Инженерный вестник Дона, №9 (2024)
ivdon.ru/ru/magazine/archive/n9y2024/9489

Обзор топологий сетей квантовых коммуникаций

А.П. Плёнкин

Южный федеральный университет, Таганрог

Аннотация: В статье рассматриваются тенденции развития высокотехнологичной отрасли квантовые коммуникации. Описаны наиболее популярные топологии квантовых коммуникационных сетей, в том числе, с доверенными промежуточными узлами. Приведены способы взаимодействия узлов магистральной квантово-криптографической сети и представлены основные методы обеспечения защищенной передачи в таких сетях. Рассмотрена упрощенная схема распределения квантового секретного ключа между конечными сегментами магистральной телекоммуникационной сети с использованием доверенных промежуточных узлов. Описаны возможные каналы утечки данных в общей структуре квантово-криптографических сетей.
Ключевые слова: квантовые коммуникации, квантовый ключ, топологии сетей, доверенные узлы.

За последние десятилетия квантовая криптография стала одной из наиболее быстроразвивающихся и актуальных областей современной науки. Проблемами отрасли являются: дальность квантовых каналов, отсутствие повторителей и корреляция между различными системами квантовой связи. Важность квантовых каналов связи заключается в том, что их реализация позволяет учитывать фундаментальные законы квантовой механики [1, 2]. К тому же, у квантовых каналов есть еще одно преимущество перед классическими - с их помощью можно передавать как квантовую, так и классическую информацию [3, 4]. Наиболее технологически развитым примером в этой области является квантовое распределение ключей. Можно говорить о том, что квантовые коммуникации сводятся к практической реализации технологии квантового распределения ключей. Особое внимание исследователей традиционно уделено квантовым протоколам с различными способами кодирования. Например, протоколы с фазовым кодированием состояний фотонов считаются наиболее стабильными в работе и достаточно простыми в реализации, что обусловлено их широким применением в сегодняшнем мире. Протоколы с поляризационным кодированием имеют преимущества при использовании в атмосферных системах передачи, так как

изменение поляризации практически не происходит в открытом пространстве. С другой стороны, передача оптических сигналов через открытое пространство сталкивается с множеством технологических трудностей. Так, например, возмущения атмосферы предсказать практически невозможно, и, следовательно, невозможно предсказать влияние паразитных помех на канал связи. Системы квантового распределения ключей с фазовым кодированием играют важную роль в реализации дорожной карты по развитию квантовых коммуникаций в Российской Федерации.

В области квантовых коммуникаций актуальным является ряд задач: разработка эффективного метода взаимодействия между узлами смешанной топологии квантово-криптографической сети; задача последней мили, когда решается проблема распределения ключа конечным пользователям; поиск новых методов синхронизации и обмена секретными ключами между устройствами (узлами) магистральной квантовой сети; квантовое распределение ключей в схемах «подвижный объект - стационарный объект», «подвижный объект - подвижный объект»; разработка фундаментальных методов, обеспечивающих синхронизацию и обмен квантовыми ключами двух и более устройств распределенной квантовой сети.

Квантово-криптографические сети.

Технология квантового распределения ключей (КРК) сегодня обеспечивает формирование секретного ключа на ограниченном расстоянии между двумя пользователями. Предельное расстояние при КРК определяется, с одной стороны, работой квантового протокола, а с другой стороны упирается в технологические свойства конструктивных элементов. В качестве квантового канала применяется стандартное одномодовое «темное» оптическое волокно. При длине волоконно-оптической линии связи более 100 км потери становятся весьма большими и могут полностью заглушить оптический сигнал. Простейшей реализацией квантово-криптографической

сети является топология «точка-точка», при которой два пользователя соединены между собой напрямую квантовым каналом. Такая топология является базовой для построения более масштабных, распределенных квантовых сетей. При построении магистральных квантовых сетей задача преодоления предельной длины квантового канала решается в том числе при помощи доверенных промежуточных узлов (ДПУ). Другая технология, позволяющая использовать квантовые сети произвольной длины, заключается в применении квантовых повторителей. В классических сетях для передачи сигналов можно использовать усилители, но в квантовых коммуникациях такой возможности нет. Усилитель в квантовых сетях равнозначен по свойствам злоумышленнику и отличить повторитель от шпиона на практике практически невозможно. Известны исследования, которые описывают идею квантового повторителя на основе перепутанных пар фотонов. В основе таких устройств лежит технология квантовой телепортации. Еще одним вектором развития квантовых сетей является создание квантовой памяти. Отметим, что на момент написания материала, технологии квантовых повторителей и квантовой памяти находятся в стадии исследования и далеки от практического использования.

Рассмотрим наиболее популярные топологии квантово-криптографических сетей. Топология «точка-точка». В базовой схеме есть отправитель (Алиса), получатель (Боб), квантовый и общедоступный каналы. На практике Алиса и Боб являются приемо-передатчиками, но для удобства трактовки принято выделять отправителя и получателя. В качестве квантового канала используется волоконно-оптическая линия связи (ВОЛС). В такой модификации нет существенных проблем распределения секретного ключа. Два удаленных пользователя получают квантовые ключи непосредственно из систем КРК. Ограничением топологии «точка-точка» по-прежнему является длина квантового канала. Топология «кольцо». Здесь

каждый сегмент сети содержит отправителя и получателя. Распределение ключей происходит между сегментами таким образом, что работа станций системы КРК одного сегмента не зависит от работы станций СКРК другого сегмента. Соответственно, в такой схеме использование полученных ключей возможно согласно топологии, т. е. между сегментами, в которых установлены системы КРК. Если требуется использование ключей из не смежных сегментов, то это потребует дополнительных действий по передаче квантовых ключей в соответствующие узлы сети. При топологии «звезда» эффективным решением является распределение отправителей на концах ВОЛС, а получателей в центральном узле. Такое расположение систем КРК обусловлено конструктивными особенностями самих станций. Как правило, в реализованных системах квантового распределения ключей станция отправителя не имеет высокотехнологичных, сложных в реализации элементов. Станция получателя, напротив, в своем составе предполагает использование лавинных фотодиодов (ОЛФД). На сегодняшний день этот элемент является краеугольным камнем при конструировании системы квантового распределения ключей. ОЛФД, как и квантовые генераторы случайных чисел являются сложными в исполнении конструктивными элементами. По этой причине при топологии «звезда» станции - получатели сконцентрированы в центральном сегменте.

Особое внимание заслуживают сети смешанной топологии (рис. 1). Как правило, именно такие сети больше остальных могут использоваться в городской инфраструктуре. При смешанной топологии распределение систем КРК носит ситуативный характер. Сегменты такой сети строятся с учетом локальных топологий. Техническая сложность реализации подобных сетей заключается в сложности организации квантовых каналов для распределения ключей. В крупных сетях смешанной топологии достаточно сложно обеспечить единообразие оборудования, т. е. в разных сегментах сети может

использоваться различное оборудование квантовой связи. Последнее означает, что необходимо иметь некий инструмент (метод, подход) для согласования отдельных вендоров оборудования в единой сети квантовых коммуникаций. Как и в вышеописанных топологиях, здесь сохраняется задача по распределению секретных ключей между сегментами.

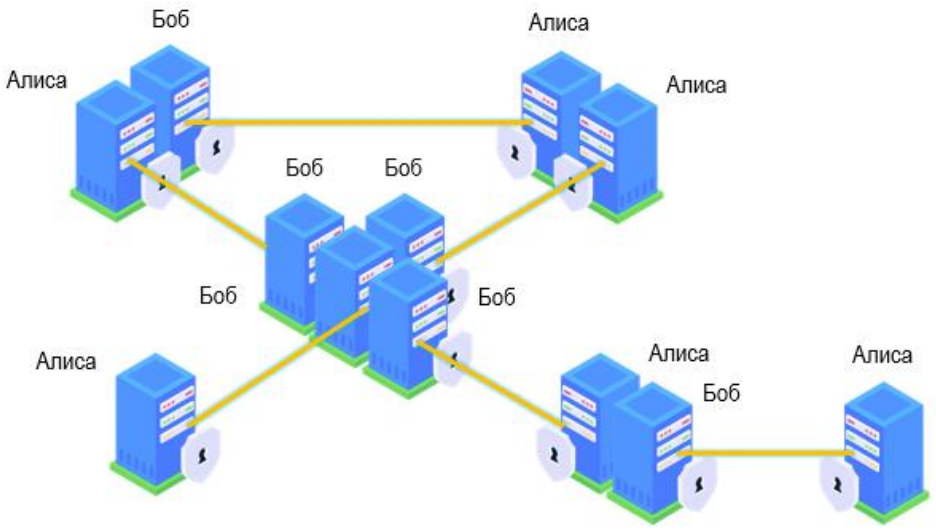

Рис. 1 – Смешанная топология квантово-криптографической сети

Наиболее ярким примером квантово-криптографической сети является анонсированная в 2021 году коммуникационная квантовая сеть, соединяющая города Пекин и Шанхай [5]. Оптическая сеть имеет общую протяженность более 4000 км и сочетает в себе как передачу сигналов через ВОЛС, так и через спутниковые системы квантовой связи. Рассматривая наземную инфраструктуру данной квантовой сети, можно выделить ряд особенностей: в основе лежит магистральная национальная волоконно-оптическая квантовая сеть; локальные городские сети преимущественно имеют топологию «звезда» и они подключены к магистральной квантовой сети посредством ВОЛС; квантово-криптографическая сеть работает с несколькими протоколами распределения ключей, но базовым протоколом является BB84; скорость формирования секретного ключа в среднем

составляет от 5 кбит/с до 80 кбит/с. (36 Мбит в неделю); тип используемых лавинных фотодетекторов – InGaAs / InP.

Как правило, реализация магистральной квантовой сети подразумевает наличие доверенных промежуточных узлов. Технически это представляет собой организацию защищенных, охраняемых помещений вдоль ВОЛС с оборудованием квантовой криптографии. Следует понимать, что доступ в ДПУ для злоумышленника практически равносилен знанию секретных ключей, поэтому защищенность ДПУ при анализе модели угроз описывается вероятностным фактором (в том числе, с учетом человеческого фактора).

Формирование и передача квантового ключа в сетях смешанной топологии.

Технология квантового распределения ключей включает несколько этапов: подготовка квантовых состояний в устройстве отправителя; передача квантовых состояний получателю; детектирование полученных состояний на стороне получателя и их интерпретация; согласование последовательности.

Рассматривая отдельно сегменты квантово-криптографической сети, необходимо выделить ДПУ. Доверенный узел в составе магистральной сети является наиболее уязвимой её частью. Это связано с тем, что внутри ДПУ данные могут передаваться или полностью в открытом виде или иметь достаточно «слабый» уровень шифрования. Считается, что защита от несанкционированного доступа к данным или элементам узла обеспечивается конструкцией ДПУ. В состав ДПУ входит средство криптографической защиты информации (СКЗИ), а основным оборудованием является СКРК. В одном доверенном узле, в зависимости от топологии сети, может находиться несколько комплектов систем КРК и СКЗИ. Рассмотрим типовую схему магистральной квантовой сети (рис. 2), в которой требуется передача секретной информации от отправителя к получателю через несколько ДПУ.

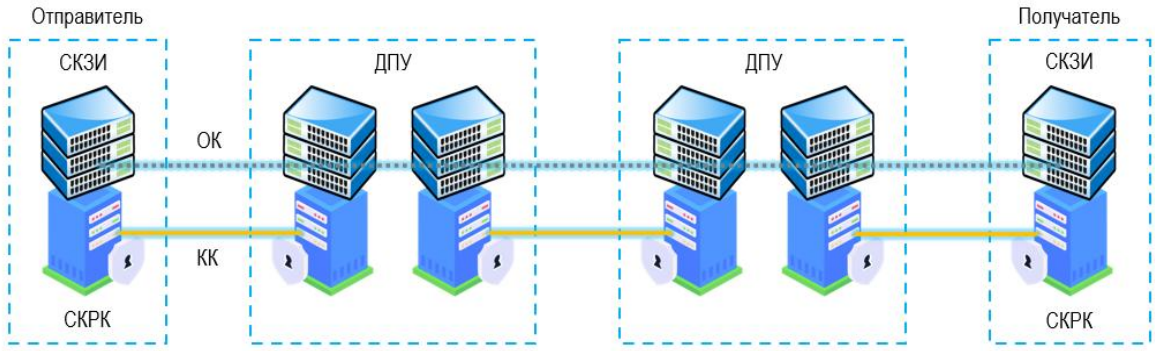

Рис. 2. – Магистральная квантовая сеть с ДПУ. КК - квантовый канал, ОК – общедоступный канал.

В подобной схеме применяется два основных подхода для передачи секретных данных: перешифрование данных и перешифрование ключей. При перешифровании данных в сетях на основе ДПУ происходит трансфер информации от одного квантового участка к другому и на каждом участке производится смена квантовых ключей шифрования. Таким образом, пользовательские данные приходят в доверенный промежуточный узел, зашифрованные одними квантовыми ключами, затем полностью расшифровываются внутри доверенного узла и далее зашифровываются другими квантовыми ключами перед передачей в следующий доверенный промежуточный узел. У такой схемы есть ряд существенных недостатков, которые отражаются как на требованиях к защищенности самого ДПУ, так и на скорости передачи. Так, многократная необходимость перешифрования большого объема информации влечет увеличение задержки при передаче данных, а наличие полностью расшифрованной информации является само по себе уязвимостью. При перешифровании ключей в сетях на основе ДПУ пользовательские данные остаются зашифрованными на всем промежутке от отправителя к получателю. Квантово-защищённые ключи в такой схеме распределяются между конечными пользователями и служат для шифрования пользовательских данных (рис. 3). Перешифрование данных в такой схеме уже не требуется, но необходим канал обмена ключами и

система управления ключами. Основные задачи такой системы управления заключаются в генерации, распределении, хранении, управлении полученными квантовыми ключами. Алгоритмы контроля за процессом выработки ключей также должны функционировать на каждом сегменте магистральной квантовой сети и следить за параметрами-индикаторами, например, за превышением уровня квантовых ошибок (QBER). Отметим, что в литературе встречается описание способа передачи ключей с перешифрованием на основе квантовых реле, а в работах [6 – 8] приводятся расчеты вероятности компрометации передачи (формирования) ключа.

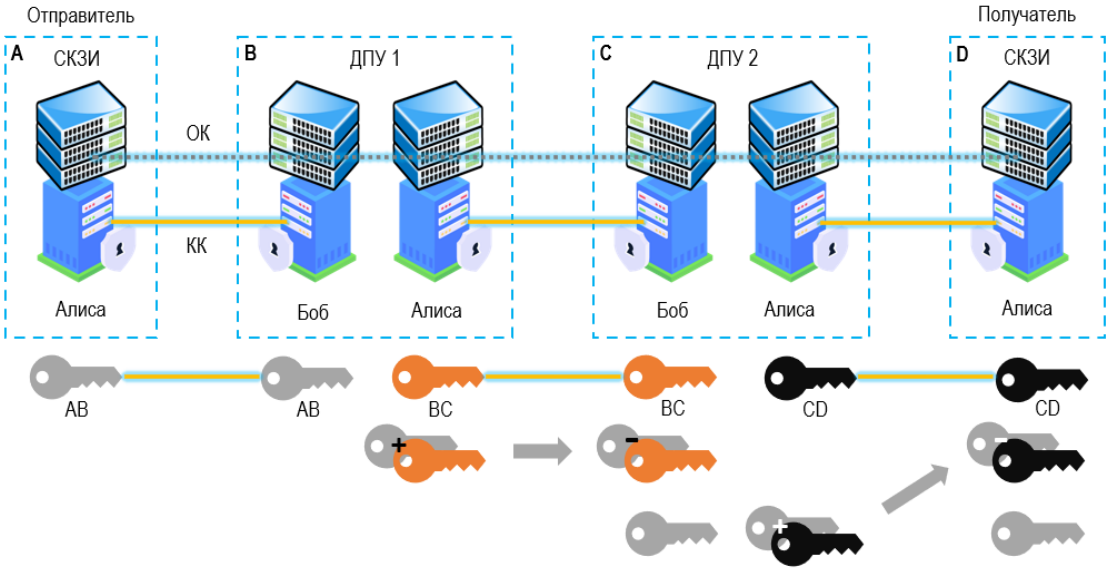

Рис. 3 – Распределение секретного ключа между ДПУ.

Каждый доверенный узел содержит комплект системы КРК, причем ключи формируются независимо между узлами A-B, B-C, C-D. Полученный на сегменте A-B квантовый ключ (AB) суммируется с квантовый ключом BC в узле B. Далее такой смешанный ключ передается по каналу связи на узел C, где из него вычитается ключ BC и прибавляется ключ CD. Далее ключ по цепочке передается к следующему сегменту и так далее, пока не достигнет целевого узла. В итоге пара конечных пользователей обладает одинаковым

квантовым ключом АВ, которым в дальнейшем могут зашифровываться пользовательские данные.

Отметим, что данная схема является упрощенной и имеет ряд очевидных недостатков. Так как сегменты сети, по сути, независимы друг от друга, то требуется постоянное согласование процесса выработки ключевого материала. На каждом доверенном узле ключ в какой-то момент появляется в «чистом» виде, что требует дополнительных мер усиления. С другой стороны, есть решения, которые предлагают усовершенствованный механизм обмена ключами [9].

Выводы и дискуссия

В данной статье мы рассмотрели общее устройство квантовых сетей на базе систем квантового распределения ключей, описали их типовые топологии. Привели примеры методов распределения квантовых ключей в сетях квантовых коммуникаций на основе доверенных промежуточных узлов. Описывая возможные каналы утечки данных в общей структуре квантово-криптографических сетей, можно выделить несколько «слабых» на наш взгляд мест: каналы взаимодействия между станцией СКРК и сервером, сервером и СКЗИ. В магистральных сетях с использованием ДПУ необходимо, в зависимости от метода распределения квантовых ключей и шифрования информации, разрабатывать специальные мероприятия по обнаружению возможных каналов утечки данных в помещениях ДПУ; ВОЛС или канал синхронизации. Исследования и практическое использование систем КРК показывают, что не менее важным является обеспечение защищенности каналов синхронизации и аутентификации [10].

В заключение можно сделать акцент на том, что реализация квантово-криптографических сетей в идеальном варианте исполнения возможна, но требует тщательной подготовки и постоянного мониторинга всех компонентов сети.

Литература

1. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography. Reviews of Modern Physics. 2002. Vol. 74, № 1. pp. 145−195.

2. Bennett C. H., Brassard G., Ekert A. K. Quantum cryptography. Scientific American. 1992. Vol. 267. №. 4. pp. 50-57.

3. Кулик С. Квантовая криптография. Фотоника. 2010. №. 2. С. 36-41.

4. Shannon C. E. Communication theory of secrecy systems. The Bell System Technical Journal. 1949. Vol. 28. № 4. pp. 656-715.

5. Chen Y. A. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature. 2021. № 7841. pp. 214-219.

6. Beals T. R., Sanders B. C. Distributed relay protocol for probabilistic information-theoretic security in a randomly-compromised network. Information Theoretic Security: Third International Conference. Proceedings 3. 2008. pp. 29-39.

7. Dianati M., Alleaume R. Architecture of the Secoqc quantum key distribution network. First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07). 2007. P. 13.

8. Barnett S. M., Phoenix S. J. D. Securing a quantum key distribution relay network using secret sharing. IEEE GCC Conference and Exhibition (GCC). 2011. pp. 143-145.

9. Сабанов А. Г., Шелупанов А. А. Идентификация и аутентификация в цифровом мире // М.: Горячая Линия–Телеком. 2022. 356 с.

10. Pljonkin A., Petrov D., Sabantina L., Dakhkilgova K. Nonclassical attack on a quantum key distribution system. Entropy. 2021. Vol. 23. № 5. URL: semanticscholar.org/paper/Nonclassical-Attack-on-a-Quantum-Key-Distribution-Pljonkin-Petrov/3d0e47b77009b0c8e63eb0938d9542d4812cbd23

References

1. Gisin N., Ribordy G., Tittel W., Zbinden H. Reviews of Modern Physics. 2002. Vol. 74, № 1. pp. 145−195.

2. Bennett C. H., Brassard G., Ekert A. K. Scientific American. 1992. Vol. 267. №. 4. pp. 50-57.

3. Kulik S. Kvantovaya kriptografiya [Quantum cryptography]. Fotonika. 2010. №. 2. pp. 36-41.

4. Shannon C. E. The Bell System Technical Journal. 1949. Vol. 28. № 4. pp. 656-715.

5. Chen Y. A. et al. Nature. 2021. № 7841. pp. 214-219.

6. Beals T. R., Sanders B. C. Information Theoretic Security: Third International Conference. Proceedings 3. 2008. pp. 29-39.

7. Dianati M., Alleaume R. First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07). 2007. P. 13.

8. Barnett S. M., Phoenix S. J. D. IEEE GCC Conference and Exhibition (GCC). 2011. pp. 143-145.

9. Sabanov A. G., Shelupanov A. A. Identifikaciya i autentifikaciya v cifrovom mire [Identification and authentication in the digital world]. Goriachaya liniya–Telekom. 2022. 356 p.

10. Pljonkin A., Petrov D., Sabantina L., Dakhkilgova K. Entropy. 2021. Vol. 23. № 5. URL: semanticscholar.org/paper/Nonclassical-Attack-on-a-QuantumKeyDistributionPljonkinPetrov/3d0e47b77009b0c8e63eb0938d9542d4812cbd23.

Дата поступления: 22.07.2024

Дата публикации: 30.08.2024