УДК 004.056.53

УЯЗВИМОСТИ РЕАЛИЗАЦИЙ СИСТЕМ КВАНТОВОЙ КРИПТОГРАФИИ

Караммаев М.М., Топорков С.Е., Короченцев Д.А., Смирнов И.А., Черкесова Л.В.
ГОУ ВПО «Донской государственный технический университет», Ростов-на-Дону, e-mail: chia2002@inbox.ru

Авторами рассмотрены уязвимости систем квантовой криптографии и квантового распределения ключей. Несмотря на надёжность самой квантовой линии связи, направлением успешной атаки злоумышленника становится программное обеспечение, осуществляющее передачу данных, или уязвимости программно–аппаратной реализации систем квантового распределения ключей. Для отечественного применения квантовых технологий возможно использование российских сертифицированных систем шифрования («Кузнечик», ГОСТ 34.12–2015, или «Магма», ГОСТ 28147–89), что способствует развитию государственной политики импортозамещения. Описаны разновидности когерентных и некогерентных кибератак, основанных на перехвате и переотправке фотонов, на перепутывании квантовых проб и др. Рассмотрена атака ослепления однофотонного детектора получателя и возможная защита от неё, связанная с установкой перед детектором источника единичных фотонов, срабатывающего в случайные моменты времени. Проанализирована атака разделения фотонов и защита от неё, связанная с использованием идеальных источников фотонов или с модификацией квантового протокола BB84. Изучена возможность хакера заменить квантовый канал с потерями – на канал без потерь, что позволит злоумышленнику получить информацию о ключе, успешно считывая все передаваемые данные и не внося ошибок. На практике следует применять только квантовые каналы с высоким коэффициентом передачи, что позволит избежать успешного применения такой атаки. Исследована атака типа «квантовый троян», заключающаяся в отправке получателю яркого светового луча и дальнейшем анализе возвращённого луча. Данная атака способна восстановить ключ, и для защиты от неё следует установить монитор–детектор, который случайным образом перенаправляет часть входящих сигналов на детектор получателя. Эффективным решением является *постоянное наблюдение за лавинными светодиодами* получателя в реальном времени. Несмотря на кажущееся совершенство, на практике имеется множество уязвимостей, дыр и брешей в структуре самого канала связи, что не гарантирует защиту передаваемых данных от атак злоумышленников.

Ключевые слова: квантовая криптография, квантовые линии связи, импортозамещение, когерентные и некогерентные кибератаки, атака с ослеплением детектора, атака разделения фотонов, атака замены квантового канала

VULNERABILITIES OF QUANTUM CRYPTOGRAPHY SYSTEMS IMPLEMENTATIONS

Karammaev M.M., Toporkov S.E., Korochentsev D.A., Smirnov I.A., Cherckesova L.V.
Don State Technical University, Rostov-on-Don, e-mail: chia2002@inbox.ru

Authors consider vulnerabilities of quantum cryptography and quantum key distribution systems. Despite of reliability on quantum communication line as such, direction of successful hacker's attack is transmitting data software, or vulnerabilities in hardware–and–software implementation of quantum key distribution systems. For domestic quantum technologies application, it is possible to use Russian certified encryption systems («Kuznechik», GOST 34.12–2015, or «Magma», GOST 28147–89), which contributes to import substitution state policy development. Different types of coherent and incoherent cyberattacks, based on photons interception and re–transmission, on quantum samples mixing–up are described. Blinding attack of single–photon receiver detector and possible protection against it, associated with installation of single photon source in front of detector, which operating at random time moments, was considered. Attack of photon separation and protection against it, associated with using of ideal photon sources or with quantum protocol BB84 modification, was analyzed. Possibility of hacker to replace quantum channel with losses – to channel without losses, which will allow attacker to get information about key, to read successfully all transmitted data, without making errors. In practice, only quantum channels with high transmission coefficient should be used, which will avoid successful application of such attack. Attack of «quantum Trojan» type, which consists in sending of bright light ray to recipient and further analyzing returned ray, is investigated. This attack can restore the key, and to protect against it, installing detector–monitor that randomly redirects some of incoming signals to receiver's detector is necessary. Effective solution is constant monitoring avalanche LEDs of receiver in real time. Despite apparent perfection, in practice there are many vulnerabilities, gaps and security holes in structure of communication channel, which does not guarantee the protection of transmitted data from hackers attacks.

Keywords: quantum cryptography, quantum communication lines, import substitution, coherent and incoherent cyber-attacks, detector blinding attack, photon separation attack, attack of quantum channel replacement

Системы квантовой криптографии до недавнего времени считались неуязвимыми, так как в них, для обеспечения секретности информации, используются не традиционные математические методы, а делается упор на передачу информации с помощью объектов квантовой механики. В действительности квантовые линии связи могут защитить, к примеру, от атак типа «человек посередине» [1]. Однако, несмотря на достаточную надёжность самой квантовой линии связи, направлением успешной ата-

ки злоумышленников может оказаться программное обеспечение, осуществляющее передачу информации, либо прочие уязвимости конкретных программно–аппаратных реализаций систем квантового распределения ключей.

Как и в классических системах распределения ключей, для осуществления передачи информации целесообразно использовать синхронный шифр, например AES–128–GCM или CHACHA20–POLY1305. Для отечественного применения новых квантовых технологий, с использованием синхронных шифров, не исключаются возможность использования российских сертифицированных систем шифрования, таких как «Кузнечик» (ГОСТ 34.12–2015) или «Магма» (ГОСТ 28147–89), что не только не противоречит, но и способствует развитию внутренней государственной политики импортозамещения [2].

С чем связано и в чем кроется причина применения синхронных шифров в квантовом шифровании? Причиной этому является довольно низкая скорость обмена данными при использовании асинхронных шифров либо низкая скорость функционирования квантовой системы распределения ключей. Допустим, что злоумышленник подключается к квантовой линии связи (рис. 1) в момент передачи фотона и пытается измерить его состояние.

Частица мгновенно изменяет своё состояние случайным образом – это следствие *эффекта наблюдателя* [3]. Отправитель и получатель сразу узнают о попытке компрометации (несанкционированного доступа к информации) и начинают передачу данных заново. Так работает система квантовой связи в идеальных условиях. Но на практике не существует технически идеальных систем, поэтому передаваемая по достаточно надёжной квантовой линии связи информация всё же может быть уязвима к целому ряду кибератак.

Для решения задач информационной безопасности и защиты данных нужны серьёзные исследования существующих сегодня уязвимостей программно–аппаратных реализаций систем квантовой криптографии, изучение разновидностей возможных кибератак, направленных на перехват (несанкционированный доступ) передаваемой информации, и разработка методов их предотвращения и отражения с целью защиты конфиденциальности информации от действий злоумышленников различного рода. Такую цель исследований авторы и поставили перед собой.

Материалы и методы исследования

Рассмотрим виды когерентных и некогерентных кибератак.

Когерентность – это совместное и скоординированное развитие колебательных или волновых процессов во времени, что становится очевидным при их сложении. Колебания можно назвать когерентными только в том случае, когда разность их фаз во времени остаётся неизменной. При суммировании колебаний этот факт и обусловливает амплитуду итогового сложения колебаний. Если разность фаз колебаний во времени изменяется, то это означает, что колебательные процессы некогерентны и несогласованы во времени [4].

Рис. 1. Схема передачи данных с использованием системы квантового распределения ключей

Простейшей атакой может являться *когерентная атака*, основанная на перехвате и переотправке фотонов. Злоумышленник считывает данные в случайном базисе и отправляет их далее по линии связи. Если базис угадан, то злоумышленник успешно перехватывает бит информации (таблица). Квантовый протокол BB84 неуязвим к данному виду атаки при достаточно большом размере ключа, поскольку вероятность успешного применения такой атаки равна $P = \frac{1}{2^n}$, где n – количество бит ключа.

В случае если отправитель и получатель публично сравнивают некоторые биты (эти биты уже не являются секретом и не могут быть использованы в ключе), то при сравнении n битов вероятность обнаружения злоумышленника равна

$$P = 1 - \left(\frac{3}{4}\right)^n.$$

При отправке 384 бит информации, из которых только 128 случайных бит являются ключом, вероятность обнаружения злоумышленника бесконечно близка к единице.

Злоумышленник – хакер имеет возможность смешать образец каждого измерения со всем набором (рядом) переданных отдельных фотонов каким–то единым (унитарным) способом [5].

Крайний случай подобной атаки заключается в том, что хакер может перепутать свои образцы (пробы) с полным набором фотонов, последовательно передаваемых отправителем. Затем хакер сохраняет свои образцы (большой пробы) до завершения всех обменов сообщениями, происходящих между отправителем и получателем по квантовой линии связи. После этого он выполняет общее измерение состояния образцов пробы любым методом по своему желанию [5].

Составной частью когерентных атак можно назвать *коллективные атаки.* При их проведении каждый фотон, полученный с передатчика, по отдельности перепутывается с индивидуальной пробой квантового образца, точно так же, как это происходит при некогерентных атаках. Разница состоит в том, что такое измерение будет выполняться не для каждой пробы отдельно, а сразу и одновременно на всех квантовых пробах, которые рассматриваются как целостная и неразделимая квантовая система. Результат коллективной атаки – определение базиса отправителя.

В случае *некогерентных атак* хакеру приходится отдельно обрабатывать каждый приходящий из передатчика фотон. Самым простым способом такой атаки является уже рассмотренная ранее *атака перехвата и пересылки фотона*. Так как при этой атаке фотоны дальше по линии связи не пропускаются, а пересылаются уже новые фотоны, то эта стратегия называется *непрозрачной* [6].

Некогерентные атаки включают также *атаку перепутывания квантовых проб с* фотонами, пересылаемыми по каналу квантовой связи. В этом случае каждый фотон, независимо от других, должен быть перепутан с отдельным образцом (пробой). Обработанный фотон посылается на приёмник. После этого хакер может сохранять свои пробы в квантовой памяти и, по отдельности, измерять их состояния после того, как абоненты квантового канала связи завершат свой открытый обмен сообщениями. Прослушивая открытые сообщения, злоумышленник сможет получить базисы, используемые отправителем, а, значит, найти свой способ измерений для получения недостающих данных об использованном ключе [5; 7].

Этот вид атаки интерпретируется как *полупрозрачная атака*, потому что состояния фотонов, с которыми хакер перепутывает свои образцы (пробы), меняются. Уровень ошибок, вносимых хакером, может быть снижен за счёт уменьшения объёма данных о ключе, которые он получает [7].

Пример попытки применения атаки перехвата и переотправки фотонов

Случайный бит отправителя	0	1	0	0
Случайный базис отправителя	+	×	×	×
Поляризация фотона отправителя	↑	↘	↗	↗
Случайный базис злоумышленника	+	+	+	×
Поляризация фотона злоумышленника	↑	→	→	↗
Случайный базис получателя	+	×	×	×
Поляризация фотона получателя	↑	↗	↗	↗
Ошибка в ключе	нет	да	нет	нет
Утечка ключа	да	нет	нет	да

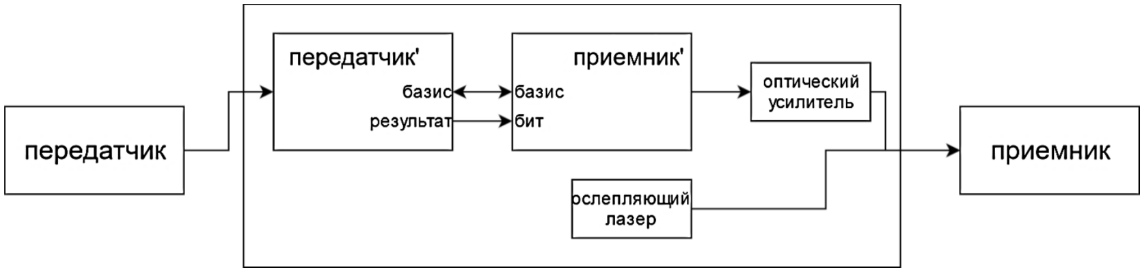

Рис. 2. Схема применения атаки с ослеплением детектора

Атаки на детектор. Рассмотрим *атаку с ослеплением однофотонного детектора получателя* [8], разработанную исследовательской группой В. Макарова в Норвежском университете естественных и технических наук. Злоумышленник считывает информацию, отправляемую передатчиком, и отправляет её дальше по каналу связи, но использует очень мощный импульс (рис. 2). Несовершенный детектор воспринимает такой импульс как обычный сигнал, в результате чего теряется эффект наблюдателя. При этом злоумышленник остается незамеченным, и получает возможность считывать всю информацию, передаваемую по квантовому каналу связи.

Защититься от такой уязвимости можно, установив перед детекторами источник единичных фотонов [9], срабатывающий в случайные моменты времени. Это позволит убедиться, что детектор не считывает световые сигналы в обычном режиме, а работает в квантовом режиме.

Еще один пример успешной атаки – *атака разделения фотонов*. В протоколе BB84 для отправки квантового состояния используются лазерные импульсы. В большинстве реализаций за каждый импульс передается очень малое количество фотонов (в основном от 0 до 2). Они распределены по импульсам в соответствии с распределением Пуассона [10].

За импульс передается ноль фотонов, иногда один, реже два или больше (рис. 3). В случае когда за один импульс передается больше одного фотона, злоумышленник может их разделить, а отведенный фотон будет перепутан с пробой [11].

Оставшаяся неизменная часть данных будет переслана получателю, а хакер–перехватчик сможет узнать правильное значение пересылаемого бита, не внося ошибок в отфильтрованный ключ. Это позволяет хакеру оставаться незамеченным и скрытным, считывая данные [9].

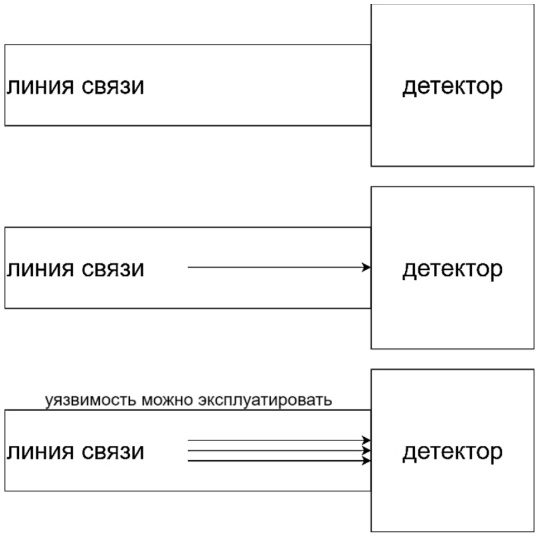

Рис. 3. Условия применения атаки разделения фотонов

Существует несколько решений этой проблемы. Лучшим решением было бы использовать идеальные источники фотонов. Они находятся в активной разработке и уже давно успешно применяются [12]. Другое решение – модификация протокола BB84 [13].

Например, в протоколе SARG04 отправитель не анонсирует базис своего бита [14]. В результате злоумышленнику потребуется хранить гораздо больше копий измерений для того, чтобы определить состояние фотонов, что и не позволит ему успешно реализовать свою атаку.

На практике все еще используют слабые когерентные импульсы, излучаемые лазерными светодиодами – *многофотонные источники*. Поскольку большая часть импульсов несет всего один фотон, злоумышленник должен пропускать их, чтобы остаться незамеченным. При малом количестве импульсов, с числом фотонов более одного, количество перехваченной информации очень

мало. Скорее всего, перехватчик будет вынужден обратиться к другой стратегии, например к блокированию импульсов только с одним фотоном. Такая стратегия может позволить злоумышленнику остаться незамеченным, восстановив всю информацию о ключе.

Замена квантового канала. Обсудим также вероятность того, что хакер может поменять квантовый канал, имеющий потери, используемый абонентом, на канал, потерь не имеющий. Такую замену канала с потерями на канал без потерь вполне может *не заметить* ни отправитель, ни получатель. Если ему это удастся, то тогда злоумышленник сможет задержать и заблокировать большинство импульсов (при условии, что исходный канал имел большой процент потерь) так, чтобы приёмник получил приблизительно ожидаемое число импульсов [15]. Так, хакер сможет получить всю информацию о ключе, успешно считывая все передаваемые данные и не внося никаких ошибок. Отсюда следует, что на практике следует применять только *квантовые каналы с высоким коэффициентом передачи* во избежание успешного применения такой атаки.

В институте Макса Планка была разработана *квантовая атака типа «квантовый Троян» (Троянский конь).* Она заключается в отправке достаточно яркого луча света получателю и анализе возвращенного луча [16]. Будучи направленной на протокол SARG04, данная атака восстанавливает ключ, считывая случайный базис получателя с вероятностью выше 90%. Протокол SARG04 более устойчив к атаке разделения фотонов, чем BB84 [10; 13], однако уязвим к атаке «Троянский конь», и требует установки монитора–детектора, который случайным образом перенаправляет некоторую часть входящих сигналов на детектор получателя [17].

Также эффективным решением может оказаться *постоянное наблюдение за лавинными светодиодами* получателя в реальном времени [18].

Результаты исследования и их обсуждение

В реальности не существует технически идеальных систем. Это относится и к квантовым системам связи. Поэтому передаваемая по квантовому каналу информация, несомненно, может быть уязвима к целому ряду различных квантовых атак: когерентным и некогерентным, атакам на детектор, атакам разделения фотонов и др. На данный момент времени известно около 20 атак на квантовые линии связи. Можно утверждать, что со временем и с расширением использования во всём мире квантовых линий связи (квантового Интернета) количество разновидностей потенциальных квантовых атак будет только возрастать.

В процессе формирования системы и комплекса документов сертификации по квантовой криптографии возникает проблема, связанная с тем, что теоретически квантовые системы связи являются надёжными и принципиально невзламываемыми, но на практике – далеко не идеальны. Они очень сложны, а квантовый протокол можно уместить на двух страницах текста. На практике, чтобы провести оптическую обработку сигнала, в квантовой системе связи имеются 20–30 сложных электрооптических компонентов, имеется обилие программного кода, тысячи электронных компонентов, огромное количество алгоритмов синхронизации, которые в *описании протокола вообще отсутствуют,* и многое другое. Однако оптические компоненты имеют многие несовершенства и неидеальности, а также отклонения от того, каким образом квантовый протокол предписывает им работать. Системы делают люди – инженеры, которые должны выполнить план и всё сдать в срок. Это порождает значительное число уязвимостей, брешей и дыр в безопасности; различий между идеальным проектом разработчика и небезупречной, далекой от идеала его практической реализацией.

Заключение

Последние разработки и новшества в области квантовой криптографии, несмотря на своё кажущееся совершенство, имеют достаточно много уязвимостей, дыр и брешей в своей структуре, и вовсе не могут гарантировать на 100% защиту передаваемой информации от атак злоумышленников различных категорий. Всё сказанное выше и является питательной средой для осуществления квантового хакинга.

Список литературы

1. Huang D., Chen Z., Guo Y., Lee M. Quantum Secure Direct Communication Based on Chaos with Authentication. Journal of the Physical Society of Japan. 2007. Vol. 76. No. 12. P. 124001.

2. TLS (Channel SSP) changes in Windows 10 and Windows Server // Microsoft. Docs. 2018. [Electronic resource]. URL: https://docs.microsoft.com/en-us/windows-server/security/tls/tls-schannel-ssp-changes-in-windows-10-and-windows-server (date of access: 09.05.2020).

3. Квантовый троян: «абсолютно защищённая» связь оказалась дырявой // РИА Новости. 2018. [Электронный ресурс]. URL: https://ria.ru/20181122/1533223834.html?utm_source=news.mail.ru&utm_medium=region_informer&utm_campaign=rian_partners (дата обращения: 09.05.2020).

4. Что такое квантовая когерентность? Физик Сергей Филиппов о квантовой когерентности и её практической значимости // Постнаука. 2019. [Электронный ресурс]. URL: https://postnauka.ru/faq/92455 (дата обращения: 09.05.2020).

5. Василиу Е.В. Стойкость квантовых протоколов распределения ключей типа «приготовление–измерение» // Computer Sciences and Telecommunications. 2007. № 2 (13). С. 52–64.

6. Кузнецова А.В. Стратегии атак на квантовые протоколы защиты информации // Цифровые технологии. 2013. № 14. С. 145–149.

7. Василиу Е.В., Мамедов Р.С. Анализ стойкости к некогерентным атакам квантовых протоколов распределения ключей типа «приготовление–измерение» с кудитами // Современные информационные технологии. Информационная безопасность. [Электронный ресурс]. URL: http://www.rusnauka.com/29_NNM_2008/Informatica/35980. doc.htm (дата обращения: 09.05.2020).

8. Lydersen L., Wiechers C., Wittmann C., Elser D., Scaar J., Makarov V. Hacking Commercial Quantum Cryptography Systems by Tailored Bright Illumination. Nature Photonics. 2010. № 4 (10). P. 686–689.

9. Действительно ли надежна квантовая криптография? // Блог компании Toshiba. 2019. [Электронный ресурс]. URL: https://habr.com/ru/company/toshibarus/blog/444502/ (дата обращения: 09.05.2020).

10. Bennett C., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. Theoretical Computer Science. 2014. Vol. 560 (Part 1). P. 7–11.

11. Brassard G., Lütkenhaus N., Mor T., Sanders B.C. Security Aspects of Practical Quantum Cryptography. EUROCRYPT 2000. Advances in Cryptology. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2000. Vol. 1807. P. 289–299.

12. Intallura P.M., Ward M.B., Karimov O.Z., Yuan Z.L., See P., Shields A.J. Quantum Key Distribution Using a Triggered Quantum Dot Source Emitting near 1.3 μm. Applied Physics Letters. 2007. Vol. 91(16). P. 161103.

13. Череданова Е.М., Мамченко Е.А., Марчук А.М., Речкунов А.А. Математическое моделирование квантового распределения ключа протокола BB84 // Политехнический молодёжный журнал. 2018. № 5. [Электронный ресурс]. URL: http://ptsj.ru/articles/319/319.pdf (дата обращения: 09.05.2020).

14. Scanari V., Acin A., Ribordi G., Gisin N. Quantum Cryptography protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulses Implementations. Physical Review Letters. 2004. (Feb). Vol. 92 № 5. Art. 057901.

15. Niederberger A., Scarani V., Gisin N. Photon–number–splitting Versus Cloning Attacks in Practical Implementations of the Bennett–Brassard 1984 Protocol for Quantum Cryptography. Physical Review A. 2005. Vol. 71. Art. 042316.

16. Jain N., Anisimova E., Khan I., Makarov V., Marquardt C., Leuchs G. Trojan–Horse Attacks Threaten the Security of Practical Quantum Cryptography. New Journal of Physics. 2014. Vol. 16 (12), Art. 123030. P. 1–22.

17. Da Silva T.F., Temporao G.P. Von der Weid J.P., Xavier G.B. Real–Time Monitoring of Single–Photon Detectors against Eavesdropping in Quantum Key Distribution Systems. Optics Express. 2017. Vol. 20. № 17. P. 18911–18924.

18. Все важные секреты перестанут быть секретами в будущем // KNEWS. 2019. [Электронный ресурс]. URL: https://knews.kg/2019/08/20/vse-vazhnye-sekrety-perestanut-byt-sekretami-v-budushhem-o-kvantovoj-kriptografii-dyrah-v-sistemah-i-atakah-na-sputniki/ (дата обращения: 09.05.2020).