DOI: 10.18137/RNU.V9187.24.04.P.91 УДК 004.056

Д.А. Глозштейн

СПОСОБЫ МАРШРУТИЗАЦИИ В СЕТЯХ С КВАНТОВЫМ РАСПРЕДЕЛЕНИЕМ КЛЮЧЕЙ

Аннотация. В статье рассматриваются вопросы адаптации методов квантовой криптографии для современных сетей. В частности, проанализированы возможности использования квантового распределения ключей как одной из наиболее активно развивающихся областей квантовой криптографии. Рассмотрена возможность использования классической маршрутизации для интеграции квантового распределения ключей. Систематизированы и обобщены возможные стратегии разработки способов маршрутизации в сетях с использованием квантового распределения ключей, определены эффективные подходы к созданию протоколов маршрутизации в квантовых сетях. Выделены основные технические барьеры при реализации технологии квантового распределения ключей, такие как невысокая скорость выработки защищенного ключа, ограниченное расстояние прямого взаимодействия, необходимость в доверенных узлах-посредниках. Рассмотрены проблемы при интеграции квантовых технологий, таких как нарушение когерентности квантовой памяти, ограниченность диапазонов передачи данных, необходимость в сложном специализированном оборудовании. Представлены ключевые аспекты квантовой маршрутизации и связанные с этим свойства, описывающие квантовое распределение ключей, определен выбор подхода, который позволит построить наиболее эффективную сеть квантового распределения ключей.

Ключевые слова: информационная безопасность, квантовые методы защиты информации, квантовая криптография, квантовое распределение ключей, способы маршрутизации, архитектура компьютерных сетей, программно-определяемые сети.

D.A. Glozshtein

ROUTING METHODS IN NETWORKS WITH QUANTUM KEY DISTRIBUTION

Abstract. The article discusses the adaptation of quantum cryptography methods for modern networks. In particular, the possibilities of using quantum key distribution (QKD) as one of the most actively developing areas of quantum cryptography are analyzed. The article discusses the possibility of using classical routing to integrate quantum key distribution. Possible strategies for the development of routing methods in networks using QKD are systematized and generalized, and effective approaches to the creation of routing protocols in quantum networks are identified. The main technical barriers to the implementation of the QKD technology are highlighted, such as the low speed of generating a secure key, the limited distance of direct interaction and the need for trusted intermediary nodes. The problems in the integration of quantum technologies, such as violation of the coherence of quantum memory, the limited range of data transmission and the need for complex specialized equipment, are considered. The article presents the key aspects of quantum routing and related properties describing the QKD, and selects an approach that will build the most efficient QKD network.

Keywords: information security, quantum methods of information protection, quantum cryptography, quantum key distribution, routing methods, architecture of computer networks, software-defined networks.

Введение

Создание защищенных криптографических ключей в общедоступных сетях является одним из ключевых вопросов информационной безопасности [1]. Несмотря на безопасность, инфраструктура открытых ключей на данный момент теоретически уязвима

Глозштейн Даниил Александрович
старший преподаватель кафедры информационной безопасности, Поволжский государственный технологический университет, город Йошкар-Ола. Сфера научных интересов: информационная безопасность, квантовые методы защиты информации, информационная безопасность систем видео-конференц-связи. Автор 20 опубликованных научных работ. ORCID: 0000-0002-0726-547X. Электронный адрес: glozshtejnda@volgatech.net

к атакам злоумышленников. Развитие квантовых компьютеров и появление алгоритмов, решающих сложные задачи за полиномиальное время (например, алгоритм Шора [2]), приводит к появлению новых возможностей для злоумышленников. Для решения этой проблемы можно использовать квантовое распределение ключей (далее – КРК) [3]. Сети КРК отличаются тем, что в качестве фундамента безопасности используют защиту на основе физических законов, а не сложность решения математических задач [4]. Классические протоколы маршрутизации не рассчитаны на особенности КРК, поэтому их взаимная интеграция вызывает определенные сложности. Таким образом, разработка нового протокола маршрутизации с возможностью использования квантово защищенных ключей является одной из важнейших задач для развития систем КРК [5].

Особенности сетей с использованием КРК обусловлены значительными различиями в сравнении со стандартными коммуникационными сетями, вызванными специфическими свойствами квантовых каналов связи и сложностью их технической реализации. КРК имеет ряд серьезных технических барьеров, как, например, невысокая скорость выработки защищенного ключа и ограниченное расстояние прямого взаимодействия из-за ограниченной эффективности обнаружения фотонов, а также помех в канале связи и потерь при передаче сигнала. Кроме того, всё еще нет конкретных реализаций квантовых повторителей, что сильно снижает возможности расширения и масштабирования таких сетей. Совместное использование квантовых и классических каналов требует весьма точного планирования маршрутов передачи данных. Для организации этого процесса требуется несколько квантовых повторителей и доверенных узлов сети, которые упрощают взаимодействие сторон. Эти промежуточные узлы необходимы для повышения дальности связи за счет снижения потерь сигнала благодаря уменьшению длины отдельных прямых каналов передачи. Также посредник может проводить контрольные измерения состояний для повышения безопасности. Рост количества возможных маршрутов для сетей КРК также позволяет повысить скорость генерации ключей, так как их можно равномерно распределить по всем возможным каналам передачи.

Целью данной статьи является систематизация и обобщение возможных стратегий разработки способов маршрутизации в сетях с использованием КРК, что необходимо для определения эффективных подходов к созданию протоколов маршрутизации в квантовых сетях, развития технического понимания режимов работы этих сетей и подходов к реализации их отдельных элементов. Это позволит выполнить более эффективное моделирование и предложить конкретные решения в области выстраивания квантовых каналов связи, а также для обобщения представления о проектировании полноценной сети КРК, интегрированной в общие сети передачи данных.

Архитектура сети КРК

Общая структура сети. На данный момент нет решений, которые позволяют абстрагировать квантовую защиту от классической сети. Архитектура сетей КРК может быть разнообразной, и количество уровней при их формализации зависит от уникальных функций, предоставляемых квантовыми методами защиты информации. Если обобщить известные решения в данной области, можно выделить три логических уровня при построении системы с использованием КРК (см. Рисунок 1).

Рисунок 1. Архитектура сети КРК
Источник: здесь и далее рисунки выполнены автором.

1. *Уровень инфраструктуры* описывает обязательные элементы сети. Они должны располагаться в доверенных узлах (узлах КРК), которые должны быть защищены от возможных атак на физическом уровне. Эти узлы могут устанавливать соединение как по беспроводным, так и по оптоволоконным каналам. Сами ключи и их основные характеристики (идентификатор, размер, тип, временные метки и др.) надежно хранятся на доверенных узлах [6]. Кроме того, узлы хранят информацию о параметрах канала.

2. *Уровень управления* включает контроллер сети и управляющее устройство [7]. К ведению контроллера относится активация и настройка всех узлов КРК. Управляющее устройство отвечает за обслуживание сети, в том числе за мониторинг и сбор данных о параметрах соединений и узлах сети. Секретные ключи хранятся в физически изолированных расположениях. Эти меры гарантируют, что они недоступны для устройств уровня управления, что обеспечивает безопасность ключей [8].

3. К *прикладному уровню* относятся характерные для сети КРК криптографические сервисы. В частности, на прикладном уровне происходит передача приложениями требований безопасности управляющему устройству. Затем оно запрашивает ключи. Если они доступны, сетевому контроллеру передается запрос на предоставление этих ключей для шифрования. Далее каждое приложение самостоятельно отвечает за их использование и управление [9].

Составляющие сети КРК. С учетом общей структуры среди элементов сети КРК можно выделить следующие:

• сетевые узлы – основа для квантово защищенной сети; они проектируются с возможностью полной защищенности от подслушивания, взлома и прочих атак;

• контроллер сети – обычно представлен сервером, который отвечает за управление сетевыми узлами, их подключение и настройку, выполняет функции контроля доступа к узлам, аутентификации и маршрутизации, передавая секретные ключи и обеспечивая возможности восстановления после неисправностей;

• криптографический сервис – фактически представляет собой интерфейс пользователя с учетом необходимых требований безопасности, таких как запросы на получение ключей, с учетом их параметров: размера, скорости и частоты обновления ключей.

Методики проектирования сетей КРК

В настоящее время идет активная работа по преодолению проблем, которые возникают при технической реализации сетей КРК. Существует несколько принципиально разных подходов к их проектированию.

КРК на основе программно-определяемых сетей (SDN-сети). Примером такой сети является модель, предложенная в [10], которая объединяет идеи систем КРК и SDN (Software Defined Network), для которой необходим способ их согласования с классическими сетевыми устройствами (см. Рисунок 2). В частности, при проектировании такой модели необходимо отойти от внутренней структуры КРК и рассмотреть взаимодействие с SDN-контроллером более абстрактно. Такой подход помогает при стандартизации разрабатываемых технологических решений, которые ранее специфицировались под требования отдельных клиентов.

В узел КРК в такой модели входят четыре основных компонента:

1) интерфейсы между узлами и системами КРК, которые объединены в пределах сетевого узла;

2) приложения как внутренние и внешние объекты, использующие полученные из управляющей системы ключи;

3) физические или виртуальные каналы связи между узлами сети;

4) дополнительная информация, в качестве которой могут выступать идентификаторы, физическое местонахождение узлов и др. Такая информация обычно используется для повышения качества работы сетевых узлов.

Таким образом, подсистема КРК поддерживает квантовые каналы связи и предоставляет клиентам доступ к защищенным ключам, распределяемым системой управления клю-

чами, а подсистема SDN собирает данные с узлов сети, связывается с контроллером и выполняет обновления при поступлении соответствующих запросов от контроллера КРК. Модель требует слаженной работы от систем SDN, КРК и управления ключами.

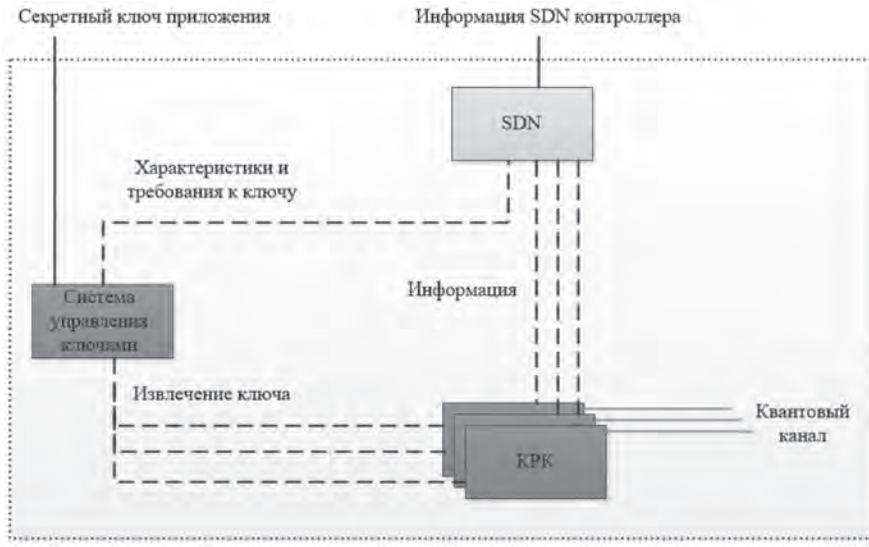

Рисунок 2. КРК на основе программно-определяемых сетей

КРК на основе маршрутизации и диапазона ключей была описана в [6]. В статье делается предположение, что КРК-сеть включает в себя множество автономных систем типа P2P (точка-точка), которые постоянно вырабатывают секретный ключ для смежных узлов сети (см. Рисунок 3). У каждого активного узла должен быть доступ к обычному и квантовому каналам связи. Классический канал работает как виртуальное соединение в сети (пунктирная линия на Рисунке 3).

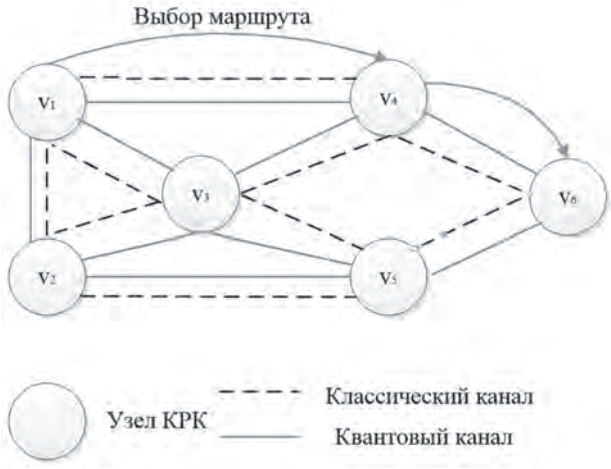

Рисунок 3. КРК на основе маршрутизации и диапазона ключей

Основная цель работы такого канала связи – передача данных для управления сетью, шифрования и др. Квантовый канал формируется с помощью оптоволоконной среды, соединяющей два соседних узла. Его задача – простая и быстрая генерация секретного ключа для каждой системы КРК. В такой сети каждая P2P-система работает независимо друг от друга, создавая ключи для пары своих узлов. Эти ключи хранятся в локальных диапазонах секретных ключей. В ряде случаев, если квантовый канал недоступен, создать надежный ключ между взаимодействующими узлами сети довольно сложно [11]. В такой ситуации общий ключ можно установить только за счет ретрансляции через систему из нескольких посредников. Такие глобальные ключи требуют использования значительного объема локальных ресурсов для их генерации и обслуживания. Однако подобная система обеспечивает защищенное взаимодействие даже без наличия прямого квантового канала связи. Фактически на основе этого ключа и обеспечивается безопасность приложений пользователей, таких передача файлов и обмен медиаданными. Если ситуация упрощается до прямого взаимодействия двух узлов, они могут использовать локальные диапазоны секретных ключей в качестве глобального ключа. Если же узлы не являются соседями, они получают ключ с помощью промежуточных узлов. Такая процедура называется обменом ключами, а комплекс промежуточных каналов КРК, используемых в этом процессе, называется путем ретрансляции.

КРК на базе промежуточных узлов снимает физические ограничения для построения сетей КРК. Так как излучение света (в соответствии с фундаментальными требованиями измерений и теоремой об отсутствии клонирования [12]) невозможно усилить, необходима разработка решений, позволяющих реализовать ретрансляцию квантового сигнала. Отсутствие таких ретрансляторов – одна из основных проблем развития и применения сетей КРК. Перспективным подходом является использование доверенных ретрансляторов, которые бы постепенно передавали ключи по маршруту в сети, начиная от исходного узла-отправителя и заканчивая получателем. При этом секретные ключи расшифровываются, а затем зашифровываются повторно. Этот процесс реализуется с помощью алгоритма одноразового блокнота.

На Рисунке 4 показана схема масштабирования системы КРК на значительное расстояние с использованием надежных ретрансляторов.

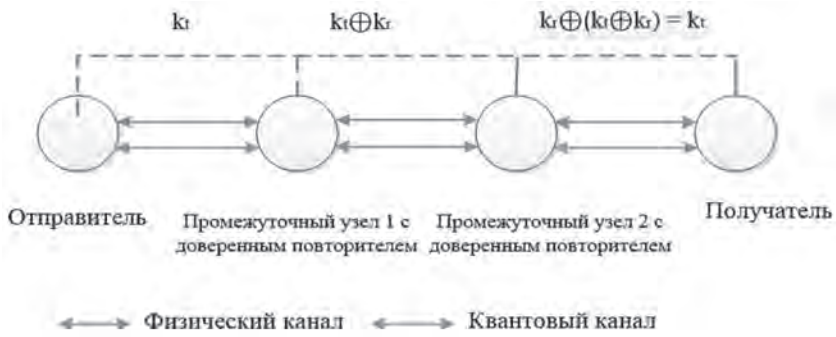

Рисунок 4. КРК на базе промежуточных узлов

Основная задача в данном случае заключается в установлении трех различных секретных ключей одинакового размера, каждый из которых служит для взаимодействия пар элементов системы:

1) сначала формируется секретный ключ между отправителем и первым промежуточным узлом, который определяет безопасность информационного обмена между ними;

2) на втором этапе вырабатывается ключ для промежуточных узлов, который убирает разрыв между отправителем и получателем, при этом обеспечивает необходимый уровень защищенности информации;

3) затем формируется ключ для последнего промежуточного узла и получателя, который обеспечивает сквозную безопасность соединения, сохраняя данные по мере их поступления.

КРК на основе оверлейной сети (см. Рисунок 5) является подходом, позволяющим вместо использования специфических квантовых каналов реализовать взаимодействие на основе классических каналов.

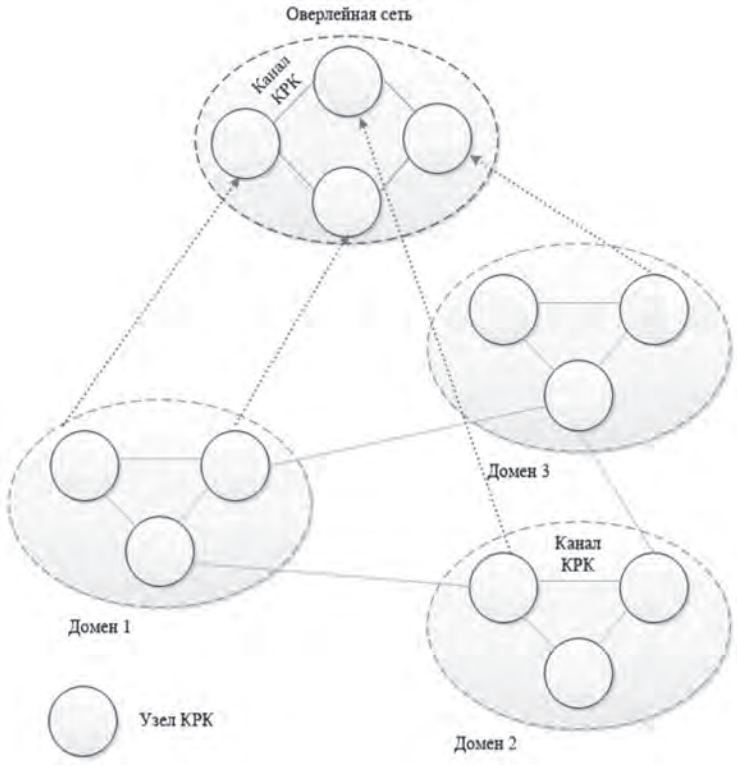

Рисунок 5. КРК на основе оверлейной сети

Такая организация сети применяется для создания инфраструктуры, обеспечивающей должное качество работы на более низких уровнях. Такие сети работают вне определенных поставщиками сетевых услуг маршрутов взаимодействия. Характерными чертами такого подхода является поиск альтернативных маршрутов, быстрая адаптация маршрутов к изменениям в сети и использование соединений с множеством путей передачи [13]. Использование таких соединений является эффективным решением для увеличения производительности сети, включая меры защиты от сетевых сбоев, распределение нагрузки, повышение общей пропускной способности и выбор маршрутов с наименьшей задержкой при передаче данных. При работе внешних протоколов маршрутизации (например, BGP)

снижается время ответа сети, поскольку протоколам необходимо определенное время для сбора и анализа информации об ошибках или перегрузке в работе сетевого соединения. Из-за этого согласование сети после отключения может продлиться довольно длительное время (до нескольких минут), что является весьма значительным временным интервалом для работы большинства приложений. Кроме того, использование в BGP только одного маршрута затрудняет определение альтернативных маршрутов передачи данных [14].

Для решения указанных проблем в оверлейной сети применяется одноранговый подход, упрощающий соединения и обеспечивающий поиск альтернативных маршрутов за счет инкапсуляции трафика в нижележащую сеть. Таким образом, при передаче данных промежуточные узлы получают пакет, распаковывают его, изучают адрес отправителя, повторно инкапсулируют его и пересылают прочим потенциальным получателям. В общем и целом, данный подход представляет собой стандартный пошаговый процесс, обычно реализуемый в сетях КРК (см. Рисунок 5). Достоинством оверлейных сетей является возможность строить маршруты в обход недоверенных узлов и быстро менять маршруты передачи данных в том случае, если какой-то узел утрачивает доверенное состояние.

Основные направления дальнейшей работы

1. Квантовые ретрансляторы необходимы для увеличения возможностей применения сетей КРК. Повторители убирают ограничение на дальность передачи, эффективно пересылая квантовую информацию и усиливая сигналы без потери квантовых свойств. Эта способность обеспечивает надежность КРК даже при значительных расстояниях между отправителем и получателем.

2. Так как в большинстве систем КРК скорость выработки ключа крайне низка, особенно для современных высокопроизводительных пользовательских сервисов, актуальным вопросом является создание высокоскоростных систем КРК. Низкая скорость генерации вызвана в основном физической природой квантовых сигналов, в частности, отдельные фотоны в принципе имеют довольно низкое соотношение сигнал/шум, что значительно снижает скорость генерации ключей.

3. Для квантовых сетей необходимо использование специфических топологий. Грамотно составленная топология играет важную роль в обеспечении безопасности распределения секретных ключей.

4. Для регламентации передачи и обработки квантовой информации требуется разработка квантовых протоколов. В квантовых криптографических протоколах используются принципы квантовой механики для создания ключей с гарантированной защитой от определенных атак, например, от подслушивания. Квантовые сетевые протоколы определяют создание, передачу и измерение квантовых состояний между сетевыми узлами. Кроме того, в число функций этих протоколов входит исправление ошибок, усиление конфиденциальности и очистка ключа.

5. Определяющим фактором для дальнейшего развития квантовых методов защиты информации является возможность интеграции в существующую сетевую инфраструктуру. Для более доступного применения квантовых технологий современные исследования направлены в первую очередь на создание простого, надежного и общедоступного аппаратного обеспечения. Появление доступных систем КРК является ключевым фактором для их массового использования максимально широким кругом клиентов, что в итоге будет способствовать их использованию в большинстве секторов экономики.

Заключение

Сети КРК обеспечивают длительную безопасность данных и надежную защиту широкого диапазона сетевых приложений. Однако в области технической реализации и практического внедрения квантовых методов защиты информации существует значительное количество проблем и нерешенных вопросов. В данной статье проведен всесторонний обзор существующих решений в области проектирования сетей КРК. Классифицируются варианты реализации сетей КРК и их возможные сценарии дальнейшего развития, такие как разработка более надежных ретрансляторов, интеграция с архитектурой SDN и использование диапазонов ключей на основе маршрутизации [15]. Также рассмотрена общая архитектура сетей КРК, их основные компоненты, протоколы и интерфейсы. Оценены перспективы различных направлений дальнейших исследований в области внедрения квантовых методов защиты информации и формирования масштабной инфраструктуры квантового интернета. Дальнейшее развитие данной сферы исследований требует значительной концентрации интеллектуальных и технологических ресурсов на стыке областей квантовой физики, информационной безопасности и коммуникаций.

Литература

1. *Maurer U.M.* Secret key agreement by public discussion from common information // IEEE transactions on information theory. 1993. Vol. 39. No. 3. P. 733–742. DOI: 10.1109/18.256484

2. *Shor P.W.* Algorithms for quantum computation: Discrete logarithms and factoring // Proceedings 35th annual symposium on foundations of computer science. Santa Fe, NM, USA, November 20–22, 1994. P. 124–134. DOI: 10.1109/SFCS.1994.365700

3. *Shor P.W., Preskill J.* Simple proof of security of the BB84 quantum key distribution protocol // Physical review letters. 2000. Vol. 85. No. 2. P. 441–444. DOI: https://doi.org/10.1103/PhysRevLett.85.441

4. *Nejatollahi H., Dutt N., Ray S., Regazzoni F., Banerjee I., Cammarota R.* Post-quantum lattice-based cryptography implementations: A survey // ACM Computing Surveys (CSUR). 2019. Vol. 51. No. 6. Article no. 129. Pp. 1–41. DOI: https://doi.org/10.1145/3292548

5. *Mustafa O.S., Askar S.* A Novel Security Survival Model for Quantum Key Distribution Networks Enabled by Software-Defined Networking // IEEE Access. 2023. Vol. 11. P. 21641–21654. DOI: 10.1109/ACCESS.2023.3251649

6. *Yang C., Zhang H., Su J.* Quantum key distribution network: Optimal secret-key-aware routing method for trust relaying // China Communications. 2018. Vol. 15. No. 2. Pp. 33–45. DOI: 10.1109/CC.2018.8300270

7. *Cao Y., Zhao Y., Wang Q., Zhang J., Ng S.X., Hanzo L.* The evolution of quantum key distribution networks: On the road to the qinternet // IEEE Communications Surveys & Tutorials. 2022. Vol. 24. No. 2. Pp. 839–894. DOI: 10.1109/COMST.2022.3144219

8. *Schoute E., Mancinska L., Islam T., Kerenidis I., S Wehner.* Short-cuts to quantum network routing // arXiv. 2016. DOI: https://doi.org/10.48550/arXiv.1610.05238

9. Recommendation ITU-T Y.3800: Overview on networks supporting quantum key distribution. International Telecommunication Union : Geneva, Switzerland, 2019. URL: https://handle.itu.int/11.1002/1000/13990 (дата обращения: 11.10.2024).

10. *Yao J., Wang Y., Li Q., et al.* An Efficient Routing Protocol for Quantum Key Distribution Networks // Entropy. 2022. Vol. 24. No. 7. Article no. 911. P. 137–147. DOI: https://doi.org/10.3390/e24070911

11. *Aguado A., Lopez V., Martinez-Mateo J., Szyrkowiec T., Autenrieth A., Peev M., Lopez D., Martin V.* Hybrid Conventional and Quantum Security for Software Defined and Virtualized Networks // Journal of Optical Communications and Networking. 2017. Vol. 9. Vol. 10. P. 819–825. DOI: https://doi.org/10.1364/JOCN.9.000819
12. *DiAdamo S., Qi B., Miller G., Kompella R., Shabani A.* Packet switching in quantum networks: A path to the quantum internet // Physical Review Research. 2022. Vol. 4. No. 4. Article no. 043064. DOI: https://doi.org/10.1103/PhysRevResearch.4.043064
13. *Mehic M., Niemiec M., Rass S., Ma J., Peev M., Aguado A., Martin V., Schauer S., Poppe A., Pacher C., et al.* Quantum key distribution: A networking perspective // ACM Computing Surveys (CSUR). 2020. Vol. 53. No. 5. P. 1–41. DOI: https://doi.org/10.1145/3402192
14. *Pant M., Krovi H., D Towsley., Tassiulas L., Jiang L., P Basu., Englund D., Guha S.* Routing entanglement in the quantum internet // npj Quantum Information. 2019. Vol. 5. No. 1. P. 25. DOI: https://doi.org/10.1038/s41534-019-0139-x
15. *Waxman B.M.* Routing of multipoint connections // IEEE journal on selected areas in communications. 1988. Vol. 6. No. 9. P. 1617–1622. DOI: 10.1109/49.12889

References

1. Maurer U.M. (1993) Secret key agreement by public discussion from common information. In: *IEEE transactions on information theory*. Vol. 39. No. 3. Pp. 733–742. DOI: 10.1109/18.256484
2. Shor P.W. (1994) Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th annual symposium on foundations of computer science. Santa Fe, NM, USA. November 20–22, 1994. Pp. 124–134. DOI: 10.1109/SFCS.1994.365700
3. Shor P.W., Preskill J. (2000) Simple proof of security of the BB84 quantum key distribution protocol. *Physical review letters.* 2000. Vol. 85. No. 2. Pp. 441–444. DOI: https://doi.org/10.1103/PhysRevLett.85.441
4. Nejatollahi H., Dutt N., Ray S., Regazzoni F., Banerjee I., Cammarota R. (2019) Post-quantum lattice-based cryptography implementations: A survey. *ACM Computing Surveys (CSUR)*. Vol. 51. No. 6. Article no. 129. Pp. 1–41. DOI: https://doi.org/10.1145/3292548
5. Mustafa O.S., Askar S. (2023) A Novel Security Survival Model for Quantum Key Distribution Networks Enabled by Software-Defined Networking. In: *IEEE Access*. Vol. 11. Pp. 21641–21654. DOI: 10.1109/ACCESS.2023.3251649
6. Yang C., Zhang H., Su J. (2018) Quantum key distribution network: Optimal secret-key-aware routing method for trust relaying. *China Communications.* Vol. 15. No. 2. Pp. 33–45. DOI: 10.1109/CC.2018.8300270
7. Cao Y., Zhao Y., Wang Q., Zhang J., Ng S.X., Hanzo L. (2022) The Evolution of Quantum key Distribution Networks: On the Road to the Qinternet. In: *IEEE Communications Surveys & Tutorials.* Vol. 24. No. 2. Pp. 839–894. DOI: 10.1109/COMST.2022.3144219
8. Schoute E., Mancinska L., Islam T., Kerenidis I., S Wehner. (2016) Short-cuts to quantum network routing. *arXiv.* DOI: https://doi.org/10.48550/arXiv.1610.05238
9. Recommendation ITU-T Y.3800: Overview on networks supporting quantum key distribution. International Telecommunication Union : Geneva, Switzerland, 2019. URL: https://handle.itu.int/11.1002/1000/13990 (accessed 11.10.2024).
10. Yao J., Wang Y., Li Q., et al. (2022) An Efficient Routing Protocol for Quantum Key Distribution Networks. *Entropy*. Vol. 24. No. 7. Article no. 911. Pp. 137–147. DOI: https://doi.org/10.3390/e24070911

11. Aguado A., Lopez V., Martinez-Mateo J., Szyrkowiec T., Autenrieth A., Peev M., Lopez D., Martin V. (2017) Hybrid Conventional and Quantum Security for Software Defined and Virtualized Networks. *Journal of Optical Communications and Networking*. Vol. 9. Vol. 10. Pp. 819–825. DOI: https://doi.org/10.1364/JOCN.9.000819
12. DiAdamo S., Qi B., Miller G., Kompella R., Shabani A. (2022) Packet switching in quantum networks: A path to the quantum internet. *Physical Review Research*. Vol. 4. No. 4. Article no. 043064. DOI: https://doi.org/10.1103/PhysRevResearch.4.043064
13. Mehic M., Niemiec M., Rass S., Ma J., Peev M., Aguado A., Martin V., Schauer S., Poppe A., Pacher C., et al. (2020) Quantum key distribution: A networking perspective. *ACM Computing Surveys (CSUR).* Vol. 53. No. 5. Pp. 1–41. DOI: https://doi.org/10.1145/3402192
14. Pant M., Krovi H., D Towsley., Tassiulas L., Jiang L., P Basu., Englund D., Guha S. (2019) Routing entanglement in the quantum internet. *npj Quantum Information*. Vol. 5. No. 1. P. 25. DOI: https://doi.org/10.1038/s41534-019-0139-x
15. Waxman B.M. (1988) Routing of multipoint connections // IEEE journal on selected areas in communications. vol. 6. no. 9. P. 1617–1622. DOI:10.1109/49.12889