УДК 004.056.5 DOI: 10.47813/rosnio.2022.3.142-147 EDN: STOIJD

Протокол распределения квантовых ключей BB84

В.А. Аксельрод[1,*], В.С. Аверьянов[2], И.Н. Карцан[1,2,3,4]

[1]ФГАОУ ВО «Севастопольский государственный университет»,
ул. Университетская, 33, Севастополь, 299053, Россия
[2]Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, просп. им. газ. «Красноярский рабочий», д. 31,
Красноярск, 660037, Россия
[3]Морской гидрофизический институт РАН, ул. Капитанская, д.2,
Севастополь, 299011, Россия
[4]ФГБНУ «Аналитический центр», ул. Талалихина, 33/4,
Москва, 109316, Россия

*E-mail: vadimlewanow@yandex.ru

Аннотация. Представлены основные объекты использования перспективных квантовых сетей передачи информации в телекоммуникационной среде. Рассмотрено развитие нового направления защищенного способа передачи информации. Сформулированы основные задачи при использовании квантовых сетей в образовательной среде при подготовке специалистов по защите информации.

Ключевые слова: квантовая сеть, защита информации, передача информации, образовательная среда

BB84 quantum key distribution protocol

V.A. Axelrod[1,*], V.S. Averyanov[2], I.N. Kartsan[1,2,3,4]

[1]Sevastopol State University, University Str. 33, Sevastopol, 299053, Russia
[2]Reshetnev Siberian State University of Science and Technology, 31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660037, Russia
[3]Marine Hydrophysical Institute, Russian Academy of Sciences», 2, Kapitanskaya Str., Sevastopol, 299011, Russia
[4]"Analytical Center", Talalikhina Str., 33, Building 4, Moscow, 109316, Russia

*E-mail: vadimlewanow@yandex.ru

Abstract. The main objects of the use of promising quantum information transmission networks in the telecommunications environment are presented. The development of a new direction of the protected method of information transmission is considered. The main tasks in the use ofquantum networks in the educational environment in the training of information security specialists are formulated.

Keywords: device quantum network, information protection, information transfer, educational environment

1. Введение

Способы передачи информации прошли длинный путь, от гонцов и вестников, минуя голубиную почту, от первых проводных сетей и радиопередатчиков до оптоволоконной и, интересующей нас сегодня, квантовой связи.

Информация, которая передается от объекта до объекта, является одним из весьма уязвимых мест, где организуется канал утечки важной информации. Поэтому основная задача стоит в организации защиты информации в момент ее передачи. Одним из перспективных направлении, на сегодняшний день является квантовая технология передачи сообщений. Квантовая сеть — это система передачи данных, основанная и работающая по законам квантовой механики. Носителем информации является кубит — это поляризованный фотон, который транслируется по каналу оптической связи. Да, от оптических каналов нам (пока что) не уйти, но есть особенности при передаче.

Стремительное развитие науки и техники, коммерческая реализация идей и принципов, основанных на постулатах квантовой механики, физики и оптики в области квантовых вычислений, за последние годы позволило существенно нарастить объем систем на базе симметричного шифрования с квантовым распределением ключа (КРК) безопасности. Преимущественно технологии КРК основаны на взаимодействии с множеством оконечных устройств в виде цифровых абонентов, реализации концепции передачи информации в виде релятивистских частиц – фотонов, свойства которых невозможно подделать без обнаружения в квантовом канале связи. О данных обстоятельствах свидетельствует теорема о запрете клонирования [1, 2], сформулированная в 1982 году Wootters W.K. и Zurek W.H.

2. Основная часть

Квантовые сети подчиняются законам квантовой механики и, следовательно, ей присущи такие явления как: невозможность клонирования (теорема о запрете клонирования), квантовое измерение, запутывание и телепортация. Все эти факты накладывают некоторые ограничения на проектирование квантовых сетей. Ввиду всех этих закономерностей, становится невозможным использование классических функций, таких как механизмы контроля ошибок (ARQ) или overheadcontrol (кэширование).

Также как и в обычных сетях, информация не передается в «открытом» виде. Для распространения по сети используется:

- квантовая криптография;

- протоколы передачи.

В классической криптографии используются методы, которые опираются исключительно на математические методы. Однако, в квантовой криптографии обеспечение конфиденциальности передаваемой информации основывается на фундаментальных законах квантовой механики.

Существуют основные классические протоколы эффективной рассылки квантовых кодирующих последовательностей кубитов в оптических линиях связи: BB84, B92, DPS, COW, E91, Lo05, протокол на основе OT (неявная передача) и BC (битовая схема обязательства). Протокол передачи данных BB84 для квантовых систем связи, является первым, реализованным на практике квантовым протоколом установления соединения двух удаленных абонентов по оптической линии [3-5].

Одной из особенностей и в тоже время трудностей квантовой криптографии является то, что необходимо доставить однофотонное сообщение (когерентное квантовое состояние фотона), которое достигается за счет ослабленных лазерных импульсов. Подобное действие позволяет обеспечить защиту от атак называемых «человек посередине». Это основывается на законе о запрете клонирования квантового состояния фотона и делает невозможным «вклинивание» в линию передачи информации. Но в некоторых случаях встречается нарушение в подобных когерентных посылках и отправляется более одного фотона, что может привести к перехвату злоумышленником. Такие действия называются атаками с разделением по числу фотонов (Photon number splitting attack, PNS-атаки) [6]. Существуют протоколы, которые устойчивы к PNS-атакам, один из них SARG04. Если злоумышленник сможет блокировать все посылки, состоящие из одного, двух, трех фотонов, только в таком случае сообщение перестает быть секретным.

Для квантового распределения ключа используются различные протоколы. Простейший протокол BB84 был разработан еще в 1984 Черльзом Беннетом и Жилем Брассардом. Главными участниками в разборе данного алгоритма будут Алиса, которая является отправителем, и Боб, получатель. Работа алгоритма организована следующим образом [7]:

- Первичная квантовая передача. В ходе первого действия Алиса генерирует фотоны со случайной поляризацией (0, 45, 90 и 135°), (рисунок 1);

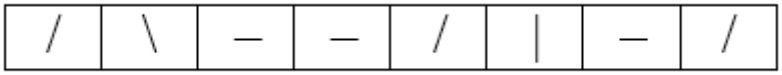

Рисунок 1. Фотоны, сгенерированные Алисой.

- Боб, после получения фотонов, применяет к каждому из них перпендикулярный (+) или вертикальный (×) способ изменения поляризации, при этом выбирая их случайным образом (рисунок 2);

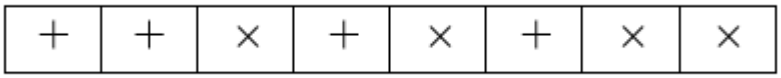

Рисунок 2. Выбранные способы поляризации.

- Исходя из способа поляризации, получаем изменения (рисунок 3);

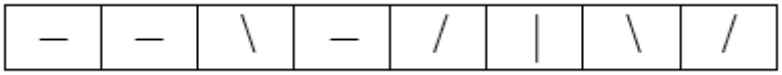

Рисунок 3. Результат изменений.

- Затем, он отправляет по открытому каналу выбранные для каждого фотона способы поляризации Алисе. Она в свою очередь сообщает Бобу, верно, выбранные виды изменений для каждого фотона и также отправляет по открытому каналу (рисунок 4);

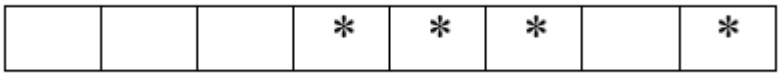

Рисунок 4. Правильные и неправильные виды изменений.

- После подтверждения со стороны Алисы, сведения о неверных изменения отбрасываются, а оставшиеся заменяются в биты: фотоны с горизонтальной или 45°-ной поляризацией заменяются на двоичный «0», а фотоны с вертикальной и 135°-ной поляризацией – на «1». Данная последовательность является итоговым результатом первого этапа (рисунок 5).

Рисунок 5. Полученная последовательность.

Оценка возможности перехвата информации. Что бы проверить есть ли подобная возможность, Алиса и Боб случайным образом раскрывают и сравнивают значения бит

по открытому каналу. Затем данные биты отбрасывают. В том случае, если обнаружен перехват, то запускается процедура заново, в ином – поляризация остается прежней.

3. Выводы

В заключении стоит отметить, что развитие технологий привело нас к использованию квантовой физики. В свою очередь, квантовая криптография является очень перспективной отраслью, ведь подобные направления, используемые там, позволяют нам перейти на новый уровень безопасности информации. По этим причинам создание современных и безопасных сетей связи является одной из приоритетных задач при выборе систем передачи данных государственных органов, крупных технологических компаний, финансовых структур, владельцев критической информационной инфраструктуры и граждан. Успешное взаимодействие государственных учреждений с бизнесом во многом зависит от сохранности полученных и обрабатываемых данных. Новые информационные технологии способствуют осуществлению активных, качественных преобразований в большинстве сфер РФ, многие из которых являются наукоемкими.

Благодарности

Работа выполнена в рамках государственного задания Минобрнауки России по теме «Разработка новых методов автономной навигации космических аппаратов в космическом пространстве» 121102600068-5.

Работа выполнена в рамках государственного задания по теме № 0555-2021-0005.

Список литературы

1. Bennett, C. Quantum cryptography: Public key distribution and coin tossing / C. Bennett, G. Brassard // Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. – Institute of Electrical and Electronics Engineers, New York, 1984. – P. 175-179.
2. Acin, A. Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks / A. Acin, N. Gisin, V. Scarani // Phys. Rev. A. – 2004. – № 69. – 012309.
3. Аверьянов, В. С. Гибридный квантово-классический подход для защиты наземных линий связи / В. С. Аверьянов, И. Н. Карцан // Южно-Сибирский научный вестник. – 2019. – Т. 4(28). – С. 264-269.

4. Агеева, Е. С. Защищенный протокол для передачи данных в спутниковой связи / Е. С. Агеева, И. Н. Карцан // Актуальные проблемы авиации и космонавтики. – 2015. – № 1(11). – С. 68-70.
5. Bennett, C. H. Quantum cryptography using any two no orthogonal states / C. H. Bennett // Phys. Rev. Lett. – 1992. – № 68(21). – P. 3121-3124.
6. Tamaki, K. Security of the Bennett 1992 quantum-key distribution against individual attack over a realistic channel / K. Tamaki, M. Koashi, N. Imoto // Phys. Rev. – A 67. – 032310.
7. Bennett, C. Experimental quantum cryptography / C. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin // J. Cryptology. – 1992. – № 5. – P. 328.