ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 61 **2025** **Вып. 1**

УДК 621.391.7 : 530.145 : 004.056.5

© 2025 г. **В.И. Морозов, О.О. Евсютин, С.И. Нефедов**

О ВЛИЯНИИ ПАРАМЕТРОВ АППАРАТНОГО И АЛГОРИТМИЧЕСКОГО ОБЕСПЕЧЕНИЯ НА ДОПУСТИМУЮ ПРОТЯЖЕННОСТЬ ЛИНИИ ДЛЯ ПРОТОКОЛА КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С ФАЗОВО-ВРЕМЕННЫМ КОДИРОВАНИЕМ[1]

Квантовое распределение ключей является одним из перспективных направлений современной криптографии. Оно позволяет сторонам информационного обмена выработать общий криптографический ключ, секретность которого обеспечивается законами квантовой механики. В статье исследуется влияние характеристик квантового канала, а также параметров применяемых алгоритмов на максимальную допустимую протяженность линии связи для протокола с фазово-временным кодированием и состояниями-ловушками. Посредством вычислительных экспериментов с имитационной моделью системы квантового распределения ключей, основанной на указанном протоколе, было установлено, что стабильная работа протокола возможна при длине линии не более 210 км. Также было показано, что данное значение может быть увеличено за счет построения более эффективных алгоритмов очистки просеянного ключа.

Ключевые слова: квантовая криптография, квантовое распределение ключей, помехоустойчивое кодирование, LDPC-коды

DOI: 10.31857/S0555292325010024, **EDN:** MVBFJF

§ 1. Введение

Современные темпы развития технологий обработки и передачи информации определяют новые вызовы в области разработки средств обеспечения информационной безопасности [1,2]. В число таких средств входят и системы криптографической защиты информации. Появление новых паттернов взаимодействия сторон информационного обмена приводит к необходимости разработки новых криптографических схем (см., например, [3]).

Одним из передовых подходов в современной криптографии, привлекающим все более активное внимание исследователей, является квантовое распределение ключей (КРК). Это метод выработки общего секретного ключа сторонами информационного обмена, безопасность которого обеспечивается фундаментальными законами квантовой механики. В качестве носителей ключевой информации в этом методе используются квантовые состояния, что и позволяет разработчикам опираться на особенности квантовых явлений в ходе построения безопасных протоколов [4,5]. Тогда как многие классические криптографические протоколы нельзя назвать полностью защищенными от атаки “перехват-пересылка”, протоколы КРК делают такую атаку практически нереализуемой, чем и обусловлено внимание к ним со стороны исследователей в области криптографии. Данное полезное свойство достигается за

[1] Исследование осуществлено в рамках Программы фундаментальных исследований НИУ ВШЭ.

счет того, что информация, передаваемая по квантовому каналу, не может быть перехвачена злоумышленником так, чтобы это осталось незамеченным законными пользователями. Это следует из теоремы о запрете клонирования [6], которая гласит, что создание копии произвольного квантового состояния невозможно. Таким образом, в отличие от классических каналов связи, где, включившись в линию, злоумышленник может незаметно копировать каждый передаваемый бит, в канале КРК он не может это сделать, не внеся значительных изменений в перехваченную информацию, чем он сразу же обнаружит свое присутствие.

С того времени, когда был теоретически описан первый протокол КРК, технологии сделали большой шаг вперед, и в настоящий момент реализация каналов, пригодных для этой задачи, является возможной [7]. Однако несмотря на значительные достижения в области совершенствования аппаратного обеспечения квантовой криптографии, квантовые каналы все еще являются достаточно нестабильными [8, 9]. Одним из наиболее важных следствий несовершенства каналов связи, используемых в системах квантового распределения ключей (СКРК), является крайне ограниченная длина линий связи, на которых возможно развертывание и бесперебойное функционирование таких систем.

В оптоволоконных линиях длиной 200 км при средних потерях 0,2 дБ/км при передаче теряется порядка 99,99% передаваемой информации. Справиться с таким объемом теряемой информации отчасти помогает тот факт, что во время передачи обе стороны имеют синхронизированные часы [10], в результате чего сторона-приемник может с высокой вероятностью предположить, какие именно (по порядковому номеру) квантовые состояния, переданные стороной-отправителем, были потеряны, а какие – приняты. Однако помимо того, что большая часть информации теряется в ходе передачи, принятая часть содержит искажения, которые должны быть исправлены принимающей стороной. В ранних работах по КРК данной задаче уделялось достаточно малое внимание [11, 12]. Исследователи сосредоточивали свои усилия на аппаратной составляющей СКРК, пренебрегая алгоритмической. Однако позже было установлено, что квантовый канал существенно отличается от классических каналов телекоммуникаций и требует новых подходов к исправлению ошибок в нем, в связи с чем в последние годы направление исследований, связанное с применением кодов, корректирующих ошибки, в КРК, стало достаточно активно развиваться (можно отметить работы [13–15] и другие).

Основной целью данного исследования является оценка корректирующей способности LDPC-кодов на линиях связи предельной дальности, которая, как было отмечено выше, составляет 200 км и более. Данная оценка проводится на примере перспективного протокола КРК с фазово-временным кодированием [16], который является развитием классического протокола BB84, но имеет несколько существенных преимуществ. Первое из них состоит в отсутствии поляризационно-чувствительных элементов на принимающей стороне, что позволяет убрать из СКРК дорогостоящий контроллер поляризации, схему управления для него и упростить программное обеспечение [17]. Также, как отмечается в [18, 19], данный протокол позволяет выявлять факт вмешательства противника в квантовый канал по двум параметрам, а не по одному. Для оценки эффективности выбранного протокола КРК, включая исправляющую способность помехоустойчивого кодирования, была построена имитационная модель, учитывающая особенности работы аппаратуры и физические свойства среды передачи.

Дальнейшая часть статьи организована следующим образом. В § 2 представлен обзор актуальной научной литературы в проблемной области квантовых коммуникаций. В § 3 содержится описание протокола КРК с фазово-временным кодированием. В § 4 рассматриваются особенности построенной имитационной модели. В § 5 описываются результаты вычислительных экспериментов, которые затем обсуждаются в § 6. Наконец, в заключении подводятся итоги проведенного исследования.

§ 2. Обзор проблемной области квантового распределения ключей

2.1. Протоколы квантового распределения ключей. Квантовая криптография представляет собой одно из направлений современной криптографии, которое можно определить как науку об использовании квантово-механических свойств для решения криптографических задач. Основной решаемой задачей является распределение секретных ключей между удаленными пользователями, сообщающимися по открытым каналам связи. Решение данной задачи с использованием принципов квантовой физики называется квантовым распределением ключей.

Базовым законом для квантовой криптографии является теорема о запрете клонирования [6, 20], констатирующая, что произвольное квантовое состояние не может быть достоверно скопировано. Это определяет важнейшее свойство квантового распределения ключей: пассивный злоумышленник, даже получив доступ к каналу передачи, не сможет достоверно скопировать передаваемую информацию и, более того, попытавшись это сделать, обнаружит свое присутствие.

Любая система квантового распределения ключей базируется на некотором квантовом криптографическом протоколе выработки и распределения ключей (протоколе КРК). В настоящее время известны десятки различных протоколов КРК, отличающихся друг от друга показателями скорости и дальности передачи информации, а также особенностями физической реализации.

Первым протоколом КРК, положившим начало квантовой криптографии, стал протокол BB84 [11]. Данный протокол позволяет двум пользователям (Алисе и Бобу) безопасно сгенерировать криптографический ключ в присутствии пассивного злоумышленника (Евы). Взаимодействие Алисы и Боба осуществляется с использованием двух каналов связи: квантового и классического открытого канала. Квантовый канал служит для передачи от Алисы к Бобу квантовых состояний, кодирующих биты секретного ключа. В зависимости от физической реализации это может быть, например, оптоволокно. Открытый канал – это любой аутентифицированный классический канал коммуникации между сторонами информационного обмена (например, Ethernet-кабель). Предполагается, что информация, передаваемая по этому каналу, доступна для просмотра пассивному злоумышленнику.

Общая схема работы BB84 представлена на рис. 1. Данный протокол можно разделить на несколько этапов, которые характерны и для иных протоколов, развивающих BB84.

Эти этапы описаны далее.

1. *Первоначальная генерация битов и базисов.* Алиса вырабатывает последовательность одиночных фотонов, выбирая для каждого из них один из четырех видов поляризации: 0°, 45°, 90° или 135°. Данные виды поляризации называются базисами. При этом поляризация 0° и 90° соответствует прямолинейному базису, а 45° и 135° – диагональному. Сгенерированные фотоны передаются Бобу по квантовому каналу.

2. *Измерение.* Для каждого принятого фотона Боб случайно выбирает один из двух возможных базисов и измеряет состояние фотона в соответствии с этим базисом. Результаты измерений Боб сохраняет в тайне. Последовательность битов, сформированная в результате измерения квантовых состояний, называется “сырым” ключом.

3. *Просеивание ключа.* Боб сообщает Алисе, какие базисы он выбрал для каждого из принятых фотонов. Алиса, в свою очередь, сообщает Бобу, в каких случаях его выбор был верным. Обе стороны отбрасывают те биты, для которых Боб выбрал неправильный базис. Последовательность битов, сформированная на данном этапе, называется просеянным ключом.

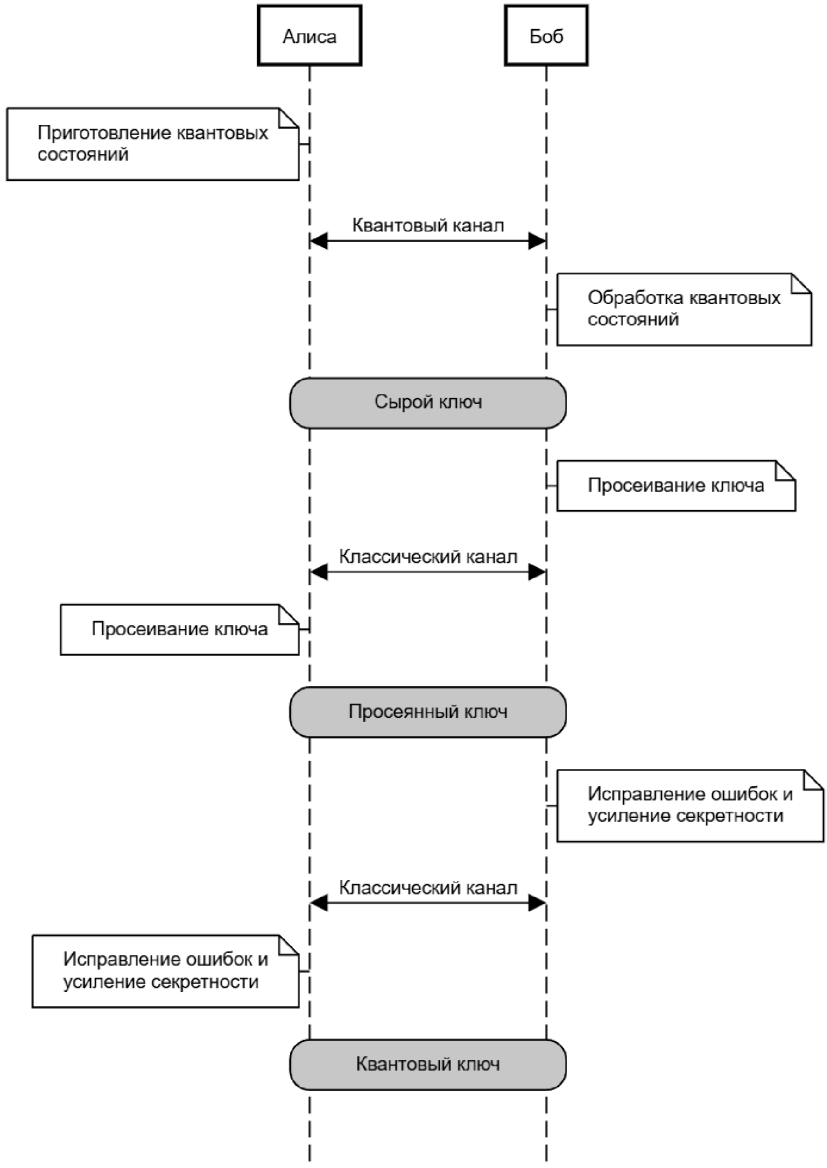


Рис. 1. Схема работы протокола BB84

4. *Оценка и исправление ошибок в ключе.* Боб и Алиса оценивают QBER (quantum bit error rate) полученной двоичной последовательности и сравнивают его с некоторым максимальным значением, заранее известным для данного канала. Здесь под QBER понимается доля информационных битов, которые были искажены (инвертированы) при передаче по квантовому каналу. При этом биты, соответствующие фотонам, не принятым Бобом, не учитываются как ошибочные. Если полученное значение QBER превышает заданный максимум, констатируется наличие злоумышленника в канале, и ключ отбрасывается. В противном случае применяются классические методы исправления ошибок. Последовательность битов, сформированная на данном этапе, называется очищенным ключом.

5. *Усиление секретности.* Как правило, полученная случайная последовательность битов подвергается дополнительной постобработке с целью усиления секретности полученного криптографического ключа. Результирующая последовательность битов называется усиленным ключом.

Реализация шагов 4 и 5 нетривиальна и заслуживает особого внимания. Так, оценка и исправление ошибок в ранних работах (например, [21]) проводились по наиболее простой схеме с использованием проверок четности различных пар бит ключа. Как отмечают авторы работы [21], такой подход далек от оптимального. По этой причине в современных работах, таких как [16], используется более мощный аппарат LDPC-кодов, а также некоторые его усовершенствования, описанные, например, в [14, 15].

В дальнейшем исследователями были предложены различные модификации оригинального протокола BB84, направленные на улучшение его характеристик. Некоторые из таких модификаций будут кратко рассмотрены далее.

В работе [12] исследователи представляют простой способ уменьшения потерь при реализации КРК, состоящий в неравновероятном выборе базисов. Уязвимость, возникающую в таком подходе, авторы работы предлагают компенсировать дискретной оценкой ошибок по каждому из базисов.

Другие ученые сосредоточили свои усилия на протоколах с более чем двумя базисами. Так, в работе [21], наряду с прямолинейным и диагональным, авторы предлагают использовать еще один базис — циркулярный. Представленные результаты показывают, что такая модификация позволяет достичь лучшего уровня секретности, но при этом также приводит к увеличению количества потерь в линии.

В свою очередь авторы [22] обобщают протоколы с множеством базисов, представляя численные оценки для критического уровня ошибок и вероятности компрометации ключа в таких подходах.

Наконец, в [23] обсуждается подход с использованием множества базисов и вспомогательного ключа, позволяющий вдвое снизить потери в линии. Однако способы предварительного распределения вспомогательного ключа не приводятся.

Другие исследования посвящены защите от конкретных видов атак на протоколы КРК. Так, в [24] приводится протокол SARG04, предусматривающий защиту от известной атаки с разделением по числу фотонов (PNS – photon number splitting attack) [25]. Протокол с состояниями-ловушками, представленный в работе [26], также создан для защиты КРК от указанной атаки. Данный протокол предлагает случайным образом заменять информационные импульсы на стороне Алисы специальными многофотонными на этапе приготовления квантовых состояний, а затем, на стороне Боба, измерять уровень ошибки для таких импульсов. Если этот уровень будет ниже, чем для остальных импульсов, это будет означать, что однофотонные импульсы были блокированы, а значит, была применена атака с разделением по числу фотонов. В таком случае протокол завершается. В работе [26] также доказано, что общий уровень ошибки будет совпадать с уровнем ошибки для ловушечных состояний в случае, если атака не производилась. Рассмотренный метод получил широкое развитие в дальнейших разработках в области квантовой криптографии.

2.2. Последние достижения и вызовы в области квантовой криптографии. Среди последних достижений в области развития и доработки протокола BB84 можно отметить следующие:

1) Протокол с использованием третьей стороны – доверенного центра [27].
2) Протокол с использованием геометрически однородных состояний [28].
3) Протокол с фазово-временным кодированием [16].

В работе [27] рассматривается протокол квантового распределения ключей, в котором количество получаемой в результате ключевой информации значительно увеличивается за счет дополнительного участника взаимодействия – доверенного центра, называемого Чарли. В данном протоколе Чарли выступает одновременно и принимающей, и передающей стороной.

Среди преимуществ данного протокола отмечается увеличение длины результирующего ключа, так как доверенный центр можно расположить так, чтобы длина линии от каждой из сторон до него была вдвое меньше, чем длина линии между этими сторонами. Таким образом можно значительно снизить потери информации. Кроме того, протокол обладает повышенной криптостойкостью, поскольку для перехвата ключа злоумышленнику будет необходимо прослушивать сразу две линии.

Авторы работы [28], в свою очередь, обобщили BB84, SARG04 и ряд других схожих протоколов, под одним термином – протоколы с геометрически однородными состояниями. Данная версия протокола включает в себя все шаги BB84 с единственной модификацией: на всех шагах протокола количество базисов берется равным $N/2$ для произвольного четного N вместо двух базисов для BB84.

Исследователи рассматривают эффективность протоколов такого вида в противостоянии атакам PNS [25] и USD (unambiguous state discrimination attack – атака с измерениями с определенным исходом [29]). Результаты экспериментов и расчетов, представленные в [28], показывают, что наибольшей эффективности против данных атак можно достичь при $N = 8$, так как при этом обеспечивается достаточно низкий уровень вероятности безошибочного измерения фотонов злоумышленником.

Описанные протоколы, как правило, используют поляризационно чувствительные активные элементы (например, фазовые модуляторы и контроллеры поляризации) и, следовательно, требуют подстройки поляризации на выходе из линии связи. В работе [16] представлен протокол квантового распределения ключей с фазово-временным кодированием, допускающий волоконно-оптическую реализацию приемной части, не использующую поляризационно чувствительные активные элементы, что позволяет избежать отмеченной проблемы. Более того, обнаружение присутствия злоумышленника в квантовом канале в данном протоколе происходит на основании анализа ошибок в информационных временных окнах и отсчетов в контрольных временных окнах, что позволяет увеличить предельную дальность передачи ключей. Для эффективного противостояния PNS-атакам разработчики протокола используют ловушечные состояния, которые позволяют приемной стороне обнаружить атаку по изменению статистики фотоотсчетов в посылке.

Различные стратегии использования помехоустойчивого кодирования на основе LDPC-кодов, предложенные в работе [30], позволяют достичь компромисса между тремя важнейшими характеристиками: скоростью работы алгоритма декодирования, конфиденциальностью исправляемой информации и количеством избыточных бит, которые необходимо отправить, чтобы провести процедуру исправления.

Более подробно этот протокол будет описан в последующих параграфах настоящей статьи.

Таким образом, анализ актуальной научной литературы в области квантового распределения ключей позволяет заключить, что работа Ч. Беннета и Ж. Брассара по-прежнему обладает практической ценностью. Подавляющее большинство протоколов КРК, полученных в более поздние годы, представляют собой модификации протокола BB84, направленные на построение более производительных систем КРК, но сохраняющие ключевые особенности оригинального протокола.

Также следует отметить, что основными целями улучшений, вносимых в BB84, являются повышение производительности выработки секретного ключа и устойчивость к атакам на протокол. Эти проблемы наиболее актуальны, так как квантовый канал в гораздо большей степени, чем классические каналы, подвержен влиянию

различных побочных воздействий, в результате чего существенная часть передаваемой в нем информации теряется. Что касается атак на КРК, не следует оставлять без внимания тот факт, что рост уровня технологического оснащения, позволивший создавать практические реализации квантовых криптографических протоколов, позволил также проводить более сложные атаки на такие протоколы, что приводит к необходимости повышать уровень защищенности. Так, например, в работе [31] была построена эффективная атака на протокол с фазово-временным кодированием [16], демонстрирующая некоторые недостатки в доказательстве его стойкости.

§ 3. Протокол квантового распределения ключей с фазово-временным кодированием

В данном параграфе приводится описание протокола КРК с фазово-временным кодированием, который является объектом настоящего исследования. Исследуемый протокол базируется на работе [16], однако содержит некоторые отличия. В рассматриваемом протоколе используется только три временных окна, в результате чего повышается скорость генерации ключа, однако контрольные временные окна отсутствуют. В качестве второго параметра для оценки информации злоумышленника в данном протоколе используется вероятность срабатывания детекторов в те временные промежутки, когда отправитель посылал вакуумные состояния.

Участников протокола традиционно будем называть Алисой и Бобом, где Алиса является передающей стороной, отвечающей за приготовление и отправку квантовых состояний, а Боб – принимающей стороной, отвечающей за прием квантовых состояний.

Кодирование битов “сырого” ключа на стороне Алисы осуществляется следующим образом. Оптическая часть Алисы состоит из импульсного источника света, фазового модулятора и модулятора интенсивности, светоделителя, оптического полосового фильтра, двух оптических изоляторов и нескольких аттенюаторов. Источник света генерирует импульс света длительностью τ с периодом повторения T.

Для противодействия атаке с разделением по числу фотонов используются ловушечные состояния. Для этого импульсы генерируются с разной средней мощностью, т.е. с разным средним количеством фотонов, приходящихся на один оптический импульс. Значение мощности для каждого импульса выбирается случайным образом из заданного множества вариантов. Значения, использованные в данной статье, и их количество представляют реализацию подхода с двумя ловушечными состояниями [32, 33]. Однако следует отметить, что в общем случае может быть использовано большее количество состояний (например, как описано в [34]).

Оптический импульс попадает на светоделитель 1×2 с коэффициентом деления 50/50. В одном из плеч светоделителя устанавливается короткий отрезок оптического волокна, в другом – более длинный, причем оптическая задержка, вносимая длинным участком волокна Δt, должна удовлетворять неравенству $\tau < \Delta t < T/3$. Импульс без задержки будем называть “импульс 1”, задержанный импульс – “импульс 2”.

Далее оба импульса объединяются светоделителем 1×2 с коэффициентом деления 50/50 в общий канал, к импульсам применяется последовательно фазовая модуляция и модуляция интенсивности в зависимости от выбранного базиса и бита “сырого” ключа в соответствии с табл. 1.

В таблице приняты следующие обозначения:

μ_i – аттенюация i-го импульса;

φ_i – фазовый сдвиг i-го импульса.

Измерение битов “сырого” ключа на стороне Боба осуществляется следующим образом. Оптическая часть Боба состоит из циркулятора, светоделителя и двух зер-

Таблица 1

Базисы, используемые для кодирования битов квантовыми состояниями

Базис	Кодируемый бит	μ_1	μ_2	φ_1	φ_2
B_{I}	0	1	∞	0	0
	1	∞	1	0	0
B_{II}	0	2	2	0	0
	1	2	2	0	π

кал Фарадея, составляющих интерферометр Маха – Цендера, и пьезоэлемента для точной подстройки зеркал Фарадея.

Проходя циркулятор, оптический импульс попадает на светоделитель 2×2 с коэффициентом деления 50/50. На выходе светоделителя установлены два отрезка оптического волокна разной длины, при этом разность оптического хода, создаваемого длинным участком волокна, равна $\Delta t/2$. Двойное прохождение оптического импульса по этому участку волокна компенсирует задержку импульса 2.

Детектирование импульса осуществляется в трех временных окнах, сдвинутых на время Δt и $2\Delta t$. В среднем временном окне результат детектирования зависит от интерференции оптических импульсов. В случае конструктивной интерференции происходит срабатывание только детектора 1, в случае деструктивной – только детектора 2.

Значение принятого бита "сырого" ключа определяется Бобом на основании номера сработавшего детектора и временного окна, в котором произошло срабатывание, после раскрытия Алисой соответствующего данному биту базиса.

Обозначения, используемые в дальнейшем описании, приведены в табл. 2.

Таблица 2

Основные обозначения

№	Обозначение	Расшифровка обозначения
1	μ	Средняя мощность импульса, генерируемого источником квантового оптического излучения, определяющая среднее количество фотонов на импульс.
2	$p = (p_1, p_2, \ldots, p_L)$, $p_i \in \{1, 2, 3\}$	Последовательность случайных чисел, определяющих выбор значений средней мощности импульсов, генерируемых источником квантового оптического излучения и соответствующих битам "сырого" ключа.
3	$p' = (p'_1, p'_2, \ldots, p'_M)$, $p'_i \in \{1, 2, 3\}$, $M < L$	Последовательность случайных чисел, определяющих выбор значений средней мощности импульсов, для которых на стороне Боба произошло срабатывание детекторов.
4	$CTR = (CTR_1, CTR_2, CTR_3)$, $CTR_i \in \mathbb{N}$	Вектор-счетчик, предназначенный для подсчета импульсов с разной средней мощностью.
5	θ	Коэффициент, определяющий предельное превышение скорости генерации просеянного ключа для импульсов большей средней мощности над скоростью генерации квантового ключа для импульсов меньшей средней мощности.
6	$x = (x_1, x_2, \ldots, x_L)$, $x_i \in \{0, 1\}$	"Сырой" ключ, генерируемый Алисой и передаваемый Бобу.
7	$b = (b_1, b_2, \ldots, b_L)$, $b_i \in \{B_{\mathrm{I}}, B_{\mathrm{II}}\}$	Базисы, выбираемые Алисой для кодирования битов "сырого" ключа квантовыми состояниями (см. табл. 1).

Таблица 2. Продолжение

№	Обозначение	Расшифровка обозначения
8	$d^j = (d_1^j, d_2^j, \ldots, d_L^j)$, $d_i^j \in \{0, 1, 2, 3\}$, $j \in \{1, 2\}$	Последовательность номеров временных окон, в которых сработал детектор D_j на стороне Боба при приеме квантовых состояний, передаваемых Алисой, где значения 1, 2, 3 указывают номер временного окна, а значение 0 указывает на то, что при приеме соответствующего квантового состояния детектор не сработал.
9	$\nu = (\nu_1, \nu_2, \ldots, \nu_M)$, $\nu_i \in \mathbb{N}$, $M < L$	Последовательность номеров квантовых состояний, для которых было зафиксировано срабатывание детектора D1 или D2 на стороне Боба.
10	$b' = (b'_1, b'_2, \ldots, b'_M)$, $b'_i \in \{B_{\text{I}}, B_{\text{II}}\}$, $M < L$	Последовательность базисов, соответствующих квантовым состояниям, для которых было зафиксировано срабатывание детектора D1 или D2 на стороне Боба.
11	$y^B = (y_1^B, y_2^B, \ldots, y_N^B)$, $y_i^B \in \{0, 1\}$, $N < M$	Просеянный ключ Боба, сформированный Бобом после получения от Алисы значений базисов, соответствующих квантовым состояниям, для которых было зафиксировано срабатывание детектора D1 или D2 на стороне Боба.
12	$u = (u_1, u_2, \ldots, u_N)$, $u_i \in \mathbb{N}$, $N < M$	Последовательность номеров квантовых состояний, принятых Бобом без неопределенности.
13	$y^A = (y_1^A, y_2^A, \ldots, y_N^A)$, $y_i^A \in \{0, 1\}$, $N < M$	Просеянный ключ Алисы, сформированный Алисой после получения от Боба значений номеров квантовых состояний, принятых Бобом без неопределенности.
14	t	Максимальное число попыток исправления ошибок в просеянном ключе.
15	H	Проверочная матрица LDPC-кода размера $K \times N$, с помощью которой выполняется очистка просеянного ключа.
16	H'	Расширенная матрица размера $K \times (N + K)$, полученная посредством присоединения слева к матрице H единичной матрицы E порядка K.
17	$s^A = (s_1^A, s_2^A, \ldots, s_K^A)$, $s_i^A \in \{0, 1\}$, $K < N$	Синдром Алисы, полученный в результате умножения проверочной матрицы LDPC-кода H на транспонированный просеянный ключ Алисы y^A.
18	$s^B = (s_1^B, s_2^B, \ldots, s_K^B)$, $s_i^B \in \{0, 1\}$, $K < N$	Синдром Боба, полученный в результате умножения проверочной матрицы LDPC-кода H на транспонированный просеянный ключ Боба y^B.
19	y'	Расширенный вектор длины $N + K$, полученный посредством присоединения слева к просеянному ключу Боба y^B синдрома Алисы s^A.
20	r	Количество бит просеянного ключа, раскрываемых Алисой после одной итерации очистки ключа при неуспешном завершении попытки исправления ошибок на стороне Боба.
21	$w = (w_1, w_2, \ldots, w_r)$, $w_i \in 1..N$, $\forall i \neq j : w_i \neq w_j$	Последовательность номеров бит просеянного ключа, раскрываемых Алисой после одной итерации очистки ключа при неуспешном завершении попытки исправления ошибок на стороне Боба.
22	$y'' = (y''_1, y''_2, \ldots, y''_r)$, $y''_i \in \{0, 1\}$	Последовательность значений бит просеянного ключа, раскрываемых Алисой после одной итерации очистки ключа при неуспешном завершении попытки исправления ошибок на стороне Боба.

Таблица 2. Окончание

№	Обозначение	Расшифровка обозначения
23	t_A	Счетчик числа неуспешных попыток исправления ошибок в просеянном ключе, обновляемый на стороне Алисы.
24	t_B	Счетчик числа неуспешных попыток исправления ошибок в просеянном ключе, обновляемый на стороне Боба.
25	$\mathbb{F}_2[x]$	Кольцо многочленов над конечным полем $\mathbb{F}_2$.
26	$f(x) \in \mathbb{F}_2[x]$	Неприводимый многочлен степени N, используемый Алисой и Бобом для построения универсальной хеш-функции второго порядка.
27	$\mathbb{F}_{2^N}$	Поле Галуа, представляющее собой расширение простого поля $\mathbb{F}_2$ посредством неприводимого многочлена $f(x)$ степени N.
28	$\Delta\colon \{0,1\}^\ell \to \mathbb{F}_2[x]$	Биективное отображение, ставящее в соответствие двоичному вектору $(\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ многочлен $\alpha(x) \in \in \mathbb{F}_2[x]$, $\alpha(x) = \alpha_1 + \alpha_2 x + \ldots + \alpha_\ell x^{\ell-1}$.
29	$\nabla\colon \mathbb{F}_2[x] \to \{0,1\}^\ell$	Биективное отображение, ставящее в соответствие многочлену $\alpha(x) \in \mathbb{F}_2[x]$, $\alpha(x) = \alpha_1 + \alpha_2 x + \ldots + \alpha_\ell x^{\ell-1}$, двоичный вектор $(\alpha_1, \alpha_2, \ldots, \alpha_\ell)$.
30	$\bigotimes\colon \mathbb{F}_2[x] \times \mathbb{F}_2[x] \to \mathbb{F}_{2^N}$	Операция умножения произвольных многочленов из $\mathbb{F}_2[x]$ по модулю неприводимого многочлена $f(x) \in \in \mathbb{F}_2[x]$ степени N

Далее приведено пошаговое описание действий Алисы и Боба, направленных на формирование общего секретного ключа с использованием оптической линии связи и классического открытого канала. Обязательным условием корректности работы соответствующего протокола является синхронизация времени между Алисой и Бобом.

Шаг 1 представленного протокола описывает этап первоначальной генерации битов и базисов. Это единственный этап, в котором задействован квантовый канал связи. Далее, на шагах 2–8 стороны обмена производят просеивание ключа, оставляя только те биты, которые были детектированы Бобом, причем детектированы без неопределенности. При этом участники протокола также выполняют действия, направленные на противодействие атаке PNS (шаги 1.3–1.4, 4). Выбор значений битов на шаге 6.2 осуществляется в соответствии со статистическим распределением состояний по временным окнам (см., например, [16]). После этого на шагах 9–18 выполнение протокола переходит к стадии исправления ошибок, в ходе которой стороны итерационно избавляются от инверсий бит в ключе Боба. И наконец, шаги 19–21 обеспечивают усиление секретности, во время которого Алиса и Боб хешируют полученную ключевую информацию, отбрасывая при этом биты в том объеме, который был раскрыт на предыдущих этапах.

Шаг 1. Для $i = \overline{1, L}$ выполняется следующее:

Шаг 1.1. Алиса вырабатывает случайное значение бита $x_i \in \{0, 1\}$ с помощью генератора случайных чисел.

Шаг 1.2. Алиса вырабатывает случайное значение номера базиса $a \in \{0, 1\}$ с помощью генератора случайных чисел. Если $a = 0$, то Алиса принимает $b_i = B_{\mathrm{I}}$, в противном случае – $b_i = B_{\mathrm{II}}$.

Шаг 1.3. Алиса вырабатывает случайное значение $p_i \in \{1, 2, 3\}$ с помощью генератора случайных чисел и задает значение средней мощности импульсов, генериру-

емых источником квантового оптического излучения, следующим образом:

$$\mu = \begin{cases} 0{,}01, & \text{если } p_i = 1, \\ 0{,}20, & \text{если } p_i = 2, \\ 1{,}00, & \text{если } p_i = 3. \end{cases}$$

Шаг 1.4. Алиса устанавливает среднюю мощность импульсов, генерируемых источником квантового оптического излучения, равной μ, осуществляет кодирование значения бита x_i квантовым состоянием в соответствии с базисом b_i и передает квантовое состояние по оптической линии связи Бобу.

Шаг 1.5. Боб запоминает номер временного окна, в котором произошло срабатывание детектора D1 или детектора D2, следующим образом:

$$d_i^1 = \begin{cases} j, & \text{если детектор D1 сработал во временном окне } j \in 1,2,3, \\ 0, & \text{если детектор D1 не сработал,} \end{cases}$$

$$d_i^2 = \begin{cases} j, & \text{если детектор D2 сработал во временном окне } j \in 1,2,3, \\ 0, & \text{если детектор D2 не сработал.} \end{cases}$$

Шаг 2. Боб формирует вектор, содержащий номера временных окон, в которых произошло срабатывание детектора D1 или детектора D2, следующим образом:

Шаг 2.1. Выполняется инициализация счетчика принятых бит $M = 0$.

Шаг 2.2. Для $i = \overline{1, L}$ выполняется следующее:

Шаг 2.2.1. Если ни один из детекторов не сработал (т.е. $d_i^1 = 0$ и $d_i^2 = 0$), выполняется переход к шагу 2.2.1. В противном случае выполняется присваивание

$$M = M + 1, \quad v_M = i.$$

Шаг 3. Боб передает вектор $\nu = (\nu_1, \nu_2, \ldots, \nu_M)$ Алисе по классическому открытому каналу.

Шаг 4. Алиса проверяет наличие признака атаки с разделением по числу фотонов со стороны злоумышленника, потенциально присутствующего в канале связи, следующим образом:

Шаг 4.1. Алиса формирует вектор, указывающий значения средней мощности импульса, для которых на стороне Боба произошло срабатывание детекторов,

$$p' = (p_{v_1}, p_{v_2}, \ldots, p_{v_M}) = (p'_1, p'_2, \ldots, p'_M).$$

Шаг 4.2. Алиса выполняет присваивание

$$CTR = (0, 0, 0).$$

Шаг 4.3. Для $i = \overline{1, M}$ выполняется следующее:

Шаг 4.3.1. Обновляется значение счетчика

$$CTR_{p'_i} = CTR_{p'_i} + 1.$$

Шаг 4.4. Если

$$(CTR_3 - CTR_1)/(CTR_2 - CTR_1) > \theta$$

(т.е. превышено предельное соотношение импульсов большей и меньшей средней мощности, характерное для передачи в отсутствии злоумышленника), то осуществляется переход к шагу 1 в связи с обнаружением признака атаки с разделением по числу фотонов. В противном случае осуществляется переход к шагу 5.

Шаг 5. Алиса формирует вектор раскрываемых базисов

$$b' = (b_{v_1}, b_{v_2}, \ldots, b_{v_M})k = (b'_1, b'_2, \ldots, b'_M)$$

и передает его Бобу по классическому открытому каналу.

Шаг 6. Боб формирует просеянный ключ

$$y^B = (y_1^B, y_2^B, \ldots, y_N^B), \quad N < M,$$

следующим образом:

Шаг 6.1. Выполняется инициализация счетчика длины просеянного ключа $N = 0$.

Шаг 6.2. Для $i = \overline{1, M}$ выполняется следующее:

Шаг 6.2.1. Если базис $b'_i = B_{\mathrm{I}}$, выполняется переход к шагу 6.2.2. В противном случае выполняется переход к шагу 6.2.3.

Шаг 6.2.2. Если $d^1_{v_i} = 2$ или $d^2_{v_i} = 2$, констатируется неопределенность и выполняется переход к шагу 6.2. В противном случае выполняется присваивание

$$N = N + 1, \quad u_N = v_i, \quad y_N^B = (d^1_{v_i} + d^2_{v_i} - 1)/2$$

и переход к шагу 6.2.1.

Шаг 6.2.3. Если $d^1_{v_i} = 2$, выполняется присваивание

$$N = N + 1, \quad u_N = v_i, \quad y_N^B = 0$$

и переход к шагу 6.2.1. В противном случае выполняется переход к шагу 6.2.4.

Шаг 6.2.4. Если $d^2_{v_i} = 2$, выполняется присваивание

$$N = N + 1, \quad u_N = v_i, \quad y_N^B = 1$$

и переход к шагу 6.2.1. В противном случае констатируется неопределенность и выполняется переход к шагу 6.2.1.

Шаг 7. Боб передает вектор индексов состояний, принятых без неопределенности $u = (u_1, u_2, \ldots, u_N)$, Алисе по классическому открытому каналу.

Шаг 8. Алиса формирует просеянный ключ

$$y^A = (x_{u_1}, x_{u_2}, \ldots, x_{u_N}) = (y_1^A, y_2^A, \ldots, y_N^A).$$

Шаг 9. Алиса вычисляет синдром $s^A = y^A H^T$ и передает его Бобу по классическому открытому каналу.

Шаг 10. Алиса выполняет присваивание $t_A = 0$.

Шаг 11. Боб выполняет присваивание $t_B = 0$.

Шаг 12. Боб выполняет очистку просеянного ключа следующим образом:

Шаг 12.1. Вычисляется синдром $s^B = y^B H^T$.

Шаг 12.2. Если $s^B = s^A$, т.е. с вероятностью, стремящейся к единице, Боб принял вектор без ошибок, выполняется переход к шагу 18. В противном случае выполняется следующий алгоритм:

Шаг 12.2.1. Формируется расширенная матрица $H' = \langle H \parallel E \rangle$.

Шаг 12.2.2. Формируется вектор $y' = \langle y^B \parallel s^A \rangle$.

Шаг 12.2.3. Вектор y' декодируется в вектор $z = (z_1, z_2, \ldots, z_N)$ посредством алгоритма Sum-Product с использованием расширенной матрицы H'.

Шаг 12.2.4. Вычисляется синдром $s^Z = zH^T$.

Шаг 12.2.5. Если $s^Z = s^A$, т.е. декодер с вероятностью, стремящейся к единице, успешно исправил ошибки, выполняется переход к шагу 18. В противном случае выполняется переход к шагу 13.

Шаг 13. Боб вычисляет $t_B = t_B + 1$ и передает Алисе сообщение по классическому открытому каналу: “Исправление ошибок завершилось неудачей”.

Шаг 14. Алиса вычисляет $t_A = t_A + 1$.

Шаг 15. Если $t_A = t$, данный сеанс работы протокола считается неудачным и выполняется переход к шагу 1. В противном случае выполняется переход к шагу 16.

Шаг 16. Алиса вырабатывает последовательность неповторяющихся случайных индексов бит просеянного ключа $w_i \in \{1, N\}$, $i = \overline{1, r}$, с помощью генератора случайных чисел, формирует два вектора

$$w = (w_1, w_2, \ldots, w_r), \quad y'' = (y^A_{w_1}, y^A_{w_2}, \ldots, y^A_{w_r})k = (y''_1, y''_2, \ldots, y''_r)$$

и передает их Бобу по классическому открытому каналу, тем самым раскрывая часть ключа для Боба и потенциального злоумышленника.

Шаг 17. Боб выполняет присваивание

$$y^B_{w_i} = y''_i, \quad i = \overline{1, r},$$

и осуществляет переход к шагу 12.

Шаг 18. Боб передает Алисе сообщение по классическому открытому каналу: “Исправление ошибок завершилось успехом”.

Шаг 19. Алиса выбирает неприводимый многочлен $f(x)$ степени N, с помощью генератора случайных чисел вырабатывает вектор случайных значений коэффициентов случайного многочлена $\alpha_i \in \{0, 1\}$, $i = \overline{1, N}$, и передает Бобу векторы

$$\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_N), \quad \Delta(f(x)) = (f_1, f_2, \ldots, f_{N+1})$$

по классическому открытому каналу.

Шаг 20. Алиса вычисляет

$$\varkappa = \nabla(\Delta(y^A) \otimes \Delta(\alpha)) = (\varkappa_1, \varkappa_2, \ldots, \varkappa_N),$$

после чего последние rt_A бит вектора $\varkappa$ удаляются, а в качестве усиленного секретного ключа принимается вектор $k = (\varkappa_1, \varkappa_2, \ldots, \varkappa_{N-rt_A})$.

Шаг 21. Боб вычисляет

$$\varkappa = \nabla(\Delta(y^B) \otimes \Delta(\alpha)) = (\varkappa_1, \varkappa_2, \ldots, \varkappa_N),$$

после чего последние rt_B бит вектора $\varkappa$ удаляются, а в качестве усиленного секретного ключа принимается вектор $k = (\varkappa_1, \varkappa_2, \ldots, \varkappa_{N-rt_B})$.

Как следует из представленного описания, при фиксированных значениях физических параметров СКРК основное влияние на скорость генерации квантовых ключей и предельную дальность работы СКРК оказывает этап “очистки” ключа, реализующий исправление ошибок передачи с помощью некоторого LDPC-кода. Оценка данного влияния представляет собой актуальную задачу, решаемую в настоящем исследовании.

§ 4. Вычислительные эксперименты по оценке эффективности протокола квантового распределения ключей с фазово-временным кодированием

Для исследования рассмотренного выше протокола квантового распределения ключей была построена имитационная модель, учитывающая особенности соответствующей оптической схемы и физические свойства среды передачи. Данная модель

Таблица 3

Значения варьируемых параметров имитационной модели

Название параметра	Базовое значение	Миним. значение	Максим. значение	Шаг изменения
Эффективность детектора, %	80	50	100	5
Среднее число фотонов на импульс	0,2	0,01	0,5	0,01
QBER, %	3	0	10	1
Длина линии, км	200	200	400	5

реализована в виде программного модуля, который принимает на вход значения параметров протокола и характеристик квантового канала связи и возвращает на выходе данные, показывающие, с какой эффективностью было произведено квантовое распределение ключей при заданных значениях входных параметров.

Важно отметить, что основная часть настоящего исследования (рис. 2–7, 9) посвящена функционированию протокола КРК исключительно в условиях естественных помех, когда ошибки на приемной стороне появляются только вследствие влияния внешних факторов и несовершенства приемо-передающей аппаратуры. Поведение активного злоумышленника в рамках данной статьи моделируется отдельно. Результаты представлены на рис. 8.

Модель принимает следующий набор входных данных:

1) эффективность детектора, %;
2) аттенюация линии, дБ/км;
3) длина линии, км;
4) размер “сырого” ключа, бит;
5) среднее число фотонов на импульс;
6) уровень ошибок-инверсий в канале (QBER), %;
7) проверочная матрица LDPC-кода.

Результатом моделирования является следующий набор выходных значений:

1) длина просеянного ключа, бит;
2) количество итераций исправления ошибок для каждого блока просеянного ключа;
3) общее количество итераций исправления ошибок;
4) длина усиленного ключа, бит.

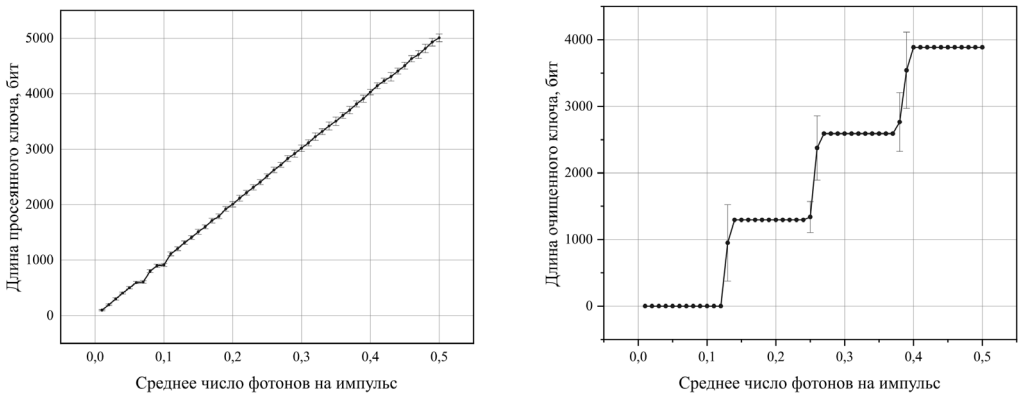
Важно отметить, что для усиления ключа всегда выбирается полином, степень которого совпадает с размером ключа, поэтому размер усиленного ключа может быть уменьшен только вследствие отбрасывания бит, раскрытых на этапе исправления ошибок. При этом следует учитывать, что данная модель усекает просеянный ключ до размера, кратного размеру проверочной матрицы, на этапе исправления ошибок.

С помощью построенной модели была проведена серия экспериментов, направленных на оценку влияния отдельных входных параметров на эффективность процесса квантового распределения ключей. В каждом эксперименте один из входных параметров варьировался в заданных пределах, а остальные – принимали фиксированные значения.

Выбранные значения параметров модели сведены в табл. 3. Под базовым значением понимается фиксированное значение параметра, не варьируемого в данном эксперименте.

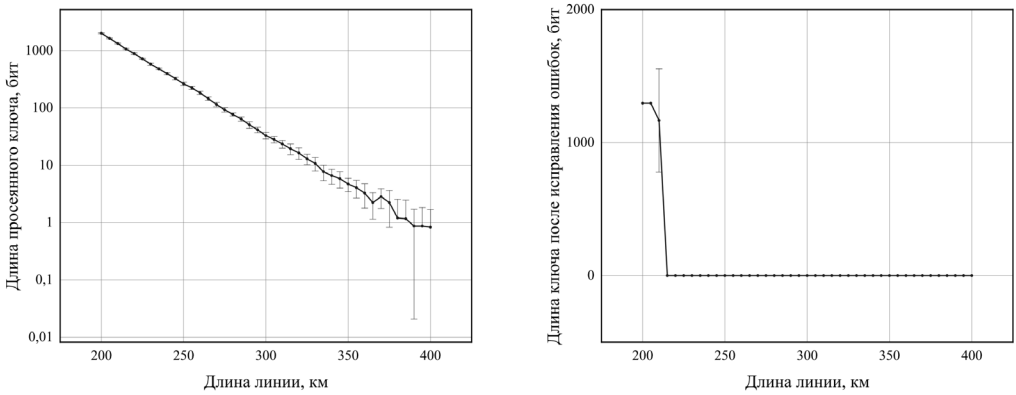
В качестве проверочных матриц LDPC-кода были выбраны две матрицы из стандарта IEEE 802.11n [35]:

- матрица H_1 размера 648×1296;
- матрица H_2 размера 336×672.



а) б)

Рис. 2. Зависимость длины ключа от среднего числа фотонов на импульс: а) для просеянного ключа; б) для очищенного ключа



а) б)

Рис. 3. Зависимость длины ключа от длины линии: а) для просеянного ключа; б) для очищенного ключа

Графики зависимостей, полученных в результате имитационного моделирования процесса квантового распределения ключей по протоколу с фазово-временным кодированием, представлены на рис. 2–9. Каждый эксперимент был выполнен 30 раз с последующим усреднением выходных значений. В результате были получены наборы зависимостей значений всех выходных характеристик от значений параметра модели, варьируемого в рамках данного эксперимента. Длина “сырого” ключа во всех экспериментах принята равной 10^8 бит.

На рис. 2 представлены результаты серии экспериментов, в ходе которых варьировалось среднее число фотонов на импульс. В качестве проверочной матрицы LDPC-кода была выбрана матрица H_1.

На рис. 3 представлены результаты серий экспериментов, в ходе которых варьировалась длина линии. В качестве проверочной матрицы LDPC-кода была выбрана матрица H_1.

На рис. 4–8 представлены результаты экспериментов, в ходе которых варьировалось значение QBER.

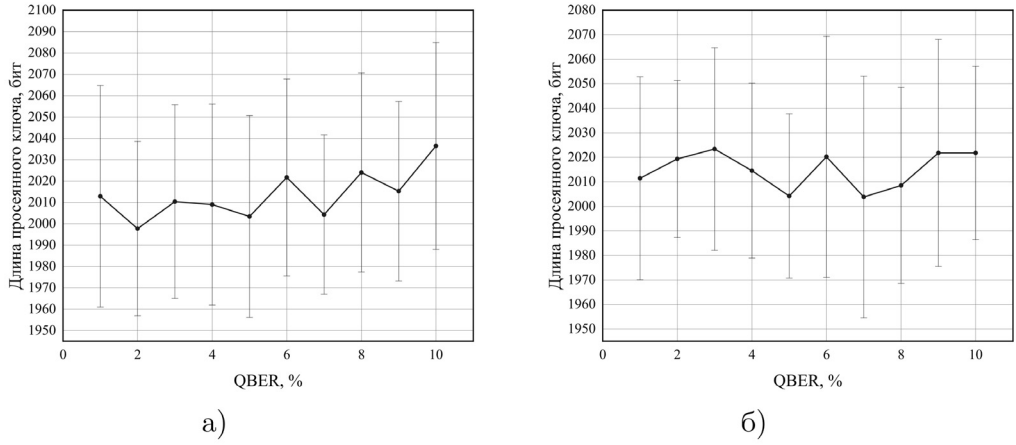


Рис. 4. Зависимость длины просеянного ключа от QBER: а) матрица H_1; б) матрица H_2

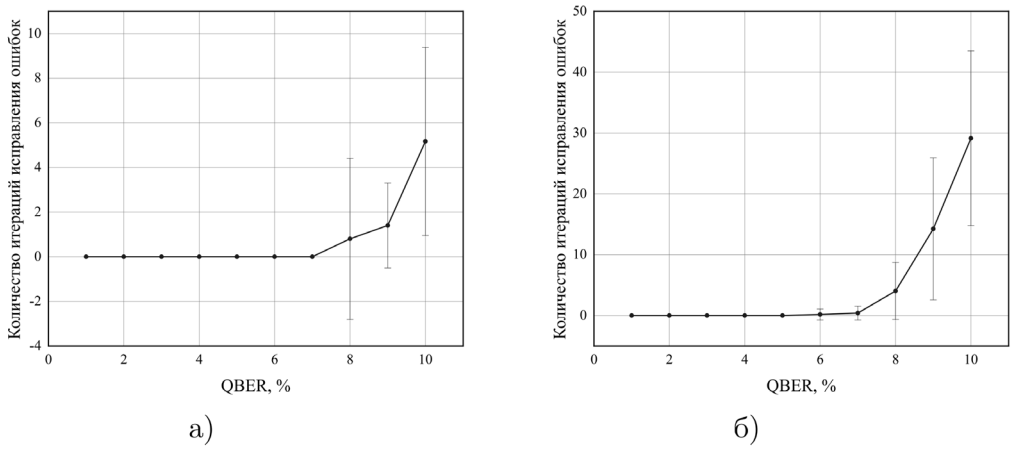


Рис. 5. Зависимость количества итераций исправления ошибок от QBER: а) матрица H_1; б) матрица H_2

На рис. 9 представлены результаты экспериментов, в ходе которых варьировалась эффективность детектора однофотонного излучения.

§ 5. Обсуждение результатов экспериментов

Проведенные эксперименты показывают, что длина просеянного ключа линейно зависит как от среднего числа фотонов на импульс (рис. $2a$), так и от эффективности детектора однофотонного излучения (рис. $9a$). Это объясняется тем, что оба этих параметра влияют на длину “сырого” ключа, биты которого принимает Боб в процессе пересылки квантовых состояний по квантовому каналу.

Графики, показывающие зависимость длины очищенного ключа от параметров протокола и квантового канала, в основном имеют ступенчатый вид ввиду того, что на этапе исправления ошибок ключевая последовательность усекается до длины, соответствующей проверочной матрице LDPC-кода. Незначительные плавные возрастания между плато, равно как и ненулевое значение среднеквадратичного отклонения в данных точках обусловлено тем, что для получения каждой точки на

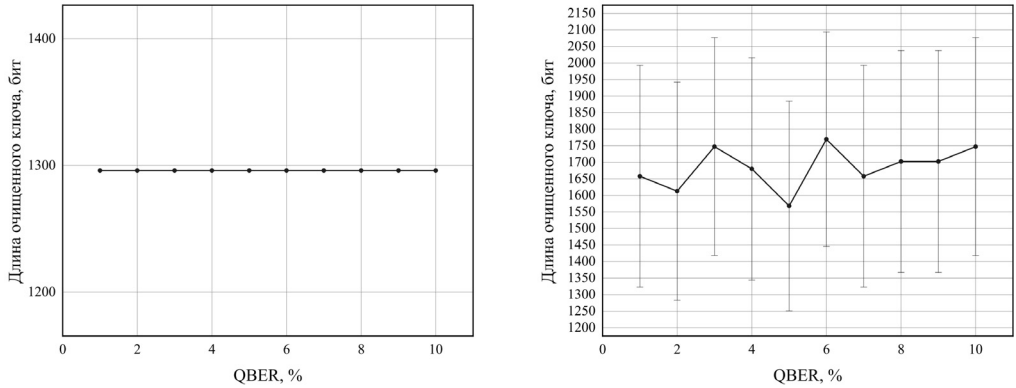


Рис. 6. Зависимость длины очищенного ключа от QBER: а) матрица H_1; б) матрица H_2

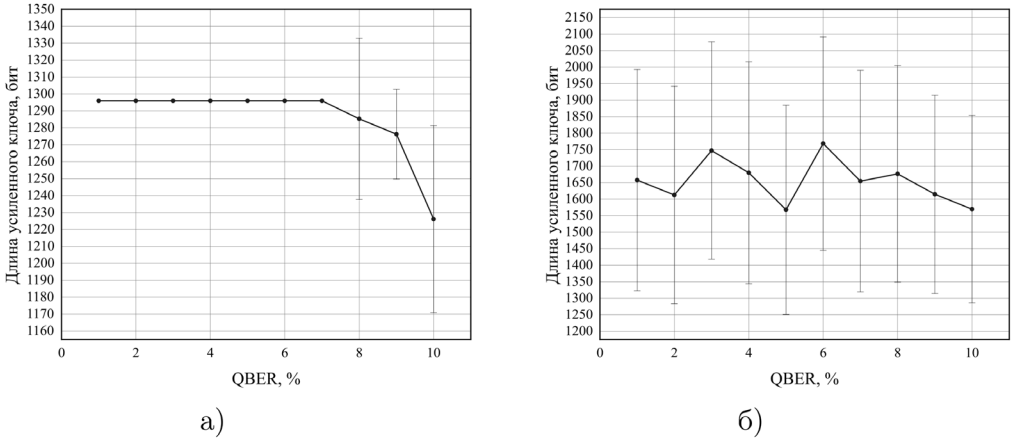


Рис. 7. Зависимость длины усиленного ключа от QBER: а) матрица H_1; б) матрица H_2

графике эксперимент выполнялся 30 раз. Во время каждого выполнения эксперимента Алиса генерировала одно и то же количество случайных двоичных значений, которые детектировались Бобом с некоторой вероятностью, зависящей от заданных входных значений параметров имитационной модели. В результате в качестве просеянного ключа каждый раз были сформированы двоичные последовательности разной длины, одни из которых были усечены до меньшего размера, а другие, длина которых превысила "пороговое" значение, кратное количеству столбцов в проверочной матрице, – до большего.

Исключением является график, показывающий зависимость длины очищенного ключа от QBER для случая, когда в качестве проверочной матрицы LDPC-кода используется матрица H_2, представленный на рис. 6*б*. Отсутствие "ступеней" на данном графике обусловлено тем, что, в отличие от экспериментов, представленных на рис. 2 и рис. 9, в данном эксперименте просеянный ключ уменьшается не настолько значительно. Это происходит потому, что матрица H_2 имеет меньший размер, что позволяет отбрасывать меньшую часть ключа для того, чтобы его размер стал кратен размеру проверочной матрицы. К тому же, это количество под влиянием фактора случайности принимает такие значения, которые от эксперимента к эксперименту приводят к их усечению в разные стороны (т.е. можно сказать, что коли-

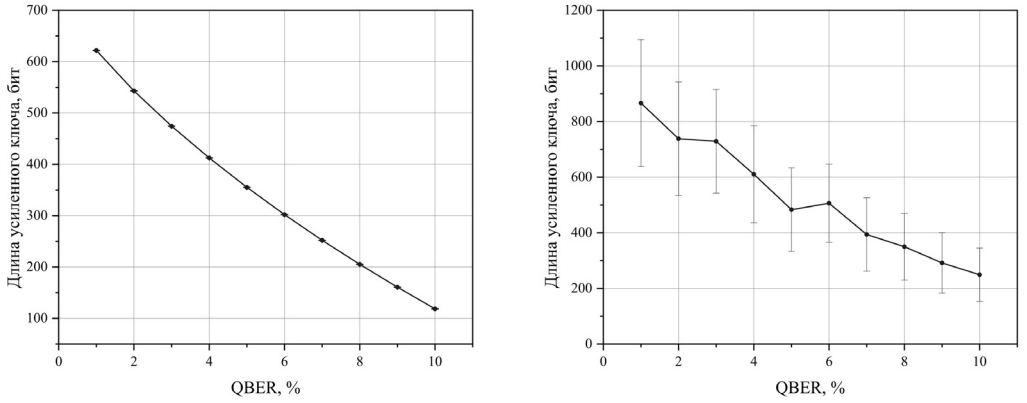


Рис. 8. Зависимость длины усиленного ключа от QBER: а) матрица H_1; б) матрица H_2

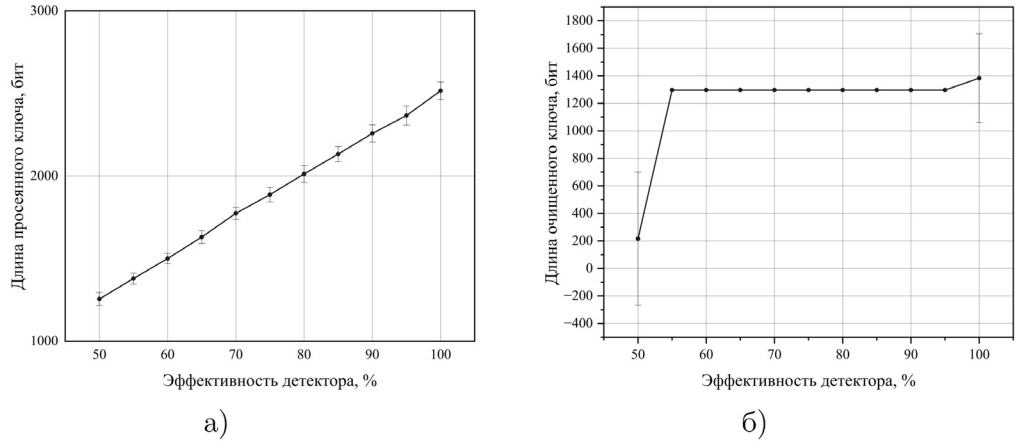


Рис. 9. Зависимость длины просеянного ключа от эффективности детектора: а) для просеянного ключа; б) для очищенного ключа

чество битов варьируется вокруг очередного "порогового" значения на протяжении всего эксперимента). Этим обусловлены более плавные переходы от значения к значению на графике, а также ненулевое значение среднеквадратичного отклонения во всех точках.

Графики зависимости количества итераций исправления ошибок от параметра QBER (рис. 5) показывают, что данная зависимость близка к экспоненциальной для обеих проверочных матриц. Однако разница между выбранными матрицами ярко проявляется на графиках зависимости длины усиленного ключа от QBER (рис. 7). Как видно из данных графиков, при использовании матрицы H_2 ошибка в канале менее заметно влияет на результирующую длину ключевой последовательности. Это может быть обусловлено меньшей размерностью проверочной матрицы и, как следствие, меньшим объемом информации, раскрываемой на этапе исправления ошибок.

Дополнительно был построен график (рис. 8) зависимости длины усиленного ключа от QBER в условиях присутствия на линии пассивного злоумышленника (подслушивателя). Значения для этого графика были рассчитаны по формуле, представленной в [18] и уточненной в [31]. При этом был учтен тот факт, что предпо-

лагаемый злоумышленник может только прослушивать открытый канал, но не совершать активные действия. Как следствие, за вероятность срабатывания детекторов в контрольных временных окнах была принята вероятность темновых отсчетов детекторов (т.е. срабатывания детекторов на вакуумные состояния, которые в случае активности злоумышленника означали бы вмешательство в канал). Как видно на рис. 8, для матрицы H_1 наблюдается меньшая результирующая длина ключа. Прежде всего это обусловлено меньшей длиной просеянного ключа при использовании этой матрицы.

Также, как видно из рис. 3, увеличение длины линии до значения, превышающего 210 км, является практически фатальным при заданной длине "сырого" ключа (10^8 бит). Так, когда длина линии составляет 210 км, длина ключевой последовательности, оставшейся после просеивания, уже недостаточна для формирования хотя бы одного блока, к которому может быть применен выбранный код, исправляющий ошибки. Иная ситуация могла бы наблюдаться при использовании матрицы меньшей размерности, однако, как показывает рис. 3, улучшение было бы незначительным. Данный эксперимент показывает, что формирование ключа для линий длиной чуть более 200 км происходит успешно, но дальнейшее увеличение длины линии может быть проблематичным.

Наконец, как видно из рис. 4, как и следовало ожидать, длина просеянного ключа никак не зависит от ошибки в канале. Флуктуации измеряемого значения обусловлены лишь фактором случайности, так как в данном случае в качестве ошибки в канале рассматриваются ошибки-инверсии, которые никак не влияют на количество битов, принятых Бобом.

Таким образом, результаты имитационного моделирования процесса квантового распределения ключей позволяют сделать следующие выводы о характеристиках исследуемого протокола:

- Наблюдается ступенчатая зависимость результирующего количества ключевой информации от эффективности детектора и среднего числа фотонов на импульс, причем ширина "ступени" зависит от выбранной проверочной матрицы. Следовательно, проверочные матрицы, содержащие меньшее количество столбцов, позволят получать более плавные зависимости.
- Увеличение длины линии имеет значительное влияние на работоспособность протокола в целом. Это говорит о необходимости увеличивать длину просеянных ключей для передачи на более дальние расстояния.
- Несмотря на независимость закона, по которому растет количество итераций исправления ошибок от выбранной матрицы, первая матрица из стандарта IEEE 802.11 позволяет получать меньше потерь результирующей ключевой информации. Поэтому в ходе продолжения работ целесообразно проведение экспериментов с иными проверочными матрицами.

Наконец, в качестве потенциальных направлений дальнейших исследований можно выделить изучение различных модификаций и усовершенствований LDPC-кодов, направленных на повышение эффективности исправления ошибок в КРК, а также их влияния на полученные в данной статье численные показатели.

§ 6. Заключение

В статье было проведено исследование протокола квантового распределения ключей с фазово-временным кодированием и состояниями-ловушками на предмет влияния на него параметров среды передачи и используемых для постобработки ключа алгоритмов. Упрощение и удешевление практической реализации СКРК, использующих данный протокол, а также высокий уровень безопасности, который он обеспечивает, позволяют использовать его в современных системах защищенных коммуникаций. Эксперименты, проведенные с имитационной моделью данного протокола,

позволили численно оценить предельную протяженность линии связи, на которой возможно его стабильное функционирование. Также были получены оценки влияния на полученное значение характеристик аппаратуры, среды передачи и алгоритмов очистки ключа. В результате было установлено, что устойчивое распределение квантовых ключей является возможным на линиях длиной до 210 километров. Более того, было показано, что этот показатель может быть улучшен за счет совершенствования помехоустойчивых кодов, используемых в ходе очистки просеянного ключа.

СПИСОК ЛИТЕРАТУРЫ

1. *Alotaibi B.* A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities // Sensors. 2023. V. 23. № 17. P. 7470 (49 pp.). https://doi.org/10.3390/s23177470
2. *Shokoor F., Shafik W., Matinkhah S.M.* Overview of 5G & Beyond Security // EAI Endorsed Trans. Internet Things. 2022. V. 8. № 30. P. e2 (15 pp.). http://doi.org/10.4108/eetiot.v8i30.1624
3. *Зяблов В.В., Иванов Ф.И., Крук Е.А., Сидоренко В.Р.* О новых задачах в асимметричной криптографии, основанной на помехоустойчивом кодировании // Пробл. передачи информ. 2022. Т. 58. № 2. С. 92–111. https://www.mathnet.ru/rus/ppi2370
4. *Aharonov D.* Quantum Computation // Annual Reviews of Computational Physics VI. Singapore: World Sci., 1999. P. 259–346. https://doi.org/10.1142/9789812815569_0007
5. *Gisin N., Thew R.* Quantum Communication // Nat. Photonics. 2007. V. 1. № 3. P. 165–171. https://doi.org/10.1038/nphoton.2007.22
6. *Wootters W.K., Zurek W.H.* A Single Quantum Cannot Be Cloned // Nature. 1982. V. 299. P. 802–803. https://doi.org/10.1038/299802a0
7. *Холево А.С., Широков М.Е.* О классических пропускных способностях бесконечномерных квантовых каналов // Пробл. передачи информ. 2013. V. 49. № 1. P. 19–36 https://www.mathnet.ru/rus/ppi2099
8. *Перминов Н.С., Смирнов М.А., Нигматуллин Р.Р., Талипов А.А., Моисеев С.А.* Сравнение возможностей гистограмм и метода ранжированных амплитуд при анализе шумов однофотонных детекторов // Компьютерная оптика. 2018. Т. 42. № 2. С. 338–342. https://computeroptics.ru/KO/Annot/KO42-2/420221.html
9. *Акатьев Д.О., Калачев А.А.* Частотная стабилизация однофотонного источника на основе спонтанного параметрического рассеяния света с помощью внешнего электрического поля // Компьютерная оптика. 2016. Т. 40. № 1. С. 26–30. https://doi.org/10.18287/2412-6179-2016-40-1-26-30
10. *Миллер А.В.* Синхронизация времени в спутниковом квантовом распределении ключей // Пробл. передачи информ. 2023. Т. 59. № 4. С. 13–27. https://doi.org/10.31857/S0555292323040022
11. *Bennett C.H., Brassard G.* Quantum Cryptography: Public Key Distribution and Coin Tossing // Theor. Comput. Sci. 2014. V. 560. Part 1. P. 7–11. https://doi.org/10.1016/j.tcs.2014.05.025
12. *Ardehali M., Chau H.F., Lo H.-K.* Efficient Quantum Key Distribution. http://arxiv.org/abs/quant-ph/9803007v4 [quant-ph], 1999.
13. *Ulidowski I., Lanese I., Schultz U.P., Ferreira C.* Reversible Computation: Extending Horizons of Computing – Selected Results of the COST Action IC1405. Lect. Notes Comput. Sci. V. 12070. Cham: Springer, 2020. https://doi.org/10.1007/978-3-030-47361-7
14. *Kiktenko E.O., Trushechkin A.S., Lim C.C.W., Kurochkin Y.V., Fedorov A.K.* Symmetric Blind Information Reconciliation for Quantum Key Distribution // Phys. Rev. Appl. 2017. V. 8. № 4. P. 044017 (12 pp.). https://doi.org/10.1103/PhysRevApplied.8.044017
15. *Kronberg D.A.* New Methods of Error Correction in Quantum Cryptography Using Low-Density Parity-Check Codes // Матем. вопр. криптогр. 2017. Т. 8. № 2. С. 77–86. https://doi.org/10.4213/mvk225

16. *Синильщиков И.В., Молотков С.В.* Состояния “ловушки”, коды коррекции ошибок с низкой плотностью проверок на четность в квантовой криптографии с фазово-временным кодированием // ЖЭТФ. 2019. Т. 156. № 2 (8). С. 205–238. https://doi.org/10.1134/S0044451019080029
17. *Klimov A.N., Balygin K.A., Molotkov S.N.* Two-Parameter Single-Pass Plug and Play Quantum Cryptography without Adjustment of States in the Quantum Channel // Laser Phys. Lett. 2018. V. 15. № 7. P. 075207. https://doi.org/10.1088/1612-202X/aabed7
18. *Molotkov S.N.* Tight Finite-Key Analysis for Two-Parametric Quantum Key Distribution // Laser Phys. Lett. 2019. V. 16. № 3. P. 035203. https://doi.org/10.1088/1612-202X/aafcaf
19. *Молотков С.Н.* О стойкости систем квантовой криптографии с фазово-временным кодированием к атакам активного зондирования // ЖЭТФ. 2020. Т. 158. № 6 (12). С. 1011–1031. https://doi.org/10.31857/S0044451020120019
20. *Dieks D.* Communication by EPR Devices // Phys. Lett. A. 1982. V. 92. № 6. P. 271–272. https://doi.org/10.1016/0375-9601(82)90084-6
21. *Bechmann-Pasquinucci H., Gisin N.* Incoherent and Coherent Eavesdropping in the Six-State Protocol of Quantum Cryptography // Phys. Rev. A. 1999. V. 59. № 6. P. 4238–4248. https://doi.org/10.1103/PhysRevA.59.4238
22. *Сыч Д.В., Гришанин Б.А., Задков В.Н.* Анализ предельно возможных информационных характеристик протоколов квантовой криптографии // Квантовая электроника. 2005. Т. 35. № 1. С. 80–84. https://www.mathnet.ru/rus/qe2886
23. *Kurochkin Y.* Quantum Cryptography with Floating Basis Protocol // Quantum Informatics 2004. Proc. SPIE. V. 5833. P. 213–221. https://doi.org/10.1117/12.620510
24. *Scarani V., Acín A., Ribordy G., Gisin N.* Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations // Phys. Rev. Lett. 2004. V. 92. № 5. P. 057901 (4 pp.). https://doi.org/10.1103/PhysRevLett.92.057901
25. *Huttner B., Imoto N., Gisin N., Mor T.* Quantum Cryptography with Coherent States // Phys. Rev. A. 1995. V. 51. № 3. P. 1863–1869. https://doi.org/10.1103/PhysRevA.51.1863
26. *Hwang W.-Y.* Quantum Key Distribution with High Loss: Toward Global Secure Communication // Phys. Rev. Lett. 2003. V. 91. № 5. P. 057901 (4 pp.). https://doi.org/10.1103/PhysRevLett.91.057901
27. *Лебедев А.Н., Соколов А.В.* Квантовое распределение ключей с доверенным центром // Сб. трудов 7-й всероссийской научно-технической конференции “Безопасные информационные технологии” (БИТ-2016). Москва, 16–17 ноября 2017 г. М.: МГТУ им. Н.Э. Баумана, 2016. С. 189–193.
28. *Kravtsov K.S., Molotkov S.N.* Practical Quantum Key Distribution with Geometrically Uniform States // Phys. Rev. A. 2019. V. 100. № 4. P. 042329 (7 pp.). https://doi.org/10.1103/PhysRevA.100.042329
29. *Brassard G., Lütkenhaus N., Mor T., Sanders B.C.* Limitations on Practical Quantum Cryptography // Phys. Rev. Lett. 2000. V. 85. № 6. P. 1330–1333. https://doi.org/10.1103/PhysRevLett.85.1330
30. *Gallager R.G.* Low-Density Parity-Check Codes // IRE Trans. Inform. Theory. 1962. V. 8. № 1. P. 21–28. https://doi.org/10.1109/TIT.1962.1057683
31. *Кронберг Д.А.* Уязвимость квантовой криптографии с фазово-временны́м кодированием в условиях затухания // ТМФ. 2023. Т. 214. № 1. С. 140–152. https://doi.org/10.4213/tmf10326
32. *Lo H.K., Ma X., Chen K.* Decoy State Quantum Key Distribution // Phys. Rev. Lett. 2005. V. 94. № 23. P. 230504 (4 pp.). https://doi.org/10.1103/PhysRevLett.94.230504
33. *Wang X.-B.* Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography // Phys. Rev. Lett. 2005. V. 94. № 23. P. 230503 (4 pp.). https://doi.org/10.1103/PhysRevLett.94.230503
34. *Ma X., Qi B., Zhao Y., Lo H.-K.* Practical Decoy State for Quantum Key Distribution // Phys. Rev. A. 2005. V. 72. № 1. P. 012326 (15 pp.). https://doi.org/10.1103/PhysRevA.72.012326

35. IEEE 802.11n-2009: IEEE Standard for Information Technology — Local and Metropolitan Area Networks — Specific Requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput. IEEE, 2009. https://doi.org/10.1109/IEEESTD.2009.5307322

Морозов Владимир Игоревич
Евсютин Олег Олегович
Нефедов Сергей Игоревич
Национальный исследовательский университет
"Высшая школа экономики", Москва
vimorozov@hse.ru
oevsyutin@hse.ru
snefedov@hse.ru

Поступила в редакцию
09.08.2024
После доработки
18.02.2025
Принята к публикации
18.03.2025

ON THE IMPACT OF HARDWARE AND ALGORITHMIC SOFTWARE PARAMETERS ON THE ACHIEVABLE LINE LENGTH FOR A QUANTUM KEY DISTRIBUTION PROTOCOL WITH PHASE-TIME CODING

© 2025 **V.I. Morozov, O.O. Evsyutin, S.I. Nefedov**

Higher School of Economics—National Research University, Moscow
vimorozov@hse.ru, oevsyutin@hse.ru, snefedov@hse.ru

Quantum key distribution is one of perspective directions of modern cryptography. It allows the parties of information exchange to develop a common cryptographic key, the secrecy of which is ensured by the laws of quantum mechanics. The paper studies the influence of the characteristics of the quantum channel, as well as the parameters of the applied algorithms on the maximum achievable length of a communication line for a protocol with phase-time coding and decoy states. By computational experiments with a simulation model of a quantum key distribution system based on the above protocol, it was found that the stable operation of the protocol is possible with line length of at most 210 km. It was also shown that this value can be increased by constructing more efficient sifted key correction algorithms.

Keywords: quantum cryptography, quantum key distribution, noise-resistant coding, LDPC codes

DOI: 10.31857/S0555292325010024, **EDN:** MVBFJF

Received 09.08.2024
Revised 18.02.2025
Accepted 18.03.2025