УДК 20.53.19, 28.23.13 Научная статья

https://doi.org/10.32603/2071-8985-2023-16-9-77-82

Передача информации в квантовом канале связи

Д. Е. Воробьева

АО «Невское проектно-конструкторское бюро», Санкт-Петербург, Россия

dinvor@mail.ru

Аннотация. В настоящее время системы генерации квантовых ключей рассматриваются как основа квантовых телекоммуникаций с применением квантовой криптографии. При этом происходит подмена понятий: такая система просто генерирует одинаковый двоичный код на двух сторонах квантового канала и не позволяет передавать данные как в канале связи. В дальнейшем такой ключ используется классической криптографической системой в обычном канале связи. Низкая скорость генерации квантового ключа требует его накопления, что лишает этот ключ подтверждения подлинности – как только он представлен в виде файла, его можно подменить. Тем не менее, неуклонное повышение скорости генерации дает возможность применения квантового ключа для прямой защищенной передачи информации в квантовом канале «бит в бит» при любом квантовом протоколе и физической реализации. Способ такой передачи рассматривается в данной статье.

Ключевые слова: квантовые системы передачи информации, скорость передачи информации в квантовом канале, генерация квантового ключа

Для цитирования: Воробьева Д. Е. Передача информации в квантовом канале связи // Изв. СПбГЭТУ «ЛЭТИ». 2023. Т. 16, № 9. С. 77–82. doi: 10.32603/2071-8985-2023-16-9-77-82.

Благодарность: Выражаю признательность заведующему кафедрой информационной безопасности СПбГЭТУ «ЛЭТИ» д-ру техн. наук, доценту Е. Г. Воробьеву за помощь в выполнении исследования и за критические замечания в адрес статьи.

Original article

Information Transmission in a Quantum Channel

D. E. Vorobyova

JSC «Nevskoye Design Bureau», Saint Petersburg, Russia

dinvor@mail.ru

Abstract. Currently, quantum key generation systems are considered as the basis of quantum telecommunications using quantum cryptography. At the same time, concepts are substituted: such a system simply generates the same binary code on two sides of the quantum channel and does not allow data to be transmitted as in the communication channel. In the future, such a key is used by a classical cryptographic system in a conventional communication channel. The low rate of generation of a quantum key requires its accumulation, which deprives this key of authentication – as soon as once it is presented as a file, it can be replaced. Nevertheless, the steady increase in the generation rate makes it possible to use a quantum key for direct secure transmission of information in a quantum channel «bit to bit» with any quantum protocol and physical implementation. The method of such transfer is discussed in this article.

Keywords: quantum information transmission systems, speed of information transfer speed in the quantum channel, generation of quantum key generation

For citation: Vorobyova D. E. Information Transmission in a Quantum Channel // LETI Transactions on Electrical Engineering & Computer Science. 2023. Vol. 16, no. 9. P. 77–82. doi: 10.32603/2071-8985-2023-16-9-77-82.

Acknowledgements: I express my gratitude to the head of the department of information security of Saint Petersburg Electrotechnical University, Dr Sci. (Eng.), Docent E. G. Vorobyov who provided assistance in carrying out the research and for critical comments to the article.

Введение. Актуальность темы данной статьи обусловлена необходимостью создания современных защищенных информационных систем, в частности в рамках проекта Сейфнет Национальной технологической инициативы РФ. При этом для получения гарантированности свойств защиты в каналах передачи информации необходимо применение технологий, которые могли бы исключить типовые атаки злоумышленника на прослушивание канала, подмену информации и т. д. Причем гарантированность свойств защиты должна обеспечиваться в условиях сверхобученности даже простого человека компьютерным технологиям, системному и прикладному программированию, теории связи, не говоря уже о возможностях иностранных государственных спецслужб.

Появление нанотехнологий впервые позволяет обеспечить пространственную скрытность защищаемых технологических устройств, так как они выводятся из зоны видимости и сильно затрудняется возможность их визуального обнаружения и физического уничтожения. К сожалению, это не гарантирует энергетической скрытности, так как все ныне используемые системы передачи информации связаны с излучением электромагнитных волн в пространство или сопровождаются им.

Поэтому основой решения требуемой задачи могут быть пока только квантовые технологии. Они обладают рядом полезных свойств:

– при соблюдении определенных условий обеспечивается невозможность получения информации при прослушивании квантового канала;

– способность двух взаимодействующих пользователей обнаруживать присутствие любой третьей стороны, пытающейся получить информацию о ключе;

– квантовый ключ в момент его генерации позволяет в силу физических свойств одновременно обеспечивать идентификацию и аутентификацию передатчика и приемника.

В настоящее время как у нас в стране, так и за рубежом, остается нерешенной задача прямой передачи данных через квантовую линию. В данной статье предлагается метод такой передачи с использованием любой существующей в настоящее время системы генерации и распределения квантовых ключей (QKD).

Для достижения поставленной цели необходимо решить следующие задачи:

– предложить способ использования системы QKD для непосредственной передачи через нее требуемой информации без изменения физической реализации квантового канала;

– оценить скорость возможной передачи информации такой системой связи;

– оценить возможность применения в практических целях.

Модель квантовой системы передачи информации. Для того чтобы рассмотреть способ использования системы QKD для непосредственной передачи через нее требуемой информации, необходимо проанализировать текущую ситуацию с имеющимися в производстве квантовыми технологиями как у нас в стране, так и за рубежом.

К наиболее известным компаниям, производящим квантовые устройства для криптографии, относятся: «AUREA Technology» (Франция), «Quintessence Labs» (США), «ID Quantique» (Женева), «MagiQ Technologies Inc.» (Нью-Йорк), «QNuLabs» (Бангалор, Индия), «QuintessenceLabs» (Австралия), «SeQureNet» (Франция), «Квантовая оптика Йена» (Германия) и «KEEQuant» (Германия), «QRate» (Россия), «Инфотекс» (Россия), «Супертел» (Россия) [1], [2].

Организовали активные исследовательские программы «KETS Quantum Security» (Великобритания), «Toshiba», HP, IBM, «Mitsubishi», NEC и NTT, ЛИКС (Россия), «Квантовый центр КАИ» (Россия) и др. [1].

На основе имевшейся квантовой электроники были реализованы ряд квантовых протоколов: BB84, SARG04 BB84(4+2), B92, Экерта, DPS, COW, E91, Decoy state QKD, протокол А. Глейма (РФ), причем их физическая реализация сильно различается, так как используются счетчики фотонов, радиофотоника, квантовая запутанность, управляемая поляризация ЭМВ в специальных ВОЛС и т. д., что делает их практически несовместимыми.

Рассмотрим возможности систем QKD по скорости и дальности возможной связи. Ограничение скорости и расстояния, также известное как компромисс скорости и потерь, описывает, как по мере увеличения расстояния между передатчиком и приемником системы QKD скорость генерации ключей экспоненциально уменьшается. В тради-

ционных протоколах QKD эта проблема была устранена добавлением физически защищенных ретрансляционных узлов, которые могут быть размещены вдоль квантовой линии связи с намерением разделить ее на несколько секций с низкими потерями.

В 2007 г. было проведено квантовое распределение ключей по 148.7 км оптического волокна с использованием протокола BB84. В 2008 г. на основе этого же протокола впервые был проведен обмен защищенными ключами со скоростью 1 Мбит/с (более 20 км оптического волокна) и 10 Кбит/с (более 100 км оптоволокна). По состоянию на август 2015 г. наибольшее расстояние для оптического волокна составляло 307 км [3].

В июне 2017 г. впервые было выполнено квантовое распределение ключей от наземного передатчика к движущемуся самолету на расстояниях от 3 до 10 км с генерацией защищенных ключей длиной до 868 Кбайт. Практически одновременно с данным экспериментом в Китае были измерены запутанные фотоны на расстоянии 1203 км между двумя наземными станциями через спутник, заложив основу для будущих межконтинентальных экспериментов по квантовому распределению ключей на суммарной длине от 1600 до 2400 км. В январе 2022 г. индийским ученым удалось успешно создать атмосферный канал для обмена зашифрованными сообщениями и изображениями.

Учитывая, что типовая архитектура генерации ключей предполагает использование для формирования текущего состояния в канале и подключения фильтров на приемной стороне независимых датчиков случайных чисел, прослушивание в канале для злоумышленника бесполезно.

Следовательно, для защищенной передачи информации через данную архитектуру необходимо решить вопрос, что означают сгенерированные биты не в смысле ключа, а в информационном (передачи требуемых данных от передатчика к приемнику) смысле. Задачу упрощает тот факт, что открытый канал для процедуры распознавания не квантовый, а классический, т. е. двунаправленный.

Рассмотрим протокол распознавания на основе BB84 (рис. 1).

Из рисунка видно, что в открытом канале от приемника к передатчику будет передана информация, что распознаны биты 1, 4, 5, 7, 9. Таким образом, на обеих сторонах квантовой линии появится один ключ – 11001.

Предположим, что нужно передать данные в виде 11010…

Тогда для передачи информации для приведенного примера требуется выполнить следующий алгоритм:

1. При сравнении первого бита ключа приемник сообщает передатчику по открытому каналу, что принял его правильно.

2. Передатчик, зная, что передавалось состояние «1», сравнивает его с первым битом передаваемых данных.

3. Поскольку и требовалось передать «1», то передатчик сообщает приемнику, что он не только подтверждает формирование 1-го бита ключа, но приемник еще и получил первый бит данных (не разглашая его информационное значение).

Те же действия нужно будет предпринять для каждого бита ключа. При этом передатчик подтвердит передачу 1-го, 2-го и 3-го битов данных, 4-й и 5-й не совпали. Таким образом, скорость передачи данных оказывается меньше, чем скорость генерации ключа.

Чтобы скорость передачи в связи с этим не уменьшалась, а равнялась скорости генерации ключа, нужно ввести код сообщений от передатчика к приемнику по ответному каналу.

Допустим, переданная единица значит, что сгенерированный бит ключа одновременно озна-

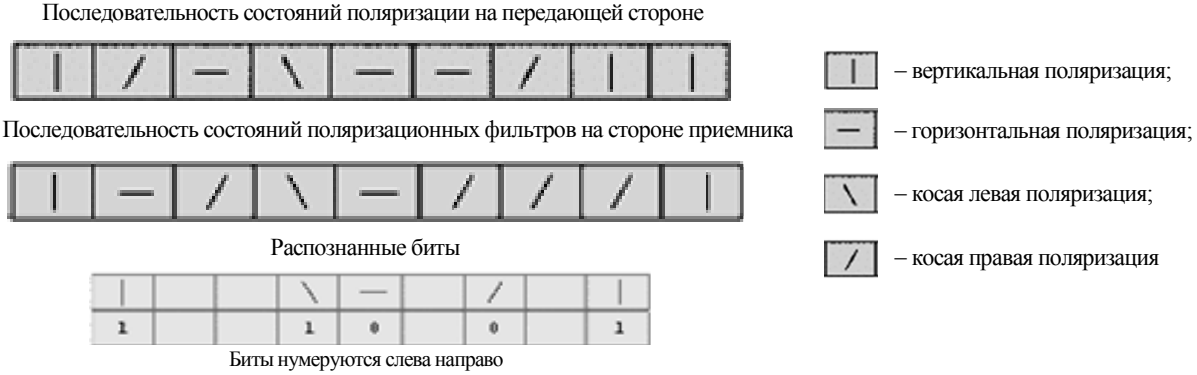

Рис. 1. Распознавание принятых битов
Fig. 1. Recognition of received bits

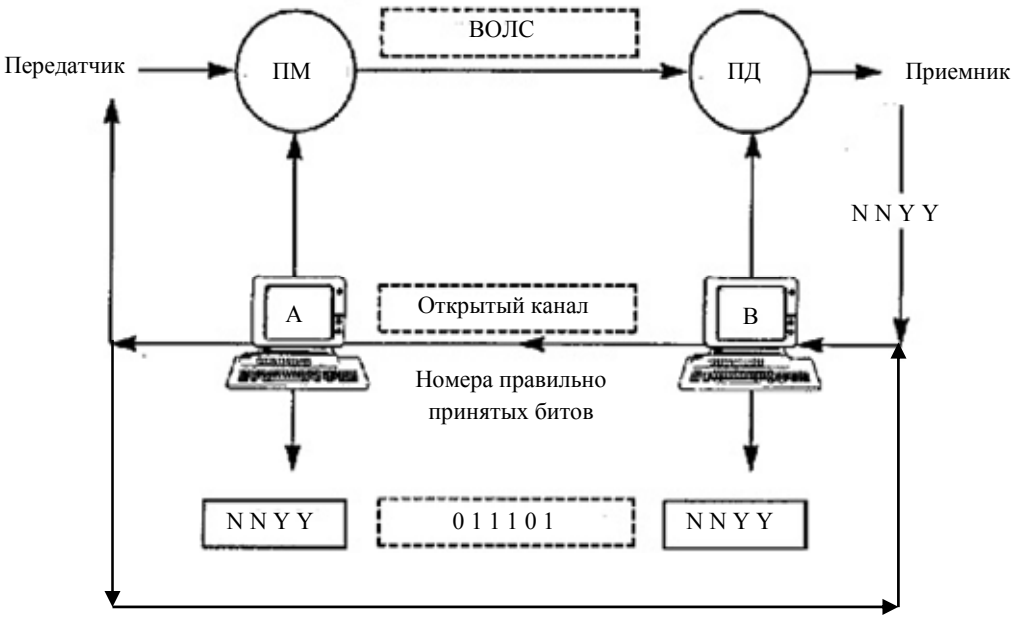

Рис. 2. Модель квантовой линия связи
Fig. 2. Quantum Communication Line Mode

чает правильно принятое значение (0 или 1) данных, а переданный «0» – что нужно взять инвертированное значение бита ключа. Модель квантового канала связи показана на рис. 2.

Здесь N, Y относятся к дополнительному подканалу (нижняя стрелка) и означают, что состояние поляризации не только распознано, но и соответствует нулю или единице информации, которая должна быть передана; ПМ – поляризационный модулятор; ПД – поляризационный детектор (фильтр); ВОЛС – волоконно-оптическая линия связи; А – Алиса, В – Боб (традиционные обозначения абонентов линии).

Модель отличается наличием дуплексного (двунаправленного) открытого канала. При этом условия неразглашения информации при прослушивании канала сохраняются. Для реализации обратной передачи потребуется внести только изменения в программную реализацию протокола согласования битов ключа.

Оценка возможной скорости передачи в квантовой линии связи и применимости ее в практических целях. Информационно-телекоммуникационные сети, применяемые в организациях, имеют необходимые для конкретных информационных сервисов скорости информационного обмена.

Главная проблема генерации квантовых ключей заключается в низкой скорости. Тем не менее, в 2019 г. в данной области был достигнут определенный успех. Компания «Toshiba Research Europe Ltd» в интересах Великобритании разработала технологию, которая за счет снижения количества темных шумов в квантовом канале сумела расширить диапазон практического QKD до 242 км при имеющей практическое значение скорости генерации ключа.

Технология имеет следующие особенности [4]:

– источник фотонов: модулированные по интенсивности слабые лазерные импульсы от телекоммуникационного лазерного диода. С помощью трех интенсивностей эффект многофотонных импульсов был смягчен («метод импульса приманки»);

– кодирование кубитов: разность фаз между двумя импульсами после интерферометра;

– активная обратная связь, используемая для компенсации фазовых и поляризационных дрейфов;

– фотонные детекторы: лавинные фотодиоды режима Гейгера комнатной температуры, «самодифференцирующийся» метод позволяет обнаруживать фотоны на гигагерцевых частотах.

Все каналы могут быть объединены на одном волокне с помощью деления по длине волны. Ключевая скорость, достигнутая на линии Бристоль–Лондон–Кембридж, составила 13.7 Мбит/с при потерях в канале 0 дБ (рис. 3) [4], где QBER – коэффициент квантовых ошибок по битам.

При этом применение охлажденных до низкой температуры детекторов позволило увеличить дальность связи до вышеуказанных значений (рис. 4) [4], [5].

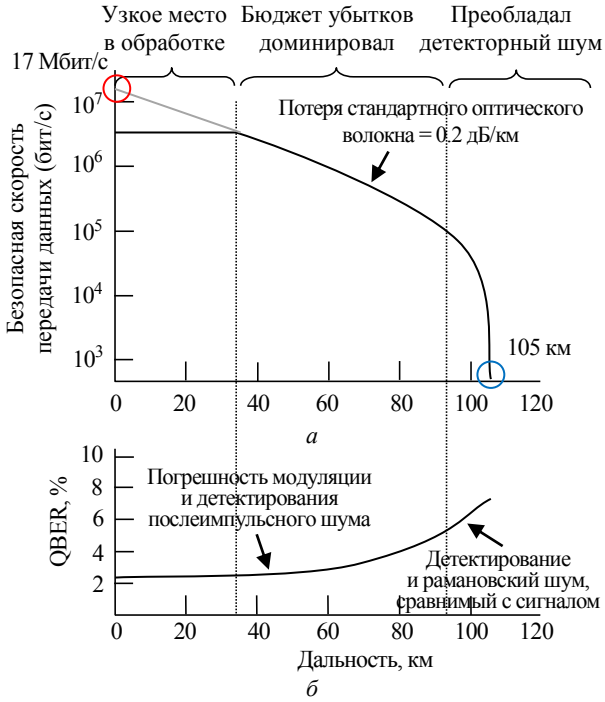

Рис. 3. Лучшая скорость генерации квантового ключа (*а*); коэффициент квантовых ошибок по битам (*б*)
Fig. 3. Better quantum key generation speed (*а*); Quantum error coefficient by bit (*б*)

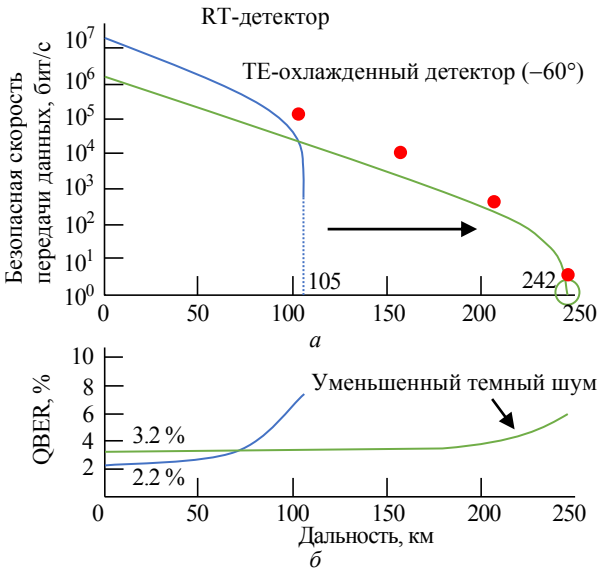

Рис. 4. Возможное увеличение дальности связи в QKD (*а*); коэффициент квантовых ошибок по битам (*б*)
Fig. 4. Possible increase in communication range in QKD (*а*); Quantum error coefficient by bit (*б*)

Поскольку в рассмотренном подходе к реализации квантовой линии связи было указано, что возможны передача данных со скоростью генерации квантовых ключей и связь на длину работы канала связи, можно сделать следующий вывод: в настоящее время появилась возможность создания чисто квантовой линии связи со скоростью передачи данных до 14 Мбит/с на дальность до 240 км [6].

Скорость 10 Мбит/с считается достаточной для реализации компьютерных сетей пригодных для использования в электронном документообороте компаний, т. е. большинстве офисных сервисов.

Заключение. Разработанная модель квантовой линии связи была реализована в виде программного комплекса, применяемого в электронных коммутационных устройствах, разрабатываемых ООО «Кьювуд» в интересах проекта Сейфнет НТИ РФ и апробирована на площадке киберполигона ИТЦ «Ингрия» (Санкт-Петербург) в 2022 г.

Применение предложенной технологии квантовой связи позволяет сделать следующий шаг к квантовым системам хранения информации, а также к современным образцам отечественных квантовых компьютеров.

Список литературы

1. Поляков А. В., Ляховская Е. И. Скорость формирования квантового распределения ключа в волоконно-оптических системах квантовой криптографии. URL: https://elib.bsu.by/bitstream/123456789/271766/1/275-279.pdf (дата обращения 30.06.2023).

2. Suma M. R., Madhumathy P. An optimal swift key generation and distribution for QKD // Scientific and Technical J. of Information Technologies, Mechanics and Optics. 2022. Vol. 22, no. 1. P. 101–113. doi: 10.17586/2226-1494-2022-22-1-101-113.

3. Скорость генерации кода в системе квантового распределения ключей / А. С. Задорин, А. В. Максимов, Д. А. Махорин, С. О. Чечулин, А. А. Маликов // Докл. ТУСУРа. 2011. № 2-2 (24). С.139–141.

4. Shields A. Performance limits for quantum key distribution networks // Toshiba Research Europe Ltd. 2019. URL: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Andrew_Shields_Presentation.pdf (дата обращения 11.04.2023).

5. Schiavon M., Vallone G., Villoresi P. Experimental realization of equiangular three-state quantum key distribution // Scientific Reports. 2016. No. 6. P. 30089. doi: 10.1038/srep30089.

6. Lightweight authentication for quantum key distribution / E. O. Kiktenko, A. O. Malyshev, M. A. Gavreev, A. A. Bozhedarov, N. O. Pozhar, M. N. Anufriev, A. K. Fedorov // IEEE Transaction on Information Theory. 2020. Vol. 66, no. 10. P. 6354–6368. doi: 10.1109/TIT.2020.2989459.

Информация об авторе

Воробьева Диана Евгеньевна – ведущий программист АО «Невское проектно-конструкторское бюро».
E-mail: dinvor@mail.ru

References

1. Polyakov A. V., Lyahovskaja E. I. Skorost' formirovanija kvantovogo raspredelenija kljucha v volokonno-opticheskih sistemah kvantovoj kriptografii. URL: https://elib.bsu.by/bitstream/123456789/271766/1/275-279.pdf (data obraschenija 30.06.2023). (In Russ.).

2. Suma M. R., Madhumathy P. An optimal swift key generation and distribution for QKD // Scientific and Technical J. of Information Technologies, Mechanics and Optics. 2022. Vol. 22, no. 1. P. 101–113. doi: 10.17586/2226-1494-2022-22-1-101-113.

3. Skorost' generatsii koda v sisteme kvantovogo raspredelenija klyuchej / A. S. Zadorin, A. V. Maksimov, D. A. Mahorin, S. O. Chechulin, A. A. Malikov // Dokl. TUSURa. 2011. № 2-2 (24). S. 139–141. (In Russ.).

4. Shields A. Performance limits for quantum key distribution networks // Toshiba Research Europe Ltd. 2019. URL: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Andrew_Shields_Presentation.pdf (data obraschenija 11.04.2023).

5. Schiavon M., Vallone G., Villoresi P. Experimental realization of equiangular three-state quantum key distribution // Scientific Reports. 2016. No. 6. P. 30089. doi: 10.1038/srep30089.

6. Lightweight authentication for quantum key distribution / E. O. Kiktenko, A. O. Malyshev, M. A. Gavreev, A. A. Bozhedarov , N. O. Pozhar, M. N. Anufriev, A. K. Fedorov // IEEE Transaction on Information Theory. 2020. Vol. 66, no. 10. P. 6354–6368. doi: 10.1109/TIT.2020.2989459.

Information about the author

Diana E. Vorobyova – Leading Programmer of JSC «Nevskoye Design Bureau».
E-mail: dinvor@mail.ru

Статья поступила в редакцию 12.08.2023; принята к публикации после рецензирования 23.08.2023; опубликована онлайн 23.11.2023.

Submitted 12.08.2023; accepted 23.08.2023; published online 23.11.2023.