей квантового распределения ключей сложных топологий, в особенности в части безопасного и стойкого распределения общих секретов в пары средств защиты информации, произвольно подключенных к узлам сети КРК.

Диссертация отвечает требованиям пункта 9 «Положения о порядке присуждения ученых степеней» ВАК РФ по актуальности, научной новизне, значимости, объему выполненных исследований, практической и теоретической значимости.

Исходя из выше сказанного, считаю, что Жиляев Андрей Евгеньевич, заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Официальный оппонент _____ / Молотков Сергей Николаевич/

Доктор физико-математических наук (специальность 010407 Физика конденсированного состояния), главный научный сотрудник Института физики твердого тела РАН

ФГБУН Институт физики твердого тела имени Ю.А. Осипьяна Российской академии наук

142432, Московская обл., г. Черноголовка, ул.Академика Осипьяна д.2, ИФТТ РАН
Телефон: +74965221982
Эл. Почта. adm@issp.ac.ru

Подпись заверяю
Ученый секретарь ИФТТ РАН

_____ /к.ф.-м.н. Терещенко Алексей Николаевич/

24 августа 2022