15. Gholizadeh N., Musilek P. *Distributed learning applications in power systems: A Review of Methods, Gaps, and Challenges*. Energies, 2022, vol. 14, pp. 3654.
16. Bishoyi P.K., Misra S. Towards Energy-and Cost-Efficient Sustainable MEC-Assisted Healthcare Systems. *IEEE Transactions on Sustainable Computing*, 2022, vol. 7, no. 2, pp. 550–556.
17. Goldstein A.B. et al. Providing QOS for OTT Services in Communication Networks. *2020 Systems of Signals Generating and Processing in the Field of on Board Communications*. Moscow: Institute of Electrical and Electronics Engineers, 2020, pp. 9078633. DOI: 10.1109/IEEECONF48371.2020.9078633.

Received 30.08.2023

НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 681.3.07

МЕТОДЫ И СРЕДСТВА КВАНТОВОЙ КРИПТОГРАФИИ

Васин Н.Н.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: vasin-nn@psuti.ru

Для обеспечения безопасного обмена данными по сети необходимо соблюдать требования к конфиденциальности, целостности и доступности передаваемой информации. Для соблюдения указанных требований производится шифрование данных на передающей стороне и дешифрование полученной информации – на принимающей стороне. Шифрование передаваемого сообщения выполняется по правилам, которые определяются алгоритмом и ключом. Криптобезопасность зашифрованной информации зависит от длины ключа. Среди алгоритмов шифрования выделяют алгоритмы с симметричным (закрытым) ключом и с асимметричным (открытым) ключом. При всех достоинствах закрытого ключа для его доставки от одного пользователя другому (распределение ключей) используют асимметричные ключи. Однако высокопроизводительные квантовые компьютеры способны дешифровать перехваченную информацию. Поэтому в современных криптографических системах используют квантовое распределение ключей. Идея использования квантовых битов была предложена в 1970 г. С. Визнером. В 1984 г. Ч. Беннет и Ж. Брассар предложили протокол BB84. Использование «запутанных» квантов для систем с квантовым распределением ключей предложил в 1991 г. А. Экерт. На основе указанных протоколов создаются все современные системы квантовой криптографии.

Ключевые слова: *передача информации, криптография, квантовое распределение ключей, поляризация, протоколы (алгоритмы) шифрования BB84, B92, E91, BBM92, запутанные кванты*

Введение

Безопасный обмен сообщениями по сети обеспечивается с помощью алгоритмов и ключей шифрования. Чем длиннее ключ, тем труднее его взломать, т.к. на это тратится больше вычислительных ресурсов. Для безопасного распределения ключей разработан целый ряд протоколов [1].

Среди множества классических алгоритмов (протоколов) шифрования можно выделить два типа: с симметричным (закрытым, секретным) ключом и с асимметричным (открытым) ключом, что позволяет компьютерам совместно использовать ресурсы сети [1–3].

В первом случае передающая и принимающая сторона имеют одинаковый ключ, который нужно заблаговременно доставить обеим сторонам обмена данными. Недостатком алгоритма является сложность доставки ключей множеству взаимодействующих пар абонентов по открытым каналам связи (сложность распределения ключей).

В алгоритмах с асимметричным (открытым) ключом используются два ключа: один ключ – при шифровании сообщения, и другой – при расшифровке. Системы шифрования с асимметричным открытым ключом требуют больших вычислительных ресурсов по сравнению с системами с секретным симметричным ключом. Поэтому обычно шифрование с открытым ключом используют для распределения ключей (для обмена ключами) и аутентификации, т.е. для шифрования сравнительно коротких сообщений. Для шифрования больших объемов передаваемых данных используют симметричный алгоритм с секретным (закрытым) ключом [2].

Развитие вычислительной техники и появление высокоскоростных квантовых компьютеров позволит дешифровать перехваченное сообщение

за несколько минут или даже секунд. Поэтому для безопасного распределения ключей разрабатываются новые системы квантовой криптографии.

Методы квантовой криптографии

Методы квантовой криптографии основаны на передаче состояния кванта по сети. В квантовых сетях и системах информацию переносят квантовые биты (q-биты, кубиты), которые представляют собой поляризованные фотоны, передаваемые по волоконно-оптическим линиям связи или беспроводным радиоканалам [3].

Идея использования квантовых битов была предложена Стивеном Визнером (Stephen Wiesner) в 1970 г., но отклонена редакцией журнала IEEE Information Theory [4]. Позднее (в 1984 г.) Чарльзом Беннетом (Charles Bennett) и Жилем Брассаром (Gilles Brassard) был предложен протокол BB84 [5; 6]. Идеи, заложенные в [5; 6] остаются актуальными до настоящего времени. Некоторые публикации, посвященные BB84, представлены в списке литературы [7–12].

Согласно протоколу BB84, носителями информации являются фотоны, которые могут быть поляризованы под углами 0°, 45°, 90°,135° (рисунок 1).

Открытый и квантовый каналы

Указанные четыре состояния относятся к двум базисам, например, в первом базисе для передачи 0 используется горизонтальная поляризация фотона (0°), а для передачи 1 – вертикальная (90°). Данный базис обычно обозначается ⊗ (рисунок 1). Во втором базисе фотон может быть поляризован под углами 45° или 135°. Базис обозначается ⊗.

Таким образом, квант может находиться в одном из четырех состояний. Два состояния поляризации внутри одного базиса ортогональны, но состояния из разных базисов –попарно неортогональны. При попытке измерения квантового состояния нелегитимным пользователем оно изменяется, квант разрушается, о чем сразу становится известно легитимному пользователю. Это свойство (запрета клонирования) и позволяет создавать безопасные квантовые системы криптографии. При этом легитимные пользователи могут обмениваться результатами кодирования по открытым каналам.

Ниже рассмотрен пример формирования согласованного квантового ключа для обмена информацией между абонентами A1 и B2 (рисунок 2).

В литературе первого абонента (A1) обычно называют Алиса, второго пользователя (B2) – Боб, а нелегитимного злоумышленника (хакера) – Ева, задачей которого является перехват трафика между Алисой и Бобом [3–12].

Для реализации протокола BB84 используются два канала: открытый и канал квантового

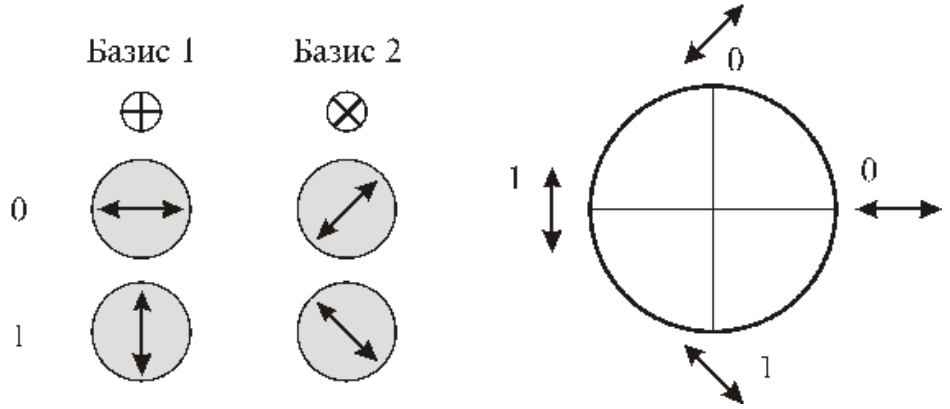

Рисунок 1. Состояния квантовых битов

Рисунок 2. Открытый и квантовый каналы связи

распределения ключей, которые связывают двух пользователей A1 и B2. Пользователь A1 генерирует случайную последовательность битов, из которой затем формируется общий секретный ключ. В литературе [3–12] рассмотрены различные последовательности битов. В приведенном ниже примере генератор случайных чисел узла A1 сформировал последовательность 11001101 (таблица 1), то есть, при формировании первого бита была сгенерирована 1, при этом использовалась диагональная поляризация ⤡. Подобное состояние передается пользователю B2 по квантовому каналу (рисунок 2).

На стороне B2 случайным образом выбирается базис поляризации (вертикальный или диагональный) для обработки полученного кубита, например, была выбрана вертикальная поляризация ⊕. Значение базиса поляризации передается пользователю A1 по открытому каналу. В приведенном примере выбранный пользователем B2 базис поляризации ⊕ не совпадает с базисом поляризации ⤡ пользователя A1. При отсутствии совпадения базисов A1 и B2 очередной бит кодовой последовательности не формируется. Таким образом, первый бит генерируемой последовательности для создания секретного ключа не был сформирован, на что указывает символ (-) в строке Ключ (таблица 1).

При передаче следующего бита (1) случайным образом выбрана вертикальная поляризация ↕. В рассматриваемом примере выбранный пользователем B2 базис поляризации второго бита ⊕ совпадает с базисом поляризации ↕ пользователя A1. При совпадении базисов A1 и B2 формируется очередной бит кодовой последовательности, т.е. второй бит генерируемой последовательности (равный 1), используется для создания первого бита секретного ключа.

При формировании секретного ключа узел B2 по открытому каналу связи передает узлу A1 значение случайно выбранного базиса поляризации, но значение бита генерируемой последовательности – не передает. Однако A1, получив подтверждение совпадения базисов поляризации, получает сообщение о том, что пользователь B2 сформировал такое же значение кубита, какое передал A1. В рассматриваемом примере на втором такте передается двоичная единица случайной последовательности. На втором такте произошло совпадение базисов поляризации. Поскольку пользователь A1 передавал значение единицы, то при совпадении базисов узел B2 также сформировал 1.

На третьем такте работы алгоритма базисы поляризации A1 (↔) и B2 (⊗) не совпали, поэтому информационный бит ключа сформирован не был.

На четвертом такте передавался ноль, было совпадение базисов поляризации, поэтому на B2 сформировался 0 (таблица 1), и т.д.

Полученная случайная последовательность битов является общей для A1 и B2, она называется просеянным ключом. Длина просеянного ключа примерно в 2 раза меньше длины исходного (сырого) ключа, в приведенном примере из восьми бит был сформирован четырехразрядный ключ (1011).

На основе протокола BB84 проводится разработка устройств, систем и сетей передачи информации по квантово-оптическим сетям. Схема практической реализации BB84 в квантовом канале сети (рисунок 3) с небольшими изменениями приводится в целом ряде работ, например [3; 7; 10].

На передающей стороне A1 (рисунок 3) формируется одно из 4-х состояний поляризации кванта, переносимого световым импульсом. Изменения поляризации квантов передаваемого потока реализуют поляризатор и ячейки Покеля (Поккельса), которые являются поляризационными модуляторами. Сигналами управления для них служат информационные биты данных.

На принимающей стороне с помощью ячейки Покеля производится анализ импульсов поляризации ⊕ или ⊕. После ячейки Покеля луч попадает на Кальцитную призму (рисунок 3), которая расщепляет луч на два фотодетектора (ФЭУ). Луч с определенной поляризацией дешифруется либо нижним фотоэлектронным умножителем ФЭУ, либо верхним ФЭУ.

Таким образом, схема работает только, если отправитель A1 и получатель B2 знают, какой вид поляризации используется при передаче очередного бита информации. В противном случае получатель не получит ожидаемую информацию, данные будут разрушены. Информацию о выбранном базисе поляризации можно передать по открытому каналу.

Таблица 1. Квантовая криптография. Формирование секретного ключа

Послед. A1	1	1	0	0	1	1	0	1
Поляр. A1	⤡	↕	↔	⤢	↔	⤡	⤢	↕
Базис B2	⊕	⊕	⊗	⊗	⊕	⊗	⊕	⊗
Совп.	нет	Совп.	нет	Совп.	Совп.	Совп.	нет	нет
Ключ	-	1	-	0	1	1	-	-

Известен целый ряд модификаций протокола BB84. Например, в работах [3; 9; 13–16] отмечено, что Чарльз Беннет предложил алгоритм B92 для выявления искажений данных, передаваемых по квантовому каналу.

Ниже приведен алгоритм B92 [15]:

1. Отправитель и получатель заранее оговаривают произвольность расположения битов в строках, что определяет произвольный характер положения ошибок.

2. Все строки разбиваются на блоки длиной k, где k выбирается так, чтобы минимизировать вероятность ошибки.

3. Отправитель и получатель определят четность каждого блока, и сообщают её друг другу по открытому каналу связи. После этого в каждом блоке удаляют последний бит.

4. Если четность двух каких-либо блоков оказалось разной, отправитель и получатель производят итерационный поиск неверных битов и исправляют их.

5. Затем весь алгоритм выполняется заново для другого (большего) значения k. Это делается для того, чтобы исключить ранее незамеченные кратные ошибки.

6. Чтобы определить точность обнаружения всех ошибок, проводится псевдослучайная проверка. Отправитель и получатель открыто сообщают о произвольной перестановке половины битов в строках, а затем вновь открыто сравнивают четности (Если строки различны, четности должны не совпадать с вероятностью 0,5). Если четности отличаются, отправитель и получатель производят двоичный поиск и удаляют неверные биты.

7. Если различий не наблюдается, после n итераций отправитель и получатель получат одинаковые строки с вероятностью ошибки 2^{-n}.

Протокол B92 не стал конкурентом протоколу BB84, поскольку при его использовании сложнее обнаружить вторжение злоумышленника [14]. Отмечена сложность реализации квантового распределения ключей для мобильных устройств телекоммуникаций [16], поскольку необходима установка сложной аппаратуры на обоих концах канала связи, что на данном этапе развития технологий невозможно реализовать в компактном корпусе телефона для мобильной связи. Однако работы по созданию мобильных устройств и систем с квантовым распределением ключей интенсивно ведутся по настоящее время.

Для дальнейшего повышения эффективности функционирования систем квантового распределения ключей используют парадокс EPR (ЭПР – Эйнштейн-Подольский-Розен). Метод квантового распределения ключей (E91) на основе ЭПР был предложен Артуром Экертом (Artur K. Ekert) в 1991 г. [17–20]. Согласно E91 генератор запутанных квантов излучает два фотона в противоположных направлениях, в сторону пользователей A1 и B2 (рисунок 4).

Поляризация каждого кванта передаваемой пары не определена, но их поляризации всегда противоположны. То есть, когда один квант будет в состоянии 0, то второй квант будет находиться в противоположном состоянии 1.

При изменении состояния первого кванта переключение второго происходит мгновенно, независимо от расстояния между «запутанными» частицами. Измерение состояния первого кванта однозначно определяет результат измерения второй «запутанной частицы».

Особенностью метода Экерта является квантовый канал с единственным источником, испускающим пары запутанных квантов (поляризованные фотоны) [17–20]. Частицы разделяются,

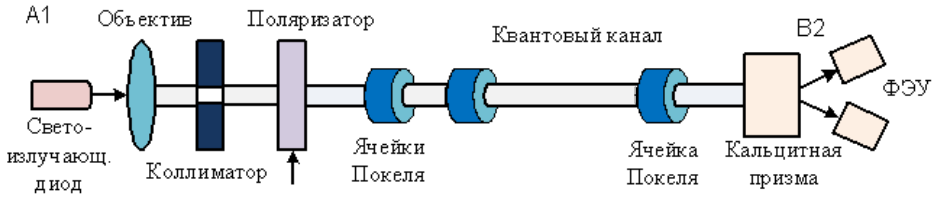

Рисунок 3. Схема практической реализации BB84 в квантовом канале

Рисунок 4. Модель КРК с «запутанными квантами»

при этом A1 и B2 получают по одной частице от каждой пары (рисунок 4). Каждый (A1 и B2) случайным образом выбирает базис поляризации для измерения полученных частиц. Как и в методе BB84, пользователи A1 и B2 открыто обсуждают, какие базисы использованы для измерений. Для каждого измерения, в котором A1 и B2 использовали одинаковые базисы, результаты будут противоположными вследствие реализации принципа квантовой запутанности. То есть, битовая строка, например A1, будет двоичным дополнением B2. Таким образом, A1 и B2 получат общий секретный ключ [17–19].

Разработка А. Экертом протокола, основанного на запутанных квантах, положила начало модификации существующих протоколов и разработке новых. Например, Ч. Беннет и Ж. Брассар создали протокол BBM92 [21], который является модификацией BB84. Протокол BBM92 использует принцип ЭПР [20–23]. Использование запутанных пар фотонов повышает безопасность обмена данными. В работе [20] подчеркивается схожесть методов BB84 и E91, а также отмечается, что любой вариант BB84 может быть адаптирован для использования источника запутанных квантов.

Новые разработки протоколов квантового распределения ключей направлены на уменьшение количества ошибок при передаче сообщений и повышение устойчивости к атакам. Например, протокол SARG04 (Scarani V. Acin A., Ribordy G., Gisin N.) [20; 23; 24], позволяет уменьшить количество ошибок при использовании двухфотонного источника запутанных квантов, вместо однофотонного. Характеризуется устойчивостью к атакам с разделением по числу фотонов (к PNS-атакам – Photon Number Splitting attack).

Протокол Lo05 [25] был разработан в 2005 г. группой исследователей (Lo H., Ma X., Chen K.). Стандартные состояния Lo05 поляризации аналогичны состояниям BB84. Злоумышленник может подавить однофотонные сигналы, затем разделить на части многофотонный сигнал, выделить одну копию для себя, а вторую отправить получателю информации B2. Поэтому безопасная передача сообщения BB84 возможна только, если на передающей стороне генерируются единичные (одиночные) фотоны, что не всегда возможно. Для обнаружения подслушивания в Lo05 создается набор дополнительных состояний (приманок), интенсивность которых отличается от стандартных. Приманки позволяют обнаружить прослушивание.

Таким образом, разработка и исследование протоколов квантового распределения ключей продолжается по настоящее время. На основании предложенных протоколов во всем мире создаются программно-аппаратные средства систем и сетей телекоммуникаций с высокой степенью безопасности.

В работах [16; 26] отмечаются корпорации, которые активно проводят исследования и разработку систем и устройств с квантовым распределением ключей КРК (QKD - Quantum Key Distribution): IBM, GAP-Optique, Mitsubishi, Toshiba и др. Проведенные исследования QKD позволили разработать принципиальные схемы связи, создать и испытать опытные линии связи длиной в несколько десятков и сотен км.

В работе [26] также приведено описание созданных компонентов QKD (генератор поляризационно-коррелированных пар фотонов; настольный модуль для счета фотонов; дискретные счетчики одиночных фотонов; модули для коррелированного по времени подсчета фотонов; электрооптические модуляторы; контроллеры поляризации; волоконно-оптические компоненты; рефлектометры для измерения характеристик элементов систем связи). Приведены принципиальные схемы систем связи, ставшие основой современных сетей.

Введение санкций ограничивает использование импортной аппаратуры криптографии. Выход из введенных санкционных ограничений видится в налаживании широкого производства отечественных устройств, систем и сетей КРК.

Разработке устройств и систем квантового распределения ключей КРК (QKD) посвящены материалы множества сайтов, статей в журналах и публикаций материалов конференций, форумов, симпозиумов [27–33]. На состоявшемся в июле 2023 г. Форуме будущих технологий «Вычисления и связь. Квантовый мир» [27] отмечалось, что основными заказчиками систем квантовой криптографии в России являются ОАО «РЖД», ОАО «Газпром», Госкорпорация «Росатом» и другие предприятия и ведомства, которым важны проблемы безопасности передачи информации по сетям связи. Значимость Форума подчеркивается его посещением Президентом России В.В. Путиным.

Правительство РФ определило, что за развитие «Квантовых коммуникаций» ответственным является ОАО «РЖД», которое в настоящее время создает магистральную квантовую сеть протяженностью более 1000 км. До конца 2023 г. ее протяженность должна составить более 2500 км. В течение 2024 г. к квантовой сети должны быть присоединены города Сочи, Волгоград, Самара, Уфа, Пермь, Екатеринбург, Челябинск. В 2025

году планируется построить участок от Уфы до Магнитогорска [27]. Сеть создается только на отечественном оборудовании, в создании сети участвуют операторы связи «Ростелеком», «Трансте-леком». Создание сети и разработку системы КРК совместно реализовали ученые из Университета ИТМО и компании ООО «СМАРТС-Кванттелеком» (Санкт-Петербург) [28]. Работа по улучшению характеристик систем с КРК продолжается; например, в Университете ИТМО предложили модификацию системы квантового шифрования с компактным детектором [29]. Разработки [28] являются продолжением и развитием работ компании СМАРТС из г. Самара [30].

В докладе [28] подчеркивается особо важная роль КРК в системах связи специального назначения. Только системы с КРК могут обеспечить криптографическую устойчивость при неограниченных вычислительных ресурсах. Также в работе [28] приведены примеры реализации квантовых криптографических сетей и систем, разработанных компонентов (оптических модуляторов, детекторов одиночных фотонов и др.), приведены основные параметры созданных систем КРК, проведен сравнительный анализ ряда импортных компонентов и отечественных аналогов.

Совместные исследования и разработки компании «СМАРТС-Кванттелеком» с Университетом ИТМО при поддержке ОАО «РЖД» [28] были широко представлены на стендах форума [27]. Особо подчеркнута разработка модуля шифрования «МШ ТР-КРК» в конструктиве 4U. Система реализована с использованием боковых частот.

Следует отметить, что многие ВУЗы РФ совместно с отечественными компаниями активно исследуют, разрабатывают и внедряют в практику технологии квантовых сетей. Результатом совместного проекта МГУ им. М. В. Ломоносова и Нижегородского университета им. Н. И. Лобачевского является межуниверситетская квантовая сеть, первый участок которой проложен между Москвой и Н. Новгородом [27].

На портале выбора технологий и поставщиков (TAdviser) [31; 32] среди отечественных разработчиков программно-аппаратных средств отмечено, что Центр квантовых технологий МГУ им. М. В. Ломоносова и компания «Инфо ТеКС» создали систему выработки и распределения ключей (ViPNet Quantum Security System – ViPNet QSS) на основе протокол квантового распределения ключей КРК. В результате совместного проекта ОАО «Инфо ТеКС» и МГУ им. М. В. Ломоносова в офисе ИнфоТеКС развернута сеть опытной эксплуатации. К сети компании подключен сегмент квантовой сети МГУ [33].

Казанский центр квантовых технологий (Russian Quantum Center) Казанского национального исследовательского технического университета имени А.Н. Туполева — КАИ (ККЦ КНИТУ-КАИ) реализовал обмен квантовыми ключами по ВОЛС длиной 143 км [31].

В Центре компетенций НТИ «Квантовые коммуникации» НИТУ Московского института стали и сплавов (МИСИС) предложили повысить уровень защищенности систем и устройств квантовой криптографии за счет оценки уровней шумов в квантовом генераторе случайных чисел [31]. Совместно с Московским техническим университетом связи и информатики (МТУСИ) создана сеть открытого доступа с квантовым распределением ключей [34]. В МТУСИ проводятся исследования по воздействию сильных электромагнитных полей на квантовую связь [31]. Показано, что разряды молнии могут изменять поляризацию передаваемого по ВОЛС кванта. Особенно важно исследовать влияние сильных электромагнитных полей на беспроводные квантовые сети [35].

Заключение

Проведенный обзор показал, что совместные разработки ВУЗов и научно-производственных компаний позволили реализовать планы по созданию квантовых криптографических систем и сетей телекоммуникаций.

Литература

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учеб. пособие для вузов. СПб: Питер, 2016. 992 с.
2. Администратор информационной безопасности. Основы криптографии. URL: https://intuit.ru/studies/mini_mba/5398/courses/547/lecture/12387 (дата обращения: 29.09.2023).
3. Семенов Ю.А. Телекоммуникационные и информационные технологии. 6.9. Квантовая криптография. URL: http://book.itep.ru/6/q_crypt.htm (дата обращения: 29.09.2023).
4. Wiesner S. Conjugate Coding // ACM SIGACT News. 1983. Vol. 15, no. 1. P. 78–88. DOI:10.1145/1008908.1008920
5. Bennett C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing // Proceedings of International Conference on Computers, Systems & Signal Processing. India, Bangalore. 1984. P. 175–179.
6. Bennett C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin

Tossing // ACM SIGACT News. 1987. Vol. 18, no. 4. P. 51–53. DOI:10.1145/36068.36070
7. BB84 – Википедия. URL: https://ru.wikipedia.org/wiki/BB84 (дата обращения: 29.09.2023).
8. Инфо ТеКС ViPNet QSS квантовый телефон. URL: https://www.tadviser.ru/index.php/Продукт:ИнфоТеКС_ViPNet_QSS_Phone_квантовый_телефон (дата обращения: 02.10.2023).
9. Lopes M., Sarwade N. Cryptography from quantum mechanical viewpoint // International Journal on Cryptography and Information Security (IJCIS). 2014. Vol. 4, no. 2. P. DOI:10.5121/ijcis.2014.4202 13
10. Слепов Н.Н. Квантовая криптография: передача квантового ключа. Проблемы и решения. Электроника: Наука, Технология, Бизнес. URL: https://www.electronics.ru/files/article_pdf/0/article_705_722.pdf (дата обращения: 01.10.2023).
11. Радько Н.М., Мокроусов А.Н. Криптографические протоколы: учеб. пособие. Воронеж: Воронежский государственный технический университет, 2006. 104 с.
12. Слепов Н.Н. Современные технологии цифровых оптоволоконных сетей связи. М.: Радио и связь, 2003. 468 с.
13. Charles H. Bennett. Quantum Cryptography Using Any Two Nonorthogonal States // Physical Review Letters. 1992. Vol. 68, no. 21. P. 3121–3124.
14. Протокол B92. URL: https://ru.wikipedia.org/wiki/B92 (дата обращения: 29.09.2023).
15. Квантовая криптография. URL: https://ru.wikipedia.org/wiki/Квантовая_криптография (дата обращения: 29.09.2023).
16. Стойкое квантовое шифрование – будущее информационной безопасности. URL: https://integral-russia.ru/2016/06/10/stojkoe-kvantovoe-shifrovanie-budushhee-informatsionnoj-bezopasnosti/ (дата обращения: 29.09.2023).
17. Artur K. Ekert. Quantum cryptography based on Bell's theorem // Physical Review Letters. 1991. Vol. 67, no. 6. P. 661–663.
18. Протокол E91. URL: https://ru.frwiki.wiki/wiki/Protocole_E91 (дата обращения: 26.09.2023).
19. Протокол квантового распределения ключей с использованием ЭПР. URL: https://ru.wikipedia.org/wiki/Протокол_кван-тового_распределения_ключей_с_использо-ванием_ЭПР (дата обращения: 26.09.2023).
20. A Survey of the Prominent Quantum Key Distribution Protocols. URL: https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/ (дата обращения: 29.09.2023).
21. Charles H.B., Gilles B. Quantum cryptography: Public key distribution and coin tossing // Theoretical Computer Science. 2014. Vol. 560, no.1. P. 7–11.
22. BBM92 – протокол квантового шифрования. URL: https://ru.wikipedia.org/wiki/BBM92 (дата обращения: 29.09.2023).
23. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations / V. Scarani [et al.] // Physical Review Letters. 2004. Vol. 92, no. 5. P. 057901. DOI: 10.1103/PhysRevLett.92.057901
24. SARG04 – протокол квантового распределения ключей. URL: https://ru.wikipedia.org/wiki/SARG04 (дата обращения: 26.09.2023).
25. Протокол Lo05. URL: https://flirt24.ru/stati/14648-lo05.html (дата обращения: 26.09.2023).
26. Системы для квантово-оптических криптографических коммуникаций. Специальные системы. Фотоника. URL: https://sphotonics.ru/solutions/quantum-cryptography/ (дата обращения: 26.09.2023).
27. Попов С.А. Квантовые коммуникации выходят на передний план // Первая миля. 2003. №5. P. 34–39. DOI: 10.22184/2070-8963.2023.113.5.34.39
28. Алексеев А.Л. Разработки ООО «СМАРТС-Квантелеком» в области квантовых коммуникаций. Квантовые криптографические системы выработки и распределения ключа. URL: https://www.smarts.ru/media/filer_public/9b/68/9b687732-ac4f-4331-8b56-03355411f6ba/smarts_kvanttelekom.pdf (дата обращения: 26.09.2023).
29. Ученые университета ИТМО предложили модификацию системы квантового шифрования с компактным детектором. URL: https://news.itmo.ru/ru/news/9580/ (дата обращения: 29.09.2023).
30. Квантовые коммуникации для защиты линий связи. URL: https://www.smarts.ru/media/filer_public/a8/a0/a8a034b5-bdb6-4762-8c7b-b1778019c77c/22.pdf (дата обращения: 29.09.2023).
31. Квантовая криптография / шифрование. URL: https://www.tadviser.ru/index.php/Статья:Квантовая_криптография_(шифрование). (дата обращения: 29.09.2023).
32. ViPNet QSS (Quantum Security System). URL: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:ViPNet_QSS_(Quantum_Security_System) (дата обращения: 29.09.2023).
33. Гусев Д. Квантовые продукты Инфо-ТеКС.

Квантовые технологии и безопасность. URL: https://infotecstechfest.ru/upload/iblock/20f/tvtc2bzrgt8sr9fk27myjwo1o4yudjww.pdf. (дата обращения: 29.09.2023).
34. Первая опытная квантовая сеть в России. URL: https://mtuci.ru/about_the_university/news/4813/ (дата обращения: 29.09.2023).
35. В МТУСИ реализовали беспроводную квантовую связь на базе серийного отечественного оборудования. URL: https://naked-science.ru/article/column/v-mtusi-realizovali-besprovodnuyu-kvantovuyu (дата обращения: 29.09.2023).

Получено 02.10.2023

Васин Николай Николаевич, д.т.н., профессор, профессор кафедры сетей и систем связи Поволжского государственного университета телекоммуникаций и информатики. 443010, Российская Федерация, г. Самара, ул. Л. Толстого, 23. Тел. +7 917 103-05-44. E-mail: vasin-nn@psuti.ru

QUANTUM CRYPTOGRAPHY METHODS AND INSTRUMENTS

Vasin N.N.
Povolzhskiy State University of Telecommunications and Informatics, Samara, Russian Federation
E-mail: vasin-nn@psuti.ru

Secure data exchange over the network is ensured by the requirements of confidentiality, integrity and availability of information. To meet these requirements, sent data is encrypted on the sending side, and the received information is decrypted on the receiving side. Transmitted message is encrypted according to rules determined by the algorithm and key. Crypto security of encrypted information depends on the key length. Among the encryption algorithms, there are algorithms with a symmetric (private) key and with an asymmetric (public) key. Despite all the advantages of a private key, asymmetric keys are used to deliver it from one user to another (key distribution). However, high-performance quantum computers are capable to decrypt intercepted data. Therefore, modern cryptographic systems use quantum key distribution method. The idea of using quantum bits was proposed in 1970 by S. Wiesner. In 1984, Ch. Bennett and G. Brassard proposed the BB84 protocol. The use of «entangled» quanta for systems with quantum key distribution was offerred in 1991 by A. Eckert. All modern quantum cryptography systems are based on these above-mentioned protocols.

Keywords: *data transfer, cryptography, quantum key distribution, polarization, BB84, B92, E91, BBM92 encryption protocols (algorithms), entangled quanta*

DOI: 10.18469/ikt.2023.21.1.09

Vasin Nikolay Nikolayevich, Povolzhskiy State University of Telecommunications and Informatics, 23, L. Tolstoy Street, Samara, 443010, Russian Federation; Professor of Networks and Communication Systems Department, Doctor of Technical Sciences, Professor. Tel. +7 917 103-05-44. E-mail: vasin-nn@psuti.ru

References

1. Olifer V.G., Olifer N.A. *Computer networks. Principles, technologies, protocols: Textbook for Universities*. Saint Petersburg: Peter, 2016, 992 p. (In Russ.)
2. Information security administrator. Basics of cryptography. URL: https://intuit.ru/studies/mini_mba/5398/courses/547/lecture/12387 (accessed: 29.09.2023). (In Russ.)
3. Semenov Yu.A. Telecommunications and information technologies. 6.9. Quantum cryptography. URL: http://book.itep.ru/6/q_crypt.htm (accessed: 29.09.2023). (In Russ.)
4. Wiesner S. Conjugate Coding. *ACM SIGACT News*, 1983, vol. 15, no. 1, pp. 78–88. DOI:10.1145/1008908.1008920
5. Bennett C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of International Conference on Computers, Systems & Signal Processing*. India, Bangalore, 1984, pp. 175–179.

6. Bennett C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. *ACM SIGACT News*, 1987, vol. 18, no. 4, pp. 51–53. DOI:10.1145/36068.36070
7. BB84 – Vikipediya. URL: https://ru.wikipedia.org/wiki/BB84 (accessed: 29.09.2023). (In Russ.)
8. InfoTEX ViPNet QSS quantum phone. URL: https://www.tadviser.ru/index.php/Продукт:ИнфоТеКС_ViPNet_QSS_Phone_квантовый_телефон (accessed: 02.10.2023). (In Russ.)
9. Lopes M., Sarwade N. Cryptography from quantum mechanical viewpoint. *International Journal on Cryptography and Information Security (IJCIS)*, 2014, vol. 4, no. 2, pp. DOI:10.5121/ijcis.2014.4202 13
10. Slepov N.N. Quantum cryptography: transmission of a quantum key. Problems and solutions. Electronics: Science, Technology, Business. URL: https://www.electronics.ru/files/article_pdf/0/article_705_722.pdf (accessed: 01.10.2023). (In Russ.)
11. Radko N.M., Mokrousov A.N. *Cryptographic protocols: Textbook*. Voronezh: Voronezhskij gosudarstvennyj tekhnicheskij universitet, 2006, 104 p. (In Russ.)
12. Slepov N.N. *Modern technologies of digital fiber optic communication networks*. Moscow: Radio i svyaz', 2003, 468 p. (In Russ.)
13. Charles H. Bennett. Quantum Cryptography Using Any Two Nonorthogonal States. *Physical Review Letters*, 1992, vol.68, no. 21, pp. 3121–3124.
14. Protocol B92. URL: https://ru.wikipedia.org/wiki/B92 (accessed: 29.09.2023). (In Russ.)
15. Quantum cryptography. URL: https://ru.wikipedia.org/wiki/Квантовая_криптография (accessed: 29.09.2023). (In Russ.)
16. Strong quantum encryption is the future of information security. URL: https://integral-russia.ru/2016/06/10/stojkoe-kvantovoe-shifrovanie-budushhee-informatsionnoj-bezopasnosti/ (accessed: 29.09.2023). (In Russ.)
17. Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 1991, vol. 67, no. 6, pp. 661–663.
18. Protocol E91. URL: https://ru.frwiki.wiki/wiki/Protocole_E91 (accessed: 26.09.2023). (In Russ.)
19. Quantum key distribution protocol using EPR. URL: https://ru.wikipedia.org/wiki/Протокол_квантового_распределения_ключей_с_использованием_ЭПР (accessed: 26.09.2023). (In Russ.)
20. A Survey of the Prominent Quantum Key Distribution Protocols. URL: https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/ (accessed: 29.09.2023).
21. Charles H.B., Gilles B. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 2014, vol. 560, no.1, pp. 7–11.
22. BBM92 – quantum encryption protocol. URL: https://ru.wikipedia.org/wiki/BBM92 (accessed: 29.09.2023). (In Russ.)
23. Scarani V. et al. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Physical Review Letters*, 2004, vol. 92, no. 5, pp. 057901. DOI: 10.1103/PhysRevLett.92.057901
24. SARG04 – quantum key distribution protocol. URL: https://ru.wikipedia.org/wiki/SARG04 (accessed: 26.09.2023). (In Russ.)
25. Protocol Lo05. URL: https://flirt24.ru/stati/14648-lo05.html (accessed: 26.09.2023). (In Russ.)
26. Systems for quantum-optical cryptographic communications. Special systems. Photonics. URL: https://sphotonics.ru/solutions/quantum-cryptography/ (accessed: 26.09.2023). (In Russ.)
27. Popov S.A. Quantum communications come to the fore. *Pervaya milya*, 2003, no.5, pp. 34–39. DOI: 10.22184/2070-8963.2023.113.5.34.39. (In Russ.)
28. Alekseev A.L. Developments of SMARTS-Quanttelecom LLC in the field of quantum communications. Quantum cryptographic systems for key generation and distribution. URL: https://www.smarts.ru/media/filer_public/9b/68/9b687732-ac4f-4331-8b56-03355411f6ba/smarts_kvanttelekom.pdf (accessed: 26.09.2023). (In Russ.)

29. Scientists from ITMO University proposed a modification of the quantum encryption system with a compact detector. URL: https://news.itmo.ru/ru/news/9580/ (accessed: 29.09.2023). (In Russ.)
30. Quantum communications to protect communication lines. URL: https://www.smarts.ru/media/filer_public/a8/a0/a8a034b5-bdb6-4762-8c7b-b1778019c77c/22.pdf (accessed: 29.09.2023). (In Russ.)
31. Quantum cryptography / encryption. URL: https://www.tadviser.ru/index.php/Статья:Квантовая_криптография_(шифрование). (accessed: 29.09.2023). (In Russ.)
32. ViPNet QSS (Quantum Security System). URL: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:ViPNet_QSS_(Quantum_Security_System) (accessed: 29.09.2023).
33. Gusev D. Quantum products Info-TeKS. Quantum technology and security. URL: https://infotecstechfest.ru/upload/iblock/20f/tvtc2bzrgt8sr9fk27myjwo1o4yudjww.pdf (accessed: 29.09.2023). (In Russ.)
34. The first experimental quantum network in Russia. URL: https://mtuci.ru/about_the_university/news/4813/ (accessed: 29.09.2023). (In Russ.)
35. MTUSI implemented wireless quantum communication based on serial domestic equipment. URL: https://naked-science.ru/article/column/v-mtusi-realizovali-besprovodnuyu-kvantovuyu (accessed: 29.09.2023). (In Russ.)

Received 02.10.2023

ТЕХНОЛОГИИ РАДИОСВЯЗИ, РАДИОВЕЩАНИЯ И ТЕЛЕВИДЕНИЯ

УДК 543.42

ОПРЕДЕЛЕНИЕ ПОРОГОВОГО РЕШЕНИЯ ДЛЯ КАНАЛА С РЕЛЕЕВСКИМИ ЗАМИРАНИЯМИ ПРИ ЗОНДИРОВАНИИ СПЕКТРА КОГНИТИВНОГО РАДИО ЭНЕРГЕТИЧЕСКИМ ДЕТЕКТОРОМ

Елисеев С.Н.[1], Степанова Н.В.[2]
[1]Московский технический университет связи и информатики, Москва, РФ
[2]Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: fgupnrsnr@yandex.ru, puhleniw@mail.ru

Характеристики систем зондирования спектра и обнаружение занятости полос спектра в когнитивном радио являются одними из основных аспектов исследования. В случае, когда рассматривается система, в которой первичный пользователь меняется или присутствуют первичные пользователи нескольких типов, используют энергетический детектор. Для работы энергетического детектора основными параметрами, которые определяют вероятностные характеристики обнаружения (вероятность обнаружения пользователя, вероятность ошибки вида «ложная тревога» и вероятность ошибки вида «пропуск цели») будут зависеть от правильного определения порога решений. В данной статье просматривается аналитический подход к определению нормированного порога решений. Цель – проанализировать и определить оптимальное значение порога решений для энергетического детектора в канале с релеевскими замираниями. Рассмотрена система зондирования спектра в когнитивном радио. Определены нормированные величины порогового решения для канала с релеевскими замираниями. Представлены графические иллюстрации результатов анализа и вычислений. Полученные результаты определения пороговых решений являются хорошим приближением для расчета характеристик систем зондирования в когнитивном радио в каналах с релеевскими замираниями, обеспечивая возможность с большей вероятностью определить полосы частот, свободные от первичных пользователей, за счет чего повышается эффективность использования радиочастотного спектра.

Ключевые слова: *зондирование спектра, когнитивное радио, Релеевские замирания, энергетический детектор, оптимальная величина порога*

Введение

Рост запросов на беспроводные услуги за последние несколько лет иллюстрирует огромный и постоянно растущий спрос бизнес-сообщества, населения и государства. С ростом коммуникационных приложений спектр становится все более перегруженным. Существующая система назначает разные полосы частот различным пользователям или поставщикам услуг, а для работы в этих полосах необходимо наличие лицензий.