DOI: 10.17725/rensit.2024.16.255

Ключевые особенности протоколов квантового распределения ключей на непрерывных переменных

Бурлаков Е.В., Коробов А.В.
Московский технический университет связи и информатики, https://mtuci.ru/
Москва 111024, Российская Федерация
E-mail: e.v.burlakov@mtuci.ru, a.v.korobov@mtuci.ru

Поступила 08.11.2023, рецензирована 15.11.2023, принята 22.11.2023, опубликована 25.04.2024

Представлена действительным членом РАЕН А.С. Дмитриевым

Аннотация: **В работе рассмотрены ключевые особенности протоколов квантового распределения ключей на непрерывных переменных. Обоснована мотивация изучения и разработки методов квантовой криптографии. Выделены основные моменты, присущие протоколам на непрерывных переменных, и проведена их классификация по различным признакам, особенностям и вариантам реализации. Подробно рассмотрен пример протокола с дискретной модуляцией и регистрацией сигнала по средствам балансного гомодинного детектирования. Приведена классификация атак на квантовый протокол. Дана общая характеристика методам постобработки. Обозначена роль шумов, и рассмотрены подходы к оценке уровня секретности, которые применимы для протоколов на непрерывных переменных. В заключении приведены основные выводы касательно текущего статуса данной проблемы, а также определены аспекты, которые требуют дальнейшего изучения.**

Ключевые слова: **квантовая информатика, квантовая криптография, квантовое распределение ключей, непрерывные переменные, гомодинное детектирование**

PACS: 03.67.Dd, 42.50.Dv, 89.70.+c

Для цитирования: Бурлаков Е.В., Коробов А.В. Ключевые особенности протоколов квантового распределения ключей на непрерывных переменных. *РЭНСИТ: Радиоэлектроника. Наносистемы. Информационные технологии,* 2024, 16(2):255-266. DOI: 10.17725/rensit.2024.16.255.

Key features of continuous-variable quantum key distribution protocols

Evgenii V. Burlakov, Alexander V. Korobov
Moscow Technical University of Communications and Informatics, https://mtuci.ru/
Moscow 111024, Russian Federation
E-mail: e.v.burlakov@mtuci.ru, a.v.korobov@mtuci.ru

Received November 08, 2023, peer-reviewed November 15, 2023, accepted November 22, 2023, published April 25, 2024

Abstract: **The key features of continuous variables quantum key distribution protocols are considered in the paper. The motivation for studying and developing methods of quantum cryptography is substantiated. The main aspects inherent to continuous-variable protocols are highlighted, and they are classified based on various characteristics, peculiarities, and implementation variants. A detailed examination of a protocol example with discrete modulation and signal registration through balanced homodyne detection is provided. A classification of attacks on the quantum protocol is presented. A general overview of post-processing methods is given. The role of noise is indicated, and approaches to assessing the level of security applicable to continuous-variable protocols are discussed. In conclusion, the main conclusions regarding the current status of this problem are presented, and aspects requiring further study are identified.**

Keywords: **quantum information, quantum cryptography, quantum key distribution, continuous variables, homodyne detection**

PACS: 03.67.Dd, 42.50.Dv, 89.70.+c
For citation: Evgenii V. Burlakov, Alexander V. Korobov. Key features of continuous-variable quantum key distribution protocols. *RENSIT: Radioelectronics. Nanosystems. Information Technologies*, 2024, 16(2):255-266e. DOI: 10.17725/j.rensit.2024.16.255.

Содержание

1. ВВЕДЕНИЕ

В наше время происходит такое стремительное развитие квантовых технологий, которое можно назвать второй квантовой революцией [1, 2]. Действительно, многие из фундаментальных свойств квантовой механики, такие как квантовая запутанность [3], телепортация [4], теорема о запрете копирования [5], получили экспериментальную проверку и легли в основу идей, которые могут быть использованы для практических целей. В то же время, мы живем в век информационных технологий, информация, в том или ином виде, все больше входит в нашу повседневную жизнь. Естественным образом возникает процесс слияния квантовых технологий и информатики, появляется такая область науки как квантовая информатика [6, 7]. Одним из разделов квантовой информатики является квантовая криптография [8-11]. На протяжении всей своей истории человечество искало конфиденциальный способ обмениваться информаций, с течением времени актуальность этой проблемы только возрастает. Сейчас без криптографии не мыслимо функционирование армии, правительства и банковской сферы.

Известно, что, чтобы достичь теоретически защищенной коммуникации, достаточно использовать метод одноразового блокнота (шифр Вернама) [12]. Этот метод частично сводит проблему обмена секретными сообщениями к проблеме распределения секретного ключа, которым кодируются сообщения, передаваемые между двумя абонентами. В настоящее время чаще всего используются классические алгоритмы шифрования для распределения секретного ключа [13]. Надежность большинства таких алгоритмов математически не доказана и основывается на том, что на сегодняшний день пока не существует классического эффективного алгоритма факторизации больших чисел [14]. Поэтому в будущем, после возможного создания эффективных алгоритмов факторизации больших чисел или достаточно мощных квантовых компьютеров [15], от современных методов классического распределения ключей придется отказаться.

Идея квантовой криптографии направлена на решение проблемы распределения секретного ключа таким образом, что безопасность ключа будет гарантироваться законами квантовой механики, тем самым секретность обеспечивается на уровне фундаментальных законов природы. Протокол квантового распределения ключей BB-84 [16] опирается на квантово-механическую теорему о запрете копирования неизвестного квантового состояния [5]. Протокол устроен таким образом, что любая попытка подслушивателя (Ева) перехватить информацию о ключе всегда может быть обнаружена при определенных согласованных действиях пользователей, распределяющих ключ (Алиса и Боб). BB-84 был исторически первым протоколом квантового распределения ключей и до сих пор остается одним из самых надежных протоколов. Однако исследования в этом направлении ведутся непрерывно, позже были предложены другие протоколы квантовой криптографии: E-91 [17], B-92 [18], GG-02 [19], Lo-05 [20], со своими уникальными особенностями. Отдельного

внимания заслуживают протоколы на так называемых непрерывных переменных (*CV QKD*) [19,21]. Целью данной работы является обобщить результаты научных исследований по ключевым особенностям протоколов квантового распределения ключей на непрерывных переменных, обосновать необходимость дальнейшего изучения и разработки данной проблемы, а также определить те ее аспекты, которые требуют дальнейшего изучения.

2. ОСОБЕННОСТИ И ВАРИАНТЫ ПРОТОКОЛОВ НА НЕПРЕРЫВНЫХ ПЕРЕМЕННЫХ

К началу 2000-х годов стало ясно, что для целей квантовой криптографии можно использовать методы, при которых информация о секретном ключе кодируется в значение комплексной амплитуды (амплитуды и фазы) оптического поля (*CV QKD*) [19,21-23]. Данная величина является непрерывной квантовой переменной, то есть при измерении дает величину, непрерывно меняющуюся в определенном интервале значений. В этом состоит отличие непрерывной квантовой переменной от кубита [6], результаты измерения которого образуют дискретный спектр. Для непрерывных переменных так же, как и для дискретных переменных справедлива теорема о запрете копирования неизвестного квантового состояния, что также является фактором, лежащим в основе секретности подобных протоколов [24].

По сравнению с протоколами КРК на дискретных переменных, протоколы на непрерывных переменных экспериментально реализуются несколько реже. Причиной этого служат возникающие сложности с обоснованиями секретности [24], особенно для протоколов с так называемой негауссовой модуляцией, а также чувствительность реализаций протокола к всевозможным шумам [25]. Однако *CV QKD* имеет несколько привлекательных особенностей, которых нет у протоколов на дискретных переменных. В *CV QKD* применяются многофотонные лазерные импульсы (порядка 250 фотонов в импульсе) [21], что благоприятно сказывается на скорости генерации секретного ключа, кроме того не требуется применение источника [26-28] и детектора [29] одиночных фотонов, которые являются коммерчески дорогими и на сегодняшних день пока несовершенными для нужд квантового распределения ключей (КРК).

Все большее число исследователей обращают свое внимание на протоколы семейства *CV QKD*. Уже были реализованы протоколы *CV QKD* в оптоволокне [30], в свободном пространстве [31], по схеме реализации в однопроходном [19] и двухпроходном вариантах [32]. Так же были реализованы варианты *CV QKD* с локальным осциллятором (опорным сигналом) доступным только на стороне получателя (дважды локальный осциллятор) [33]. Такой вариант схемы значительно повышает надежность протокола. По типу модуляции протоколы *CV QKD* делятся на протоколы с гауссовой [19] модуляцией и протоколы с дискретной модуляцией [34]. Протоколы с гауссовой модуляцией сложнее в реализации, но для них обоснована секретность против атак общего типа (когерентных атак) [35]. Протоколы с негауссовой модуляцией часто имеют более простую техническую реализацию и алгоритмы постобработки, но для них возникают сложности с обоснованиями секретности. В качестве сигнальных состояний чаще всего используются когерентные состояния оптического поля, но могут быть использованы также сжатые [36] и тепловые состояния [37]. Специфической частью для протоколов *CV QKD* является процедура балансного гомодинного детектирования [38]. Существуют варианты *CV QKD* в которых эта процедура заменена на процедуру гетеродинирования [38], что не только благоприятно сказывается на скорости генерации секретного ключа, но позволяет отказаться от источника генерации случайных [39,40] или псевдослучайных чисел на стороне получателя.

3. ОПИСАНИЕ МЕТОДА БАЛАНСНОГО ГОМОДИННОГО ДЕТЕКТИРОВАНИЯ

Как было отмечено выше, проведение балансного гомодинного детектирования является важной и специфической частью протоколов *CV QK*D, поэтому эту процедуру имеет смысл описать отдельно. Лазерное поле с высокой степенью точности может быть

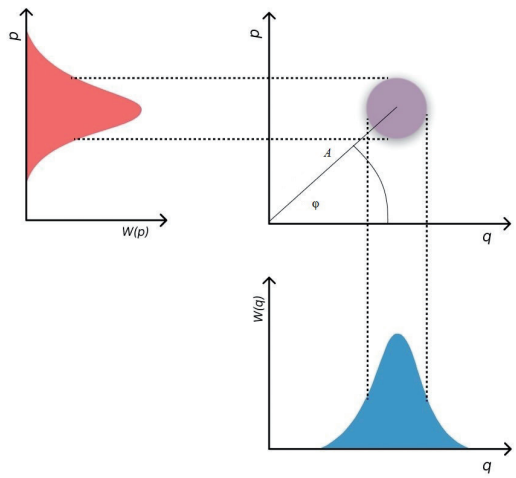

Рис. 1. *Наглядное представление комплексной амплитуды сигнального когерентного состояния* $|\alpha\rangle$. *Конец вектора амплитуды окружен "кругом неопределенностей", это отражает факт, присутствия неустранимого квантового шума.*

описано когерентным состоянием $|\alpha\rangle$, где $a = A\exp(i\varphi) = q + ip$ комплексный параметр кодирующий амплитуду и постоянную (начальную) компоненту фазы оптического сигнала. Данные характеристики однозначным образом могут быть пересчитаны в квадратурные компоненты сигнала: "координату" q и "импульс" p [22]. Эти величины получили такое название потому, что при квантовом рассмотрении электромагнитного поля, они имеют такое же (с точностью до константы) коммутационное соотношение, как и операторы координаты и импульса квантово-механической частицы: $[\hat{q}, \hat{p}] = i$. Это в свою очередь означает, что для них справедлив принцип неопределенности Гейзенберга, то есть определенное соотношение на дисперсии этих величин (**Рис. 1**). "Координата" q и "импульс" p сигнального состояния могут быть экспериментально измерены следующим образом [22]: сигнальное состояние подвергается интерференции со вспомогательным пучком, той же частоты (локальным осциллятором, гомодином), на симметричном светоделителе. Затем, каждый из выходных пучков светоделителя попадает

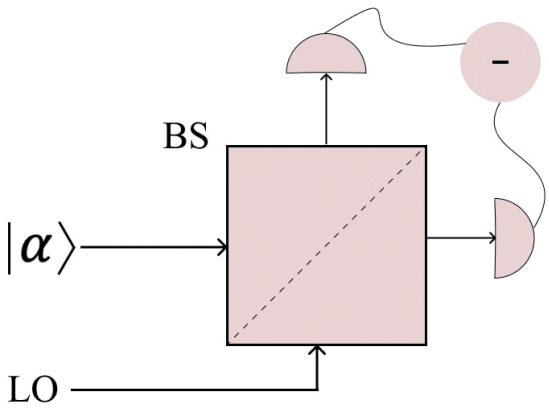

Рис. 2. *Сигнальное когерентное состояние* $|\alpha\rangle$ *смешивается на симметричном свето-делителе с опорным оптическим полем (гомодином, локальным осциллятором), результирующие пучки падают на фотодиоды гомодинного детектора, который трансформирует падающее излучение в разностный фототок.*

на фотодиоды гомодинного детектора (**Рис. 2**). Можно показать, что, в зависимости от разности фаз между сигналом и гомодином θ, результирующий разностный фототок I пропорционален либо "координате" q, либо "импульсу" p, либо их комбинации:

$$I \sim q\cos\theta + p\sin\theta. \quad (1)$$

Данный фототок I усиливается в детекторе и трансформируется в выходное напряжение, передаваемое на осциллограф. Данные с осциллографа обрабатываются, и восстанавливается информация о квадратурах. Таким образом, регулируя на своей стороне разность фаз θ между сигналом и гомодином (опорным сигналом, локальным осциллятором), Боб фактически выбирает какую квадратуру ему предстоит измерять. Описанная схема детектирования, используется не только для *CV QKD*, но и для проведения, так называемой квантовой томографии [41], восстановлении квантового состояния по данным гомодинирования. Так, например, квадратурные компоненты являются аргументами функции Вигнера $W(q,p)$ [42-45] – важного объекта квантовой оптики, представляющего собой функцию квази-распределения.

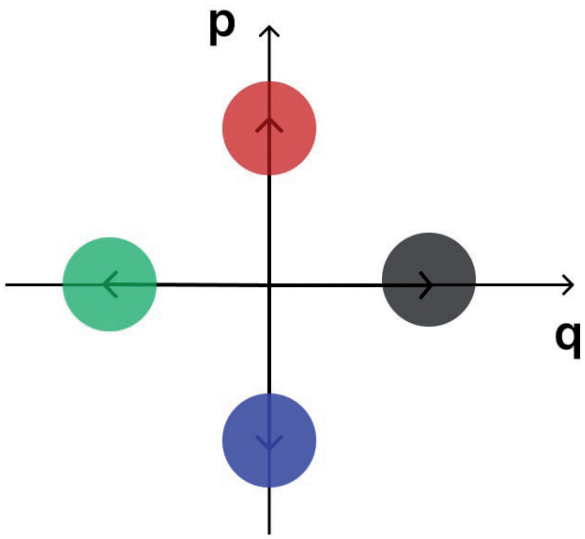

Рис. 3. *Визуализация первого и второго пункта протокола с помощью метода векторных диаграмм. Алиса готовит одно из четырех состояний в каждой посылке.*

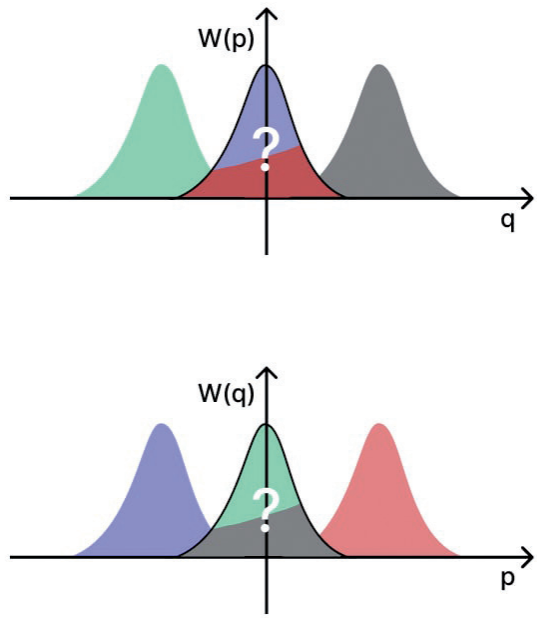

Рис. 4. *Визуализация третьего пункта протокола. Боб применяя метод балансного гомодинного детектирования проецирует полученное состояние на вертикальную или горизонтальную ось, измеряя либо "координату" q либо "импульс" p.*

4. ОПИСАНИЕ ПРОТОКОЛА CV QKD С ДИСКРЕТНОЙ МОДУЛЯЦИЕЙ

Ниже представлен вариант протокола *CV QKD* с дискретной модуляцией с использованием когерентных состояний, детектирование предполагается гомодинным. Такой вариант протокола, как правило, имеет более простую техническую реализацию по сравнению с протоколами с гауссовой модуляцией, и в то же время отражает многие важные моменты квантового распределения ключей на непрерывных переменных. Кроме того, на его примере лучше всего прослеживается аналогия с известным протоколом BB-84, особенно, если пользоваться методом визуализации в виде векторных диаграмм (**Рис. 3, 4**).

Типичная схема реализации протокола *CV QKD* с дискретной модуляцией, выглядит следующим образом [11]:

1. Отправитель (Алиса) генерирует случайную комплексную величину $|\alpha\rangle$, где $a = A\exp(i\varphi) = q + ip$ – фиксированный параметр, φ может принимать одно из четырех значений: $\varphi = \{0, \pi/2, \pi, 3\pi/2\}$. Причем, значения $\varphi = \{0,\pi\}$ кодируют "координату" q, а значения $\varphi = \{\pi/2, 3\pi/2\}$ кодируют "импульс" p.

2. Алиса повторяет пункт 1 несколько раз, то есть генерирует набор комплексных параметров $\{\alpha\}$. На основе этого набора, поочередно, создает и отправляет получателю (Бобу) когерентные состояния $\{|\alpha\rangle\}$ в виде отдельных посылок (лазерных импульсов).

3. Боб, пользуясь методом балансного гомодинного детектирования, в каждой посылке производит измерение одной из двух квадратурных компонент: "координаты" q или "импульса" p. Иными словами регулирует по своему усмотрению разность фаз между сигналом и гомодином θ. Согласно формуле (1), $\theta = 0$ соответствует измерению "координаты", а $\theta = \pi/2$ измерению "импульса". Результаты измерения составляют сырой ключ Боба.

4. Боб по открытому каналу сообщает Алисе, какую переменную: "координату" q или "импульс" p он измерил в каждой посылке, не сообщая ее конкретного значения. Предполагается, что до начала процедуры распределения ключа Алиса и Боб синхронизировали фазы сигналов и четко знают, что принимается за "координату" q, а что за "импульс" p.

5. Алиса использует информацию, полученную от Боба для получения своего "сырого" ключа,

отбрасывая те значения последовательности случайных величин, при измерении которых Боб ошибся с выбором фазы. Например, в посылке кодировалась "координата" q, а Боб измерял "импульс" p.

6. Алиса формирует бинарный ключ. Оставшимся после проведения предыдущего пункта посылкам со значениями $\varphi = \{0,\pi/2\}$ ставит в соответствие 1, а посылкам со значениями $\varphi = \{\pi, 3\pi/2\}$ ставит в соответствие 0.

7. Боб анализирует среднее значение фототока, полученное в результате гомодинирования каждой конкретной посылки из набора, полученного от Алисы. Если оно положительно и соответствует величине A, то ставит в соответствие этой посылке 1, если отрицательно и соответствует величине $-A$, то ставит в соответствие 0. Если средняя величина фототока близка к нулю, то это означает, что Боб не угадал базис, и такие посылки отбрасываются.

Если Боб замечает, что средняя величина фототока I имеет некое промежуточное значение, не соответствующее, ни A, ни $-A$, ни 0, и наблюдается рост дисперсии фототока, то это может означать, что канал связи прослушивается злоумышленником (Евой).

Ключевое отличие протоколов с гауссовой модуляцией заключается в том, что комплексные числа $a = A\exp(i\varphi) = q + ip$, которые генерирует Алиса, могут принимать не четыре разных значения, а генерируются согласно двумерному гауссовому распределению с центром в начале координат и дисперсией V_A. Тогда результирующая дисперсия квадратур с учетом квантового шума в соответствующих единицах равна $V = V_A + 1$.

Предложенный протокол не требует ни источника, ни детектора одиночных фотонов. В качестве источника излучения при реализации протокола в оптоволокне обычно используются лазеры, генерирующие излучение с длиной волны 1550 нм. [46]. В качестве устройства детектирования используются балансные гомодинные детекторы с недорогими фотодиодами на основе кремния или арсенида галлия [47]. Предложенная выше схема носит лишь принципиальный характер и не учитывает некоторые особенности, которые возникают при технической реализации. К таким особенностям можно отнести: устройство локального осциллятора (гомодина), учет шумов и потерь в канале связи и в детекторе, поляризационные искажения сигнала, особенности работы амплитудных и фазовых модуляторов оптического поля, стабилизация видности интерференционной картины. За подробностями по этим и некоторым другим вопросам следует обратиться к списку литературы [25].

5. КЛАССИФИКАЦИЯ АТАК НА КВАНТОВЫЙ ПРОТОКОЛ

Классификация атак может быть проведена несколькими способами [11]. Злоумышленник (Ева) может проводить атаки на протокол или атаки на его техническую реализацию. Атаки на протокол могут быть в свою очередь поделены на две группы, *косвенные:* с использованием Евой вспомогательной квантовой системы, называемой анциллой (ancilla), и *прямые*: без использования анциллы. Атаки с использованием анциллы делятся на три типа: *индивидуальные, коллективные и когерентные.* При проведении *индивидуальных атак* Ева заготавливает несколько вспомогательных квантовых систем (анцилл), каждая анцилла взаимодействует с соответствующим квантовым состоянием Алисы (или Боба), которое непосредственно переносит информацию о ключе. В более поздние моменты времени Ева проводит измерения над каждой анциллой в отдельности и получает некую информацию о секретном ключе. В случае *коллективной атаки* также каждая анцилла взаимодействует с определенной информационной квантовой системой, однако Ева проводит коллективное измерение над всеми анциллами сразу, это позволяет ей получить большую информацию, чем в случае индивидуальных измерений. К третьему типу возможных атак относится *когерентная атака,* эта самый общий тип атак, при котором анцилла Евы представляет, вообще говоря, многоуровневую квантовую систему, которая взаимодействует со всеми информационными состояниями сразу, после

чего Ева производит измерения над свой анциллой в подходящий для нее момент времени. В некоторых случаях удается показать эквивалентность коллективных и когерентных атак, в общем же случае далеко не всегда удается явно построить когерентную атаку или указать максимальную величину информации, которую получит Ева в результате такой атаки. Анализ индивидуальных и коллективных атак, как правило, значительно проще, кроме того позволяет ответить на вопрос секретен ли протокол в принципе, то есть выполняет роль необходимого условия секретности.

6. ОПИСАНИЕ МЕТОДОВ ПОСТОБРАБОТКИ

Как и во всех квантовых протоколах, в *CV QKD* необходимо проводить классическую пост-обработку: данные, полученные в результате квантовой части протокола должны быть классическим образом обработаны для получения окончательного секретного ключа. Классическая постобработка включает в себя [11] несколько этапов: *просеивание ключа* – Алиса и Боб отбрасывают те посылки, в которых не удалось угадать базисы друг друга. *Оценка параметров* – Алиса и Боб публично раскрывают часть ключа для оценки таких параметров как потери в канале связи и дополнительный шум, эти величины необходимы для подсчета величины взаимной информации между Алисой и Бобом и величины Холево [7]. *Согласование информации* – Алиса и Боб используют классические алгоритмы согласования информации, для проверки успешности предыдущих пунктов. К числу таких алгоритмов можно отнеси Слайс-согласование [48], Мульти-размерное согласование [49], LDPC-коды [50]. Также различают *прямое* и *обратное* согласование, в случае *CV QKD* обратное согласование предпочтительнее. *Подтверждение* – на данном этапе, как правило применяют к ключу семейство универсальных хэш-функций, для того чтобы убедится, что коррекция ошибок удалась. *Усиление секретности* – Алиса и Боб проводят процедуру хэширования для равномерного сжатия ключа и получения окончательного секретного ключа. *Аутентификация* – на каждом из этапов, приведенных выше Алиса и Боб должны быть уверены, что осуществляют обмен информацией друг с другом, а не с третьей стороной, которая может для Алисы играть роль Боба, а для Боба играть роль Алисы.

7. РОЛЬ ШУМОВ В РЕАЛИЗАЦИИ CV QKD

Учет уровня шума в каналах связи и в аппаратуре играет очень важную роль во всех протоколах квантовой криптографии, так как потенциально в шумах скрыта полезная для Евы информация. Априори считается, что Ева располагает всеми необходимыми ресурсами для извлечения интересующей ее информации из доступных ей шумов. В *CV QKD* роль шума выходит на еще более высокий уровень, неустранимый квантовый шум не позволяет Еве остаться незамеченной, но влияние шумов другой природы должно быть сведено к минимуму. К дополнительным шумам относятся: шум неидеальности системы *QKD* [25], шум утечки в детекторе χ_{det}, шум перекрытия из-за неидеальной видности интерференционной картины, шум нестабильности по интенсивности сигнала и локального осциллятора χ_{Lo}, шум неидеальности модуляции, шум рамановского рассеяния χ_{Ram}, шум дискретизации измерений. Если шумы стохастически независимы, то их дисперсии складываются:

$$\chi = \chi_{det} + \chi_{Lo} + \chi_{Ram}. \quad (2)$$

С точки зрения векторных диаграмм (Рис. 1), дополнительный шум складывается с квантовым шумом, что эффективно увеличивает круг неопределенностей.

Дополнительные шумы часто классифицируют на те, к которым Ева имеет доступ, и те, к которым Ева доступ не имеет. Например, выделяется “оригинальная” (ORM) и “улучшенная” (RRM) реалистичные модели учета шумов [38]. Подобные классификации позволяют облегчить анализ секретности в некоторых случаях. Так, например, не кажется слишком грубым допущением, считать, что Ева не имеет доступ к локальному осциллятору, в том случае, если он полностью на стороне Алисы и не подлежит передаче [25]. Однако условность таких классификаций несколько ограничивает полученные выводы.

8. ОБОСНОВАНИЯ СЕКРЕТНОСТИ

Пусть N – число посылок, которые Алиса и Боб распределяют между собой в результате квантовой части протокола. После того, как Алиса и Боб производят процедуру согласование базисов, они получают список символов длиной $n \leq N$, который называется сырой ключ. После проведения классической постобработки Алиса и Боб сжимают секретный ключ и получают окончательный секретный ключ длины $l \leq n$. Можно рассмотреть случай, когда число посылок стремится к бесконечности, так называемый ассимптотический режим, и ввести величину r, которую в англо-язычной литературе называют "секретная дробь" (secret fraction) или относительная скорость ключа [11]:

$$r = \lim_{N\to\infty} \frac{l}{n}. \tag{3}$$

Величина (3) фигурирует во многих доказательствах секретности квантовых протоколов. Также вводятся такие параметры как скорость генерации сырого ключа R, которую можно оценить экспериментально, то есть число символов сырого ключа, которое может быть сгенерировано системой КРК за единицу времени. Аналогично вводится величина $K = Rr$ – скорость генерации секретного ключа.

В случае индивидуальной атаки для величины справедлива формула Цисара-Кернера [51]:

$$r^{\infty}_{Shannon} = I_{AB} - I_{BE}, \tag{4}$$

где I_{AB} взаимная информация Алисы и Боба в смысле Шеннона [52], доля общих секретных бит, которыми располагают Алиса и Боб. Данный параметр может быть точно вычислен на этапе обратного согласования, если согласование не идеальное, что чаще всего бывает на практике, величину I_{AB} нужно заменить на βI_{AB}, где $\beta < 1$ параметр неидеальности согласования. Аналогично определяется взаимная информация между Алисой и Евой I_{AE}, а также Бобом и Евой I_{BE}. Для случая *CV QKD* предпочтительнее обратное согласование, поэтому в формуле (4) фигурирует I_{BE}. Для случая прямого согласования следует использовать I_{AE} вместо I_{BE}.

Для протокола *CV QKD* с гауссовой модуляцией данные величины равны [53]:

$$\begin{aligned} I_{AB} &= \frac{1}{2}\log_2 \frac{V+\chi}{1+\chi}, \\ I_{BE} &= \frac{1}{2}\log_2 \left((\eta T)^2 (V+\chi)(V^{-1}+\chi)\right), \end{aligned} \tag{5}$$

где $V = V_A + 1$, где V_A – дисперсия гауссовой модуляции Алисы, χ – поправка, учитывающая влияние дополнительных шумов (2), η – квантовая эффективность детектора, T – потери в линии передачи. Выражение для I_{BE} – может отличаться от (5), эта величина зависит от модели дополнительных шумов и от допустимых действий Евы, которые диктуются выбранной моделью [53].

В случае коллективной атаки для величины r справедлива формула Деветака-Винтера [54]:

$$r^{\infty}_{Holevo} = I_{AB} - I_{BE},$$

где χ_{BE} – величина Холево [7] – фундаментальная граница информации, которая может быть получена Евой, эта величина достигается при квантовых коллективных измерениях. Величина Холево может быть вычислена после рассмотрения эквивалентной ЭПР-версии протокола с помощью симплектических собственных значений матрицы ковариаций γ_{AB} Алисы и Боба, в моменты до (γ_{AB}) и после ($\gamma_{A|B}$) проективных измерений Боба. Матрица ковариаций, в свою очередь, также выражается через параметры протокола [55]. Тогда для величины Холево имеем:

$$\begin{aligned} &\chi_{BE} = G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right) - G\left(\frac{\lambda_4 - 1}{2}\right), \\ &G(x) = (x+1)\log_2(x+1) - (x)\log_2(x), \\ &\lambda_{1,2} = \frac{1}{2}[A \pm \sqrt{A^2 - 4B}], \\ &\lambda_{3,4} = \frac{1}{2}[C \pm \sqrt{C^2 - 4D}], \end{aligned} \tag{6}$$

где

$$\begin{aligned} A &= V^2(1-2T) + 2T + T^2(V + \chi_{line})^2, \\ B &= T^2(\chi_{line} + 1)^2, \end{aligned}$$

$$C = \frac{V\sqrt{B} + T(V + \chi_{line}) + A\chi_{\text{hom}}}{T(V + \chi_{tot})},$$

$$D = \sqrt{B}\frac{V + \sqrt{B}\chi_{\text{hom}}}{T(V + \chi_{tot})}.$$

Выражение для χ_{BE} также может отличаться от (6) в зависимости от выбранной модели шумов и возможностей Евы. Приведенное выше выражение (6) построено для так называемой "реалистичной" модели [55], для которой:

$$\chi_{tot} = \chi_{line} + \chi_{\text{hom}} / T,$$

$$\chi_{\text{hom}} = \frac{1 + v_{el}}{\eta} - 1,$$

$$\chi_{line} = \frac{1}{T} - 1 + \varsigma,$$

где ν_{e1} – электронный шум в детекторе, ς – дополнительный шум в линии передачи.

Существуют указания на то, что для *CV QKD* когерентная атака не дает никакой новой информации Еве по сравнению с коллективной [24].

Существуют другие подходы к оценке секретности, например, эпсилон-критерий Реннера [56], основанный на понятии следового расстояния:

$$\frac{1}{2}\left\|\rho_{S_A S_B E} - \tau_{SS} \otimes \rho_E\right\| \le \varepsilon,$$

где $\rho_{S_A S_B E}$ – матрица плотности Алисы, Боба и Евы, полученная после сеанса распределения ключей. S_A, S_B – окончательные ключи Алисы и Боба, индекс E обозначает квантовый регистр Евы, τ_{SS} – матрица плотности, соответствующая равномерному распределению ключа длины l. ρ_E – матрица плотности Евы, которая факторизована относительно системы Алисы и Боба и не коррелирует с ней. Критерий имеет прозрачную интерпретацию, матрица $\tau_{SS} \otimes \rho_E$ отражает некий идеальный результат квантового распределения ключей, а матрица $\rho_{S_A S_B E}$ реальную ситуацию, чем "ближе" реальная ситуация к идеальной, тем лучше для Алисы и Боба. Данный критерий справедлив в случае произвольной атаки Евы и не опирается на асимптотический характер генерации ключа.

9. ЗАКЛЮЧЕНИЕ

Таким образом, потенциал протоколов на непрерывных переменных достаточно высокий и может быть раскрыт на современном уровне развития технологий. Такие протоколы по-прежнему остаются одними из лидеров по скорости генерации секретного ключа (порядка 2.3 Мбит/с на дистанции 25 км. [57]), а благодаря относительно недавно разработанным методам классической постобработки значительно увеличена дальность, на которую может быть распределен секретный ключ. Дальнейшего изучения как теоретического, так и экспериментального требует учет и построение моделей шумов, возникающих при практической реализации протокола, а также анализ и приведение к единообразному виду большого числа уже существующих моделей. Другим важным полем для исследований являются обоснования секретности протоколов *CV QKD*, лишь для некоторых из них доказана безусловная секретность, для большинства доказана секретность против коллективных атак и в асимптотическом режиме. Несмотря на свою специфику, протоколы *CV QKD* в будущем могут составить серьезную конкуренцию для протоколов с дискретными переменными, к которым относится, например, BB-84.

ЛИТЕРАТУРА

1. Dowling JP, Milburn GJ. Quantum technology: the second quantum revolution. *Phil. Trans. R. Soc. Lond.,* 2003, A361:1655-1674.
2. Lars J. *The Second Quantum Revolution.* Springer International Publishing, 2018, 339 p.
3. Horodecki R, Horodecki P, Horodecki M, Horodecki K. Quantum entanglement. *Rev. Mod. Phys.*, 2009, 81:865-942.
4. Bennett CH, Brassard G, Crepeau C, Jozsa R, Peres A, Wootters WK. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.,* 1993, 70:1895-1899.

5. Wootters W, Zurek W. A Single quantum cannot be cloned. *Nature,* 1982, 299:802-803.
6. Nielsen A, Chuang IL. *Quantum computation and quantum information*. Cambridge, Cambridge University Press, 2000, 676 p.
7. Holevo AS. Quantum Systems, Channels, Information: A Mathematical Introduction. *De Gruyter Studies in Mathematical Physics,* 2012, 16, 362 p, Berlin, Germany, ISBN 978-3-11-027325-0.
8. Kulik SP. Quantum cryptography. Part 1. *Photonics Russia*, 2010, 2:36-41.
9. Kulik SP. Quantum cryptography. Part 2. *Photonics Russia*, 2010, 3:56-60.
10. Kulik SP. Quantum cryptography. Part 2. *Photonics Russia*, 2010, 4:28-34.
11. Wolf R. Quantum Key Distribution: An Introduction with Exercises. *Lecture Notes in Physics*, Switzerland, Springer, 2021, 229 p.
12. Vernam GS. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. Amer. Inst. Elec. Eng.*, 1926, 45:109-115.
13. Rivest RL, Shamir A, Adleman LM. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM,* 1978, 21:120-126.
14. Lenstra AK. *Integer Factoring in Encyclopedia of Cryptography and Security.* Boston, Springer US, 2011, p 297.
15. Shor PW. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Review*, 1999, 41:303-332.
16. Bennett CH, Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, 1984, p. 175-179.
17. Ekert AK. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.,* 1991, 67:661-663.
18. Bennett CH. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 1992, 68:3121-3124.
19. Grosshans F, Grangier P. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.,* 2002, 88:057902-1-4.
20. Lo H, Ma X, Chen K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.,* 2005, 94:230504-1-4.
21. Grosshans F, Assche GV, Wenger J, Brouri R, Cerf NJ, Grangier P. Quantum key distribution using Gaussian-modulated coherent states. *Nature,* 2003, 421:238-241.
22. Schleich WP. *Quantum Optics in Phase Space.* Berlin, Wiley-VCH, 2001, 717 p.
23. Braunstein SL, Van Loock P. Quantum information with continuous variables. *Rev. Mod. Phys.*, 2005, 77:513-577.
24. Diamanti E, Leverrier A. Distributing secret keys with quantum continuous variables: principle, security, and implementations. *Entropy,* 2015, 17(12):6072-6092.
25. Laudenbach F, Pacher C, Fung CHF, Poppe A, Peev M, Schrenk B, Hentschel M., Walther P, Hübel H. Continuous-Variable Quantum Key Distribution with Gaussian Modulation – The Theory of Practical Implementations. *Adv. Quantum Technol.,* 2018, 1:1800011-1-37.
26. Миронов ЮБ, Казанцев СЮ, Шаховой РА, Колесников ОВ, Машковцева ЛС, Зайцев АИ, Коробов АВ. Анализ перспектив развития источников одиночных фотонов в системах квантового распределения ключей. *Наукоемкие технологии в космических исследованиях Земли*, 2021, 13(6):22-33.
27. Машковцева ЛС, Болотов ДВ, Казанцев СЮ, Колесников ОВ, Миронов ЮБ, Селюков АС. Наукометрический анализ публикаций по источникам одиночных фотонов для систем связи с квантовым распределением ключей. *Научно-техническая информация. Серия 1: Организация и методика информационной работы,* 2022, 1:22-31.
28. Зайцев А, Зубилевич А, Колесников О, Коробов А. Источники одиночных фотонов для инфокоммуникационных систем. *Первая миля*, 2022, 6(106):64-69.
29. Cabrera B. Detection of single infrared, optical, and ultraviolet photons using superconducting transition edge sensors. *Appl. Phys. Lett.,* 1998, 73:735.
30. Zhang Y, Chen Z, Pirandola S, Wang X, Zhou C, Chu B, Zhao Y, Xu B, Yu S, Guo H. Long-Distance Continuous-Variable Quantum Key

Distribution over 202.81 km of Fiber. *Phys. Rev. Lett.*, 2020, 125:010502-1-6.

31. Hosseinidehaj N, Babar Z, Malaney R, Ng SX, Hanzo L. Satellite-Based Continuous-Variable Quantum Communications: State-of-the-Art and a Predictive Outlook. *IEEE Communications Surveys and Tutorials,* 2019, 21:881-919.
32. Weedbrook C, Ottaviani C, Pirandola S. Two-way quantum cryptography at different wavelengths. *Phys. Rev. A*, 2014, 89:012309-1-8.
33. Qi B, Lougovski P, Pooser R, Grice W, Bobrek M. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. *Phys. Rev. X*, 2015, 5:041009-1-12.
34. Samsonov E, Goncharov R, Gaidash A, Kozubov A, Egorov V, Gleim A. Subcarrier wave continuous variable quantum key distribution with discrete modulation: mathematical model and finite-key analysis. *Scientific Reports,* 2020, 10:10034-1-9.
35. Leverrier A, Grangier P. Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation. *Phys. Rev. Lett.*, 2009, 102:180504-1-4.
36. Cerf NJ, Levy M, Assche GV. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A,* 2001, 63:052311-1-5.
37. Filip R. Continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A*, 2008, 77:022310-1-5.
38. Chi YM, Qi B, Zhu W, Qian L, Lo HK, Youn SH, Lvovsky AI, Tian L. A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution. *New J. Phys.,* 2011, 13:013003-1-18.
39. Arbekov IM, Molotkov SN. Extraction of quantum randomness. *UFN,* 2021, 191:651-669.
40. Shakhovoy R. Digitization of a Random Signal from the Interference of Laser Pulses: Issue of Randomness Extraction for a Quantum Random Number Generator. *2023 Wave Electronics and its Application in Information and Telecommunication Systems,* St. Petersburg, 2023, p. 1-7.
41. Smithey DT, Beck M, Raymer MG, Faridani A. Measurement of the Wigner distribution and the density matrix of a light mode using optical homodyne tomography: application to squeezed states and the vacuum. *Phys. Rev. Lett.,* 1993, 70:1244-1247.
42. Wigner EP. On the quantum correction for thermodynamic equilibrium. *Phys. Rev.,* 1932, 40:749-759.
43. Perepelkin EE, Sadovnikov BI, Inozemtseva NG, Burlakov EV. The Wigner function negative value domains and energy function poles of the harmonic oscillator. *Journal of Computational Electronics,* 2021, 20:2148-2158.
44. Perepelkin EE, Sadovnikov BI, Inozemtseva NG, Burlakov EV, Afonin PV. The Wigner function negative value domains and energy function poles of the polynomial oscillator. *Physica A: Statistical Mechanics and its Applications,* 2022, 598:127339-1-15.
45. Perepelkin EE, Sadovnikov BI, Inozemtseva NG, Burlakov EV. Extended Wigner Function for the Harmonic Oscillator in the Phase Space. *Results in Physics,* 2020, 19:103546-1-8.
46. Dianov EM. Fiber lasers. *UFN,* 2004, 174:1139-1142.
47. Blakemore JS. Semiconducting and other major properties of gallium arsenide. *Journal of Applied Physics*, 1982, 53:123-181.
48. Assche GV, Cardinal J, Cerf NJ. Reconciliation of a quantum-distributed Gaussian key. *IEEE Trans. Inf. Theory,* 2004, 50:394-400.
49. Leverrier A, Alléaume R, Boutros J, Zémor G, Grangier P. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys. Rev. A*, 2008, 77:042325-1-8.
50. Richardson T, Urbanke R. *Modern Coding Theory.* New York, Cambridge University Press, 2008, 590 p.
51. Csiszár I, Korner J. Broadcast channels with confidential messages. *IEEE transactions on information theory,* 1978, 3:339-348.
52. Shannon CE. A mathematical theory of communication. *The Bell system technical journal,* 1948, 27(3):379-423.

53. Scarani V, Bechmann-Pasquinucci H, Cerf N, Dušek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 2009, 8(3):1301-1350.
54. Devetak I, Winter A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A,* 2005, 461:207-235.
55. Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf NJ, Tualle-Brouri R, McLaughlin SW, Grangier P. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A,* 2007, 76:042305.
56. Renner R. Security of quantum key distribution. *Int. J. Quantum Inf,* 2008, 6:1-127.
57. Weerasinghe A, Alhussein M, Li H, Wonfor A, Penty R. Experimental demonstration of practical high-speed Gaussian coherent state continuous variable quantum key distribution with real-time parameter monitoring and key distillation. *SPIE Photonex* (Birmingham, 2022). 2023, V. 12335.

Бурлаков Евгений Владимирович
к.ф.-м.н.
Московский технический университет связи и информатики
8А, ул. Авиамоторная, Москва 111024, Россия
E-mail: e.v.burlakov@mtuci.ru

Коробов Александр Владимирович
аспирант
Московский технический университет связи и информатики
8А, ул. Авиамоторная, Москва 111024, Россия
E-mail: a.v.korobov@mtuci.ru.