Столыпинский вестник

Научная статья

Original article

УДК 330.1

СОВРЕМЕННЫЕ КВАНТОВЫЕ ТЕХНОЛОГИИ ДЛЯ БЕЗОПАСНОГО ОБМЕНА ДАННЫМИ

MODERN QUANTUM TECHNOLOGIES FOR SAFE DATA EXCHANGE

Княжев Фёдор Романович, *студент, НИУ "МЭИ", Москва*

Knyazhev Fedor Romanovich, *student, National research university "MPEI", Moscow*

Аннотация: В современном подключенном мире мы полагаемся на коммуникационные сети во всем, от банковских услуг до сферы образования, от обмена данных при переговорах до оборонной отрасли. В настоящей статье рассмотрена концепция использования сравнительно безопасного квантового интернета и технологий, применение которых необходимо для обеспечения такой возможности, в том числе: технология квантового распределения ключей, квантового повторителя, квантовой телепортации. Приведены примеры использования вышеуказанных технологий для обеспечения безопасности связи, указаны возможные проблемы и зоны незащищенности от хакерских атак.

Abstract. In today's connected world, we rely on communications networks for everything from banking to education, from data exchange in negotiations to the

defense industry. This article discusses the concept of using a relatively secure quantum Internet and technologies, the use of which is necessary to provide such an opportunity, including: quantum key distribution technology, quantum repeater, quantum teleportation. Examples of the use of the above technologies to ensure communication security are given, possible problems and areas of vulnerability from hacker attacks are indicated.

Ключевые слова: квантовая связь, квантовый интернет, кибербезопасность, квантовое распределение ключей, безопасный интернет.

Key words: quantum communication, quantum internet, cybersecurity, quantum key distribution, secure internet.

Введение

Изучая квантовую связь, исследователи разрабатывают квантово-безопасные криптографические протоколы, а также сверхзащищенные каналы связи и глобальные квантовые сети, которые позволяют безопасно для отправителя и получателя передавать те или иные данные. Это крайне важная задача, так как ежедневно по всему миру из-за утечек данных раскрывается огромное количество конфиденциальной информации, от данных кредитных и медицинских карт, до ценной интеллектуальной собственности компаний [1-3]. Угроза, исходящая от кибератак, вынуждает правительства, вооруженные силы и бизнес искать более безопасные способы передачи информации.

Сегодня конфиденциальные данные обычно шифруются, а затем отправляются по оптоволоконным кабелям и другим каналам вместе с цифровыми «ключами», необходимыми для расшифровки информации. Данные и ключи отправляются в виде классических битов — потока электрических или оптических импульсов, представляющих *1* s и *0* s. И это делает их уязвимыми. Продвинутые хакеры имеют возможность читать и копировать передаваемые биты, не оставляя следов.

Квантовая связь использует законы квантовой физики для защиты данных. Эти законы позволяют частицам — обычно фотонам света для передачи

данных по оптическим кабелям — принимать состояние суперпозиции, что означает, что они могут одновременно представлять несколько комбинаций *1* и *0* . Частицы известны как квантовые биты или кубиты.

Прелесть кубитов с точки зрения кибербезопасности заключается в том, что если хакер попытается наблюдать за ними в процессе передачи, их сверххрупкое квантовое состояние «схлопнется» либо до *1*, либо до *0*. Это означает, что хакер не может вмешаться в кубиты, не оставив явных признаков активности.

Некоторые компании воспользовались этим свойством для создания сетей для передачи особо конфиденциальных данных на основе процесса, называемого квантовым распределением ключей, или QKD. По крайней мере, теоретически, эти сети сверхзащищены [4, 5].

Квантовое распределение ключей

Одной из величайших угроз при передаче данных является уязвимость цифровой связи. Криптография — это наука о методах обеспечения конфиденциальности, целостности данных, аутентификации, шифрования. Криптографические алгоритмы, основанные на использовании открытого распределения ключей, позволили создать систему комплексного обеспечения безопасности информации в больших компьютерных сетях и информационных базах данных. Причиной тому явилась особенность криптосистем с открытыми ключами (построенных на основе асимметричных алгоритмов шифрования) использовать гораздо меньшее количество ключей для одного и того же количества пользователей, нежели того требует криптосистема с открытыми ключами.

Существует немало готовых алгоритмов шифрования, имеющих высокую криптостойкость, шифровщику остается только создать свой уникальный ключ для придания информации необходимых криптографических качеств. Ключ используется как для шифрования, так и в процессе расшифрования.

Квантовое распределение ключей (QKD, КРК) — это процедура распределения ключей с использованием квантовых каналов связи и специальных протоколов [6].

Квантовый канал выполняет пересылку информации для согласования общего ключа по сегменту оптической линии связи. При этом способ передачи ключевой информации использует принцип квантового измерения, при котором состояние носителя информации — фотона — при измерении неизбежно изменяется. Это связано с принципом неопределенности, согласно которому нельзя измерить квантовое состояние, не нарушив его.

QKD включает отправку зашифрованных данных в виде классических битов по сети, а ключи для расшифровки информации кодируются и передаются в квантовом состоянии с использованием кубитов. Если кубиты при передаче будут нарушены, обе стороны обмена данными будут об этом осведомлены и будут иметь возможность не пересылать данные по незащищенному каналу.

Самая длинная QKD-сеть находится в Китае, который может похвастаться наземным сообщением длиной 2032 км между Пекином и Шанхаем [7]. Банки и другие финансовые компании используют её для передачи данных. В США в 2018 году стартап под названием Quantum Xchange заключил сделку , предоставляющую ему доступ к оптоволоконному кабелю протяженностью 805 километров, проложенному вдоль восточного побережья, для создания сети QKD. Первый этап строительства свяжет Манхэттен с Нью-Джерси, где у многих банков есть большие центры обработки данных. QKD для шифрования в том числе, например, использовали в 2007 году для защиты результатов выборов в Швейцарии.

Хотя QKD-сети относительно безопасны, они становятся еще безопаснее, если могут рассчитывать на применение квантовых повторителей.

Квантовый повторитель

Материалы в кабелях могут поглощать фотоны, а это означает, что они обычно могут перемещаться не более чем на осязаемые величины – десятки и

сотни километров, соответственно на это же расстояние передавая информацию. В классической сети повторители в различных точках кабеля используются для усиления сигнала, чтобы компенсировать это ослабление.

Например, такие «доверенные узлы» расположены в сети Пекин-Шанхай, их 32. В этих узлах квантовые ключи расшифровываются в биты, а затем повторно шифруются в новом квантовом состоянии для их перехода к следующему узлу. Однако, хакер, нарушивший безопасность узлов, может незаметно скопировать биты и, таким образом, получить ключ, как и компания или правительство, управляющие узлами.

В идеальном случае необходимы квантовые повторители или промежуточные станции с квантовыми процессорами, которые позволят ключам шифрования оставаться в квантовой форме по мере их отправки на большие расстояния. Исследователи продемонстрировали, что в принципе можно построить такие ретрансляторы, но им пока не удалось создать работающий прототип [8].

Есть еще одна проблема с QKD. Базовые данные по-прежнему передаются в виде зашифрованных битов по обычным сетям. Это означает, что хакер, взломавший защиту сети, может незаметно скопировать биты, а затем использовать мощные компьютеры, чтобы попытаться взломать ключ, используемый для их шифрования.

Самые мощные алгоритмы шифрования довольно надежны, но риск достаточно велик, чтобы побудить некоторых исследователей работать над альтернативным подходом, известным как квантовая телепортация.

Квантовая телепортация

Квантовая телепортация означает возможность мгновенной передачи состояния с одной частицы на другую независимо от того, как далеко друг от друга они находятся. Обязательным условием для проведения квантовой телепортации является наличие набора одинаковых атомов в точке отправления состояния и в точки получения состояния. То есть квантовая телепортация не имеет ничего общего с материальным перемещением объекта.

Эйнштейн открыл это явление в 1935 году в соавторстве с физиками Борисом Подольским и Натаном Розеном. Ученые доказали, что состояние двух частиц А и Б, однажды провзаимодейстовавших и разлетевшихся в разные направления после соударения, зависит друг от друга на любом расстоянии и эта зависимость проявляется мгновенно. Например, у нас есть две частицы А и Б, они однажды были во взаимодействии, и мы знаем, что сумма их спинов (моментов импульса) всегда равна нулю, при этом спин частицы А направлен вверх, а спин Б — вниз. Как бы далеко мы не разнесли эти частицы, при изменении спина частицы А вниз, спин частицы Б будет мгновенно направляться вверх.

У квантовой телепортации есть колоссальный технологический потенциал, и лежит он, в основном, в области связи и вычислительной техники. По словам руководителя научной группы «Квантовые информационные технологии» в Российском квантовом центре Алексея Федорова, одно из направлений, которым сегодня занимаются физики — увеличение расстояния для квантовых коммуникаций [9]. Это необходимо для создания криптографических ключей, которые используются для интернет-соединения и в мобильных банках.

Квантовая телепортация работает, создавая пары запутанных фотонов, а затем отправляя один из каждой пары отправителю данных, а другой - получателю.

Исследователи в США, Китае и Европе стремятся создать сети телепортации, способные распространять запутанные фотоны. Но масштабирование их будет серьезной научной и инженерной задачей. Многие препятствия включают в себя поиск надежных способов производства большого количества связанных фотонов по запросу и поддержание их запутанности на очень больших расстояниях — то, что квантовые ретрансляторы упростили бы.

Тем не менее, эти проблемы не помешали исследователям мечтать о будущем квантового интернета.

Квантовый интернет

Китай находится в авангарде движения к квантовому интернету. Несколько лет назад компания запустила специальный спутник квантовой связи под названием Micius, позже спутник помог провести первую в мире межконтинентальную видеоконференцию с защитой QKD между Пекином и Веной. Китай планирует запустить больше квантовых спутников, а несколько городов страны разрабатывают планы муниципальных сетей QKD.

Некоторые исследователи предупреждают, что даже полностью квантовый интернет может в конечном итоге стать уязвимым для новых атак, которые основаны на квантовых технологиях. Но столкнувшись с хакерским натиском, от которого страдает современный Интернет, предприятия, правительства и военные тем не менее будут продолжать изучать перспективу более безопасной квантовой альтернативы текущим методам шифрования.

СПИСОК ЛИТЕРАТУРЫ

1. Иванова А.П. УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ: БОЛЬШАЯ ПРОБЛЕМА В ЦИФРОВУЮ ЭПОХУ // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право: Реферативный журнал. 2020. №4.
2. Швыряев Павел Сергеевич УТЕЧКИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ: ГЛАВНЫЙ ВРАГ ВНУТРИ // Государственное управление. Электронный вестник. 2022. №91.
3. Egorova, O.V., Barbashov, N.N., Abdullina, L.R., Kiselev, R.M. (2022). Non-circular Gears: Innovative Manufacturing Technologies. In: Quaglia, G., Gasparetto, A., Petuya, V., Carbone, G. (eds) Proceedings of I4SDG Workshop 2021. I4SDG 2021. Mechanisms and Machine Science, vol 108. Springer, Cham. https://doi.org/10.1007/978-3-030-87383-7_62
4. Коломыцев Александр Сергеевич, Вердиев Орхан Ровшанович КАК ПРЕДОТВРАТИТЬ УТЕЧКУ ПЕРСОНАЛЬНЫХ ДАННЫХ // StudNet. 2022. №7.
5. Barbashov N.N., Samoilova M.V., Abdullina L.R., Selection of rational algorithms for controlling high-precision details, Journal of Physics: Conference

Series, Volume 1889, Intrumentation Technologies and Environmental Engineering, 2021

6. Козлов Роман Николаевич Квантовая криптография. Идея квантового повторителя // Евразийский научный журнал. 2015. №12. URL: https://cyberleninka.ru/article/n/kvantovaya-kriptografiya-ideya-kvantovogo-povtoritelya (дата обращения: 29.12.2022).
7. Гончаренко Д.К., Кулиш О.А., Ивахненко А.В., Сидько Н.В. Разработка способов увеличения длины волоконно-оптического канала связи квантово-криптографической системы // МНИЖ. 2019. №6-1 (84).
8. Ващинников, А. Д. Проблемы нарушения авторских прав и кибербесопазности / А. Д. Ващинников, А. А. Калистратова // Национальная безопасность России: актуальные аспекты : сборник избранных статей Всероссийской научно-практической конференции, Санкт-Петербург, 30 мая 2020 года. – Санкт-Петербург: ГНИИ «Нацразвитие», 2020. – С. 28-31. – EDN NENCVC.
9. Данеев О.В. О ПРОБЛЕМЕ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ: СОСТОЯНИЕ И ПЕРСПЕКТИВЫ // Хроноэкономика. 2020. №2 (23).

BIBLIOGRAPHY

1. Ivanova A.P. LEAKAGE OF PERSONAL DATA: A BIG PROBLEM IN THE DIGITAL AGE // Social and Humanitarian Sciences. Domestic and foreign literature. Ser. 4, State and Law: Abstract Journal. 2020. №4.
2. Shvyryaev Pavel Sergeevich LEAKAGE OF CONFIDENTIAL DATA: THE MAIN ENEMY IS INSIDE // State Administration. Electronic Bulletin. 2022. No. 91.
3. Egorova, O.V., Barbashov, N.N., Abdullina, L.R., Kiselev, R.M. (2022). Non-circular Gears: Innovative Manufacturing Technologies. In: Quaglia, G., Gasparetto, A., Petuya, V., Carbone, G. (eds) Proceedings of I4SDG Workshop 2021. I4SDG 2021. Mechanisms and Machine Science, vol 108. Springer, Cham. https://doi.org/10.1007/978-3-030-87383-7_62

4. Kolomytsev Alexander Sergeevich, Verdiev Orkhan Rovshanovich HOW TO PREVENT PERSONAL DATA LEAKAGE // StudNet. 2022. No. 7.
5. Barbashov N.N., Samoilova M.V., Abdullina L.R., Selection of rational algorithms for controlling high-precision details, Journal of Physics: Conference Series, Volume 1889, Instrumentation Technologies and Environmental Engineering, 2021
6. Kozlov Roman Nikolaevich Quantum cryptography. The idea of a quantum repeater // Eurasian scientific journal. 2015. No. 12. URL: https://cyberleninka.ru/article/n/kvantovaya-kriptografiya-ideya-kvantovogo-povtoritelya (date of access: 12/29/2022).
7. Goncharenko D.K., Kulish O.A., Ivakhnenko A.V., Sidko N.V. Development of ways to increase the length of the fiber-optic communication channel of a quantum-cryptographic system // MNIZH. 2019. No. 6-1 (84).
8. Vashchinnikov, A. D. Problems of copyright infringement and cybersecurity / A. D. Vashchinnikov, A. A. Kalistratova // National security of Russia: topical aspects: collection of selected articles of the All-Russian Scientific and Practical Conference, St. Petersburg, May 30 2020. - St. Petersburg: GNII "National Development", 2020. - S. 28-31. – EDN NENCVC.
9. Daneev O.V. ON THE PROBLEM OF QUANTUM KEY DISTRIBUTION: STATUS AND PROSPECTS // Chronoeconomics. 2020. No. 2 (23).

Для цитирования: Княжев Ф.Р. Современные квантовые технологии для безопасного обмена данными// Научный сетевой журнал «Столыпинский вестник» №1/2023.