СЕКЦИЯ 2. ИННОВАЦИИ В ПРОМЫШЛЕННЫХ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ

УДК 004.056 DOI: 10.47813/rosnio.2022.3.72-75 EDN: KYGQMC

Безопасность ключевой последовательности по протоколу Чарльза Беннета

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

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

*E-mail: kartsan2003@mail.ru

Аннотация. Рассмотрен ряд вопросов возникающих при создании квантовых волоконно-оптических систем квантовое распределение ключей. Проведено исследование основных принципов работы протокола B92, отмечены отличительные особенности от BB84. В заключении приведен ряд недостатков, накладывающих ограничения при работе на длинных маршрутах.

Ключевые слова: безопасность, вектор, поляризация, протокол, B92, устройство

Key sequence security by Charles Bennett protocol

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

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

*E-mail: kartsan2003@mail.ru

Abstract. This paper proposes an efficient and novel technique for assessment of the direction of switched capacitor bank as well as estimating its distance from the monitoring location in real distribution systems. At first, the proposed. The work considered a number of issues arising in the creation of quantum fiber-optic systems of quantum key distribution. A study of the basic principles of the work of Protocol B92 was carried out, distinguishing features from BB84 were noted. In conclusion, there are a number of drawbacks that impose restrictions when working on long routes.

Keywords: safety, vector, polarization, protocol, B92, device

1. Введение

Идея использовать квантовые объекты для защиты информации от подделки и несанкционированного доступа впервые была высказана Стефаном Вейснером в 1970 г. Спустя 10 лет ученые Беннет и Брассард, которые были знакомы с работой Вейснера, предложили использовать квантовые объекты для передачи секретного ключа [1, 2]. В 1984 г. они опубликовали статью, в которой описывался протокол квантового распространения ключа BB84.

B92 один из протоколов квантового распределения ключей безопасности, основоположник Чарльз Генри Беннетт. Принцип его работы изложен в статье от 1992 года «Квантовая криптография с использованием любых двух неортогональных состояний» [3], протокол является упрощенной версией BB84, основан на принципах неопределенности распределения пары неортогональных квантовых состояний частиц [4, 5] между легитимными пользователями квантовых систем связи. Как и BB84, для B92 формирование кодовой последовательности осуществляется кодированием световых первочастиц – фотонов, поляризованных в двух базисах, соответствующих логическим «0» и «1» ($|\varphi_0\rangle$ и $|\varphi_1\rangle$), ($\langle\varphi_0|\varphi_1\rangle \neq 0$). Основное отличие от BB84 это два, вместо четырех состояний поляризации (рисунок 1).

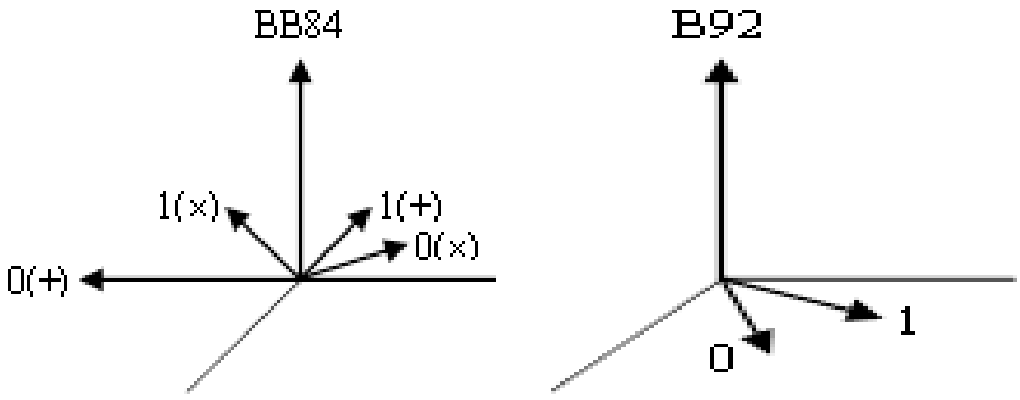

Рисунок 1. Отличительные особенности протокола BB84 (а) и B92 (б).

Условия многофотонности свойственны как для глауберовых, так и фоковских состояний квантовых частиц. Фотодетектирование и процедура измерений в таких случаях являются целочисленной функцией для всей последовательности, в отличии от однофотонных посылок.

2. Основная часть

Алгоритм протокола B92 [3] следующий: передающая сторона А случайным образом выбирает одно из неортогональных поляризованных состояний 0^0 либо 45^0, затем происходит процесс передачи кодированной последовательности по квантовому каналу связи. Сторона Б принимает однофотонные состояния через поляризационные фильтры, ориентированные под углами 90^0 и 135^0, происходит измерение. Здесь под процедурой измерения следует понимать однопараметрическое семейство проекционных операторов S_0, S_1 и S_n, действующих в гильбертово-проективном пространстве $\widehat{H}$, тогда:

$$\acute{S}_0 + \acute{S}_1 + \acute{S}_n = 1 \quad (1)$$

$$\acute{S}_0 = \widehat{H}(1 - \langle\varphi_0|\varphi_0\rangle) \quad (2)$$

$$\acute{S}_1 = \widehat{H}(1 - \langle\varphi_1|\varphi_1\rangle) \quad (3)$$

$$\acute{S}_n = 1 - (\langle\varphi_0|\varphi_0\rangle - \langle\varphi_1|\varphi_1\rangle) \quad (4)$$

$$\widehat{H} = \frac{1}{1+cos\xi} \quad (5)$$

$$cos\xi = \langle\varphi_0|1 - (\langle\varphi_0|\varphi_0\rangle - \langle\varphi_1|\varphi_1\rangle|\varphi_0\rangle = \langle\varphi_1|1 - (\langle\varphi_0|\varphi_0\rangle - \langle\varphi_1|\varphi_1\rangle|\varphi_1\rangle \quad (6)$$

Согласно (5, 6) результаты представляют собой различные - случайные исходы [6] измерений стороной Б, выраженные как: $\{0, 1, n\}$. При этом, если стороной А отправлено состояние вектора поляризации $|\varphi_1\rangle$, на приемной стороне возможны два результата измерений $\{0, n\}$, что соответствует (3) и никогда (4). Обратный вероятностный исход наблюдается при отправке состояния $|\varphi_0\rangle$, согласно выражению (2). Последующие действия аналогичны алгоритму BB84: сторона Б по классическому открытому каналу связи отправляет результаты измерений стороне А, исходы $\{n\}$ соответствуют логическому «0» и «1», в случае их несовпадения с начальной строкой отбраковываются. На заключительном этапе происходит формирование основного ключа безопасности. Результат кодированной последовательности положителен при отсутствии естественных флуктуаций и ошибок, вносимых злоумышленником. В случае, если уровень шума превышает пороговое значение, канал связи блокируется, алгоритм трансформируется в начальную позицию.

3. Выводы

К недостаткам протокола B92 по методу двух поляризационного кодирования как показывают исследования [3] следует отнести: затухания в оптической среде, где передача данных ограничена расстоянием в 20 км, техническими особенностями устройств фотодетектирования. Это позволяет злоумышленнику проводить подмену состояний измерения $\{0, 1\}$ и пересылать их стороне А с меньшими потерями в канале связи. Убеждение останется верным на длинных маршрутах, в случае коротких дистанций легитимные пользователи обнаружат стороннее «подслушивающее» устройство и прекратят обмен данными.

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. Аверьянов, В. С. Гибридный квантово-классический подход для защиты наземных линий связи / В. С. Аверьянов, И. Н. Карцан // Южно-Сибирский научный вестник. – 2019. – № 4(28). – С. 264-269.
2. 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.
3. Bennett, C. H. Quantum cryptography using any two no orthogonal states / C. H. Bennett // Phys. Rev. Lett. – 1992. – 68(21). – P. 3121-3124.
4. 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.
5. 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.
6. Bennett, C. Experimental quantum cryptography / C. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin // J. Cryptology. – 1992. – № 5. – P. 3-28.