DOI 10.37882/2223–2966.2023.02.26

МОДИФИКАЦИЯ КЛАССИЧЕСКОГО КВАНТОВОГО ПРОТОКОЛА BB84, ПОВЫШАЮЩАЯ ЕГО ХАРАКТЕРИСТИКИ

MODIFICATION OF THE CLASSICAL QUANTUM PROTOCOLBB84, INCREASING ITS CHARACTERISTICS

K. Lyashenko
V. Porksheyan
L. Cherkesova
E. Revyakina
I. Yengibaryan
O. Buryakova
O. Reshetnikova

Summary. The article draws the attention to the field of quantum cryptography, namely, to its specific section concerning the development of quantum cryptographic protocols, on the creation of which scientists from various countries have been working for almost forty years. Quantum cryptography is considered today as the technology capable to form the new unique appearance of telecommunication networks of the future. However, at the same time, no one with full confidence can to predict guaranteed what fully formed quantum Internet infrastructure will look like, and what outcome it may lead to. The article puts forward new hypothesis regarding the universal improvement of quantum protocols, using the example of modification of the classical quantum protocol BB84. The application of the idea put forward by the authors is based on the theory of artificial manufactured reconstruction of photons and their further use, which makes it possible to significantly reduce the possibility of potential threats, as well as to avoid situations associated with vulnerabilities of quantum algorithms. The proposed method is combined. By applying false photon states and creating many traps for intruders, it is possible to achieve such increasing in the resources spent on the attack that will make this attack, in the end, the useless occupation. Any hacker will be much less likely to guess the desired data transfer qubit and the quantum state of polarization. Simulated copies of photons, in addition to their main task, can become bait for any hacker, capable of driving him into the trap, thereby confirming his presence in the communication channel. At the same time, the process of breaking the communication channel will no longer be inevitable, which will avoid interrupting the functioning of the communication line.

Keywords: quantum protocols, quantum cryptography, modification of the BB84 quantum protocol, quantum key distribution, error threshold.

Ляшенко Кирилл Александрович
Донской государственный технический университет
reusn@mail.ru
Поркшеян Виталий Маркосович
К.ф.-м.н, доцент, Донской государственный технический университет
spu-40@donstu.ru
Черкесова Лариса Владимировна
Д.ф.— м.н., Донской государственный технический университет
chia2002@inbox.ru
Ревякина Елена Александровна
К.т.н., Донской государственный технический университет
revyelena@yandex.ru
Енгибарян Ирина Алешаевна
К.т.н., Донской государственный технический университет
eirina@live.ru
Бурякова Ольга Сергеевна
К.ф.н., Донской государственный технический университет
buryakovaos@yandex.ru
Решетникова Ольга Александровна
Российская Таможенная Академия, Ростовский филиал
irina_reshetnikova@mail.ru

Аннотация. Статья привлекает внимание к области квантовой криптографии, а именно, к её конкретному разделу, касающемуся разработке квантовых криптографических протоколов, над созданием которых учёные различных стран работают уже почти сорок лет. Квантовая криптография сегодня рассматривается как технология, способная сформировать новый уникальный облик телекоммуникационных сетей связи будущего. Однако, при этом никто с полной уверенностью не может гарантированно спрогнозировать, как будет выглядеть полностью сформированная инфраструктура квантового интернета, и к какому итогу она может привести. В статье выдвигается новая гипотеза относительно универсального усовершенствования квантовых протоколов, на примере модификации классического квантового протокола BB84.Использование выдвинутой авторами идеи основано на теории рукотворного воссоздания фотонов и их дальнейшего использования, что позволяет значительно снизить возможность осуществления потенциальных угроз, а также избежать ситуаций, связанных с уязвимостями квантовых алгоритмов. Предлагаемый метод является комбинированным. Применяя ложные состояния фотонов и создавая множество ловушек для злоумышленников, можно добиться такого увеличения ресурсов, затрачиваемых на атаку, что сделает эту атаку, в итоге, бесполезным занятием. Хакер будет иметь гораздо

меньшую вероятность угадать нужный кубит передачи данных и квантовое состояние поляризации. Смоделированные копии фотонов, помимо своей основной задачи, могут стать приманкой для хакера, способной загнать его в ловушку, тем самым подтверждая его присутствие в канале связи. При этом процесс обрыва канала связи станет уже вовсе не неизбежным, что позволит избежать прерывания функционирования линии связи.

Ключевые слова: квантовые протоколы, квантовая криптография, модификация квантового протокола BB84, квантовое распределение ключа, порог ошибок.

Введение

На данном этапе развития информационных технологий квантовые вычисления позволяют не только обеспечить повышенную защиту от несанкционированного доступа к передаваемой информации, но и с более высокой долей вероятности выявить сам факт такой попытки. Этот аспект крайне важен на современном уровне информационного общества, поскольку оно стремится, фактически, к полной цифровизации. Вместе с этим процессом, происходит ускоренная глобальная модернизация как аппаратного, так и программного обеспечения, возрастают нагрузки на техническое оснащение, увеличиваются объёмы информации, в том числе компрометирующей тех или иных людей. При этом неизбежно возрастает количество инцидентов кибербезопасности, модернизируются способы угроз, возникают новые виды кибератак, вызывающих серьёзные проблемы в области информационной безопасности и защиты данных. Поддержание работоспособности технического оснащения в коммуникационных сетях всё более усложняется.

Так, например, недавняя кибератака на Японию (в мае 2022 года) частично парализовало общественную деятельность граждан и вызвало серьёзные проблемы в правительственном аппарате. Другие страны ежесуточно также сталкиваются с подобными случаями, а в некоторых случаях государственные структуры становятся практически беспомощными. Представители многих государств крайне обеспокоены перспективами кибервойн, и гораздо серьёзнее взялись за реализацию процесса перехода на квантовое решение данной проблемы.

Недалек тот момент, когда процесс модернизации средств, имеющихся в арсенале современной кибербезопасности, упрётся в тупик, и тогда переход на квантовые технологии станет повсеместной неизбежностью. Вот почему правительства многих стран возлагают большие надежды на квантовые технологии. Статья направлена на понимание основ работы квантового протокола BB84 и его модификаций, на их сравнение в криптостойкости, и на их дальнейшую модернизацию. За пример взяты два хорошо известных протокола: уже устаревший, но по–прежнему конкурентоспособный алгоритм BB84, и его модификация BB84 Info–Z. Понимание основ и принципов работы квантовых протоколов становится необходимостью для многих специалистов в области информационной безопасности. Показаны приоритетные направления развития систем квантового распределения ключей, и на основе законов квантовой механики объясняются методы построения безопасных квантовых протоколов передачи данных.

Предлагаемая методология

Квантовый протокол BB84

Этот протокол назван по фамилиям его создателей и году его первого опубликования [1]. BB84 предназначен для передачи секретной информации, закодированной бинарным образом. На рис. 1 показано, как в BB84 может быть закодирован $бит$ в состоянии поляризации фотона.

Двоичный ноль (0) определяется как поляризация 0^{o} в прямолинейном координатном базисе, или 45^{o} — в диагональном базисе. Двоичная единица (1) может быть равна 90^{o} в прямолинейном базисе, или 135^{o}– в диагональном базисе. Итак, бит может быть представлен с помощью поляризации фотона в одном из двух координатных базисов.

На моменте согласования, абоненты канала связи Алиса и Боб утверждают большое целое число n, порог ошибок p_a и линейный код исправления ошибок C, а также матрицу проверки чётности P_C порядка $r \times n$. Согласовываются также линейная функция генерации ключей (для усиления конфиденциальности), представленная матрицей P_K порядка $m \times n$. Эти матрицы могут быть известны заранее, или определены во время выполнения протокола и отправлены по классическому

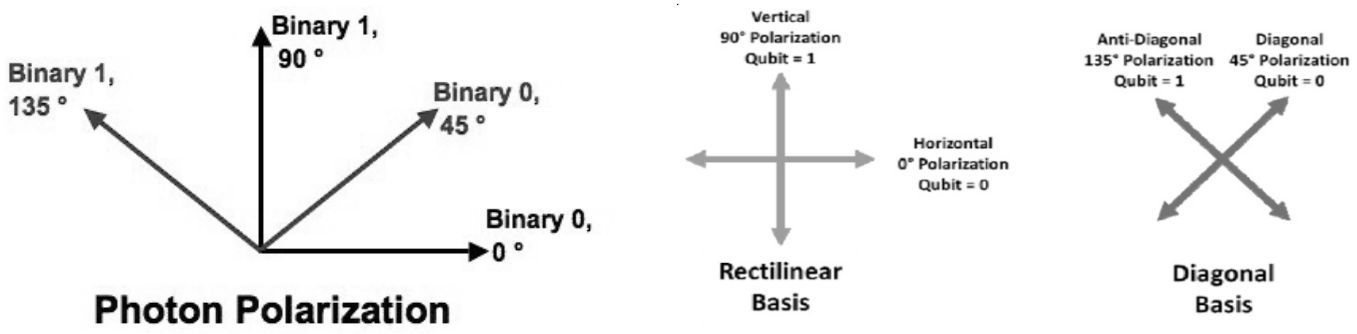

Рис. 1: Битовое кодирование квантового протокола BB84

Бит Алисы	0	1	1	0	1	0	0	1
Базис Алисы	+	+	X	+	X	X	X	+
Поляризация Алисы	↑	→	↖	↑	↖	↗	↗	→
Базис Боба	+	X	X	X	+	X	+	+
Измерение Боба	↑	↗	↖	↗	→	↗	→	→
Просеянный ключ	0		1			0		1

Рис. 2. Просеянный ключ

каналу. В свою очередь, матрица $(r + m) \times n$, строки которой являются строками P_C и P_K, вместе взятыми, должна иметь ранг $r + m$. Алиса случайно выбирает последовательности битов: $2n$–битовые строки $i, b \in F_2^{2n}$, где F_2 обозначает поле из двух элементов с элементами {0; 1}, то есть поле целых чисел по модулю 2.

Затем кодируется состояние $|i^b\rangle = |i_1^{b_1}\rangle \dots |i_{2n}^{b_{2n}}\rangle$. Для каждого бита, случайным образом выбирается базис, прямолинейный или диагональный, с помощью которого будет кодироваться бит. При передаче фотона от Алисы, Боб будет сообщать ей о получении фотона, но не будет измерять его. Для каждого фотона, который получает Боб, он будет измерять поляризацию фотона на случайно выбранном базисе, применяя к своему состоянию. Если для конкретного фотона Боб выбрал тот же координатный базис, что и Алиса, когда он выполнял преобразование $H^b = H^{b_1} \otimes \dots \otimes H^{b_{2n}}$, то фотон переходит в состояние $|i\rangle = |i_1 \dots i_{2n}\rangle$. Боб должен измерить эту же поляризацию в i^{B} строке, и, таким образом, корректно вывести бит, который отправила Алиса, в случае отсутствия шума и признаков подслушивания на линии связи.

Для определения подслушивания Алиса случайным образом выберет n бит, которые будут использоваться для обнаружения подслушивания. Путём выбора $2n$–битной строки, содержащей ровно n единиц, Алиса добивается, чтобы $|s| = n$. Алиса отправляет Бобу публично s бит, таких, что $s_j = 0$, которые используются для тестирования, а остальные — для генерации окончательного ключа. Обозначив соответствующие подстроки i, b, релевантные для тестирования i_s и b_s, в то время как подстроки, релевантные для создания ключа, обозначаются i_s и b_s. Для каждого $j \in [1..2n]$, такого, что $s_j = 0$, Алиса и Боб публикуют значение j*–го* бита.

Если Боб выбрал неправильный базис, то его результат и, следовательно, бит, который он получил, будут случайными. Стоит отметить, что если несовпадение битов, определённое в опубликованных значениях j–го бита путём сравнения, превышает np_a, то они прерывают выполнение протокола. Предварительно зафиксированный параметр протокола p_a, на самом деле, является соотношением разрешённых переворотов битов для тестирования. Алиса и Боб хранят значения оставшихся n бит в секрете. Строка Алисы обозначается $x = i_s$ и называется *информационной строкой*. Соответствующая цепочка битов на стороне Боба обозначается x^{B}.

На втором этапе, Боб уведомит Алису по любому незащищенному каналу, какой базис он использовал для измерения каждого фотона. Алиса сообщает Бобу, правильно ли он выбрал базис для каждого фотона. На этом этапе Алиса и Боб отбрасывают биты, соответствующие фотонам, которые Боб измерил с другим базисом. При условии, что ошибок не произошло или

никто не манипулировал фотонами, Боб и Алиса теперь должны иметь одинаковую строку битов, которая называется *просеянным ключом*. В приведенном ниже примере (рис. 2) показаны биты, которые выбрала Алиса; базисы, в которых она их закодировала; а также базисы, которые Боб использовал для измерения. Кроме того, на рис. 2представлен полученный просеянный ключ, после того этапа, когда Боб и Алиса отбросили свои биты, как было показано выше.

Однако, прежде чем они закончили, Алиса и Боб согласовывают случайное подмножество битов для сравнения, чтобы гарантировать согласованность. Для проверки, Алиса отправляет Бобу r–битовую строку исправления ошибок. Боб будет использовать ξ для сравнения или необходимого исправления своей строки x^{B}. Строка $\xi = xP_C^T$ называется *синдромом* строки x (относительно P_C). Если биты совпадают, то они отбрасываются, а оставшиеся биты образуют общий секретный m–битовый ключ. В отсутствие шума или любой другой ошибки измерения, несоответствие в любом из сравниваемых битов указывало бы на присутствие перехватчика в квантовом канале. Это связано с тем, что если бы перехватчик Ева пыталась определить ключ, то у неё не было бы другого выбора, кроме как измерить фотоны, посланные Алисой, прежде чем отправлять их Бобу. То есть, Ева присоединяет отдельный зонд, который, как мы предполагаем, находится в чистом состоянии, и применяет унитарное преобразование U_jк составной системе. Это верно, потому что теорема о запрете клонирования [2] гарантирует, что Ева не может воспроизвести частицу неизвестного состояния.

Поскольку Ева не будет знать, какие базисы Алиса использовала для кодирования бита, пока Алиса и Боб не обсудят свои измерения, Ева будет вынуждена угадывать. Если она измеряет на неправильных базисах, то принцип неопределенности Гейзенберга гарантирует, что информация, закодированная на других базисах, теперь будет потеряна.

Таким образом, когда фотон достигает Боба, его измерение будет случайным, и он будет считывать некорректную информацию в 50% случаев. Учитывая, что Ева будет неправильно выбирать базис измерения в среднем в 50% случаев, 25% битов, измеренных Бобом, будут отличаться от битов Алисы. Если Ева перехватила все биты, то после n–битных сравнений Алисы и Боба, они уменьшат вероятность того, что Ева останется незамеченной до $\frac{3}{4}n$.

Таким образом, вероятность того, что перехватчик Ева узнала секрет, ничтожно мала, если сравнивается достаточно длинная последовательность битов.

Протокол BB84-INFO-Z

Рассматриваемая модификация BB84, квантовый протокол BB84–INFO–Z является аналогией BB84 [3], за исключением того, что он использует:

- обобщенные битовые номера n, n_Z и n_X (n – информационные битовые номера, Z и X — тестовые биты, соответственно);
- раздел $P = (s, z, b)$ для разделения N–битной строки i на три непересекающихся набора индексов (I, T_Z и T_X);
- два отдельных порога ($p_{A,Z}$ и $p_{A,X}$) вместо одного (p_A).
- До начала запуска квантового протокола BB84–INFO–Z, Алиса и Боб должны выбрать некоторые общие, или публичные, параметры:
- номера n, n_z и n_x (обозначим $N = n + nz + nx$);
- пороги ошибок $P_{A,Z}$ *и* $P_{A,X}$, $r \times n$ (соответствующие линейному коду исправлению ошибок C);
- матрицы усиления конфиденциальности $m \times n$ (представляющие собой функцию генерации линейного ключа).

Важно, чтобы все строки $R+M$ рассмотренных ранее матриц P_C и P_K были собраны таким образом, чтобы они были линейно независимыми.

Алиса, случайным образом, выбирает раздел $\mathcal{P} = (s,z,b)N$–битных строк, случайно выбирая N–битные строки $s,z,b \in F_2^N$, которые удовлетворяют соотношениям:

| s | = n, | z | = n_z, | B | = n_z, и | s + z + b | = N.

Итак, раздел $\mathcal{P}$ разбивает набор индексов $\{1, 2, \ldots, N\}$ на три непересекающихся набора:

- I (информационные биты, где s_j = 1) размера n;
- T_z (тестовые Z биты, где z_J = 1) размера n_Z; а также
- T_x (тестовые Хбиты, где b_j = 1) размером n_X.

Алиса случайным образом выбирает N–битную строку $i \in F_2^N$ и отправляет N кубитовых состояний $\left|i_2^{b_1}\right\rangle, \left|i_2^{b_2}\right\rangle, \ldots, \left|i_N^{b_N}\right\rangle$, один за другим по квантовому каналу. Алиса использует базис Z для отправки информации тестовых Z–битов, а также базис Xдля отправки X–битов. Первоначально Боб держит каждый полученный кубит в квантовой памяти, не измеряя его.

Далее Алиса посылает Бобу по классическому каналу битовую строку $b = b_1 \ldots b_N$. Боб измеряет каждый из кубитов, которые он сохранил. При измерении i–го кубита, он измеряет его в Z–базисе, если b_i = 0, и он измеряет его в X–базисе если b_i = 1. Битовая строка, измеренная Бобом, обозначается i^{B}. Если нет шума и нет подслушивания, то битовая строка равна $i^{\mathrm{B}} = i$.

После этого Алиса посылает Бобу битовую строку s. Информационные биты (которые будут использоваться для создания окончательного ключа) являются n битами $s_j = 1$, в то время как тестовые Z и X биты (которые будут использоваться для тестирования), являются битами $n_z + n_x$ *с* $s_j = 0$. Подстроки обозначаются i, b, они соответствуют информационным битам i_sи b_s соответственно.

Далее, Алиса и Боб оба публикуют битовые значения, которые они имеют для всех тестовых Z и X битов, а затем сравнивают значения битов. Если большее количество, чем $n_z \cdot p_{a,z}$ тестовых Z–битов у Алисой с Бобом отличается, или больше, чем $n_x \cdot p_{a,x}$ тестовых X–битов отличаются между ними, то они прерывают протокол, где $p_{a,z}$и $p_{a,x}$– предварительно согласованные пороги ошибок. Значения оставшихся n битов (INFO биты с s_j = 1) Алиса и Боб хранят в секрете. Битовая цепочка Алисы обозначается как $x = i_s$, а битовая строка Боба обозначает x^{B}.

Алиса посылает Бобу *синдром* X (в отношении кода исправления ошибок C и его соответствующей проверки чётности матрицы P_C), который состоит из r бит и определяется как $\xi = xP_C^T$. Используя ξ, Боб исправляет ошибки в его строке x^{B} (так же, как x). Окончательный ключ состоит из m–битов и определяется как $k = xP_K^T$. Алиса и Боб вычисляют биты и ключ в целом.

Очевидно, что оба протокола очень похожи. Рассмотрим их защищённость против коллективных атак [4–5], которые являются одними из самых мощных теоретических атак.

Реализация атаки Евы и описание её свойств

К каждому *j*-мукубиту

$$\left|i_j^{b_j}\right\rangle_{T_j},$$

посланному Алисой $(1 \le j \le N)$, Ева присоединяет отдельный зонд, находящийся, как предполагается, в чистом состоянии, и применяет унитарное преобразование U_jк составной системе. Затем она сохраняет свои зонды в квантовой памяти для последующего измерения, и отправляет Бобу его часть системы [6]. Для каждого кубита существует определенное пробное гильбертово пространство и определенное U_j; они заранее определяются Евой и, таким образом, являются фиксированными для всех возможных вариантов выбора i, b и s.

Атака Евы на отдельный кубит

Так как атака является *побитовой*, то можно сосредоточить анализ на некотором фиксированном кубите, временно отбросив субиндекс j и выразив глобальный эффект действия Евы на конкретный кубит относительно базиса $|0^b\rangle, |1^b\rangle$:

$$U|0^E\rangle|0^b\rangle = |E_{00}^b\rangle|0^b\rangle + |E_{01}^b\rangle|1^b\rangle = |\phi_0^b\rangle \quad (1)$$

$$U|0^E\rangle|1^b\rangle = |E_{10}^b\rangle|0^b\rangle + |E_{11}^b\rangle|1^b\rangle = |\phi_1^b\rangle \quad (2)$$

где $|E_{00}^b\rangle, |E_{01}^b\rangle, |E_{10}^b\rangle$ и $|E_{11}^b\rangle$ представляют собой векторы («ненормированные состояния») в пробном гильбертовом пространстве Евы, соответствующие этому конкретному кубиту. Поскольку U унитарен, $|\phi_0^b\rangle$ и $|\phi_1^b\rangle$ имеют норму 1 и ортогональны. Это значит, что

$$\langle E_{00}^b|E_{00}^b\rangle + \langle E_{01}^b|E_{01}^b\rangle = 1 \quad (3)$$

$$\langle E_{10}^b|E_{10}^b\rangle + \langle E_{11}^b|E_{11}^b\rangle = 1 \quad (4)$$

$$\langle E_{00}^b|E_{10}^b\rangle + \langle E_{01}^b|E_{11}^b\rangle = 0 \; \langle E_{10}^b|E_{00}^b\rangle + \langle E_{11}^b|E_{01}^b\rangle = 0 \quad (5)$$

Распространение атаки на несколько кубитов — коллективная атака

Для каждого кубита $j \in [1..2n]$ Ева применяет U_j в пространстве $\mathcal{H}_j^E \otimes \mathcal{H}_2$, где $\mathcal{H}_j^E$– пробное пространство Евы, $\mathcal{H}_2$ — пространство кубитов. Выраженный относительно точки зрения Евы базис b_j, получается путём отслеживания Боба из состояний

$$\left|\phi_0^{b_j}\right\rangle_j \text{ и } \left|\phi_1^{b_j}\right\rangle_j,$$

в результате чего получаются следующие матрицы плотности:

$$\left(\rho_0^{b_j}\right)_j = \left|E_{00}^{b_j}\right\rangle_j \langle E_{00}^{b_j}| + \left|E_{01}^{b_j}\right\rangle_j \langle E_{01}^{b_j}| \quad (6)$$

$$(\rho_1^{b_j})_j = \left|E_{10}^{b_j}\right\rangle_j \langle E_{10}^{b_j}| + \left|E_{11}^{b_j}\right\rangle_j \langle E_{11}^{b_j}| \quad (7)$$

Если Алиса отправляет строку i, используя основы b, то глобальное состояние Евы является тензорным произведением этих состояний

$$\left(\rho_{i_j}^{b_j}\right)_j.$$

После раскрытия тестовых битов [7], Еве нужны только те

$$\left(\rho_{i_j}^{b_j}\right)_j,$$

для которых $s_j = 1$. Множество $\{j \,|s_j = 1\}$ имеет n элементов и является глобальным. Глобальное соответствующее s, b и x, теперь можно записать как:

$$\rho_x^{b_s} = \left(\rho_{i_{j_1}}^{b_{j_1}}\right)_{j_1} \otimes \ldots \otimes \left(\rho_{i_{j_n}}^{b_{j_n}}\right)_{j_n} = \bigotimes_{l=1}^{n} \left(\rho_{i_{j_l}}^{b_l}\right)_{j_l} \quad (8)$$

Вероятность ошибки

Если предположить, что кубит подвергается атаке U, как определено в (1) и (2), то ошибка возникает, если Алиса отправляет 0, а Боб измеряет 1, или если Алиса отправляет 1, а Боб измеряет 0. Пусть k будет значением, измеренным Бобом, i– значение, отправленное Алисой для определенного кубита, аb– базис, используемый Алисой для кодирования i.

Тогда вероятность измерения Бобом ошибки выражается

$$p_\epsilon^b \triangleq \frac{1}{2}\left[\langle E_{01}^b|E_{01}^b\rangle + \langle E_{10}^b|E_{10}^b\rangle\right] \quad (9)$$

Вероятность ошибки в сопряженном базисе

Теперь нас интересует величина $p_e^{\bar{b}}$, где $\bar{b} = 1 - b$ (т.е. $\bar{0} = 1$ и $\bar{1} = 0$) соответствует базису, сопряженному к тому, что дано b. Атака U всегда описывается формулами (1) и (2) в базисе b, но для того, чтобы вычислить вероятность или ошибку, когда Алиса кодирует i_j как $|i_j^{\bar{b}}\rangle$ вместо $|i_j^b\rangle$, теперь нужно выразить U в основе $\bar{b}$.

Из уравнения (9) известно, что вероятность ошибки для этой ситуации определяется как:

$$p_\epsilon^{\bar{b}} = \frac{1}{2}\left[\langle E_{01}^{\bar{b}}|E_{01}^{\bar{b}}\rangle + \langle E_{10}^{\bar{b}}|E_{10}^{\bar{b}}\rangle\right].$$

Используя тот факт, что

$$|0\rangle^{\bar{b}} = \frac{1}{\sqrt{2}}\left[|0^b\rangle + |1^b\rangle\right], |1\rangle^{\bar{b}} = \frac{1}{\sqrt{2}}\left[|0^b\rangle - |1^b\rangle\right]$$

и используя линейность U, из соотношений (1) и (2) выводятся выражения:

$$U|0^E\rangle|0^{\bar{b}}\rangle = \tfrac{1}{\sqrt{2}}\left(|E_{00}^b\rangle + |E_{10}^b\rangle\right)|0^b\rangle + \tfrac{1}{\sqrt{2}}\left(|E_{01}^b\rangle + |E_{11}^b\rangle\right)|1^b\rangle, \quad (11)$$

$$U|0^E\rangle|1^{\bar{b}}\rangle = \tfrac{1}{\sqrt{2}}\left(|E_{00}^b\rangle - |E_{10}^b\rangle\right)|0^b\rangle + \tfrac{1}{\sqrt{2}}\left(|E_{01}^b\rangle - |E_{11}^b\rangle\right)|1^b\rangle. \quad (12)$$

Заменив $|0^b\rangle$ и $|1^b\rangle$ в правых частях выражений на их значения в терминах $|0^{\bar{b}}\rangle$ и $|1^{\bar{b}}\rangle$, т.е.

$$|0^b\rangle = \tfrac{1}{\sqrt{2}}\left[|0^{\bar{b}}\rangle + |1^{\bar{b}}\rangle\right] \text{ и } |1^b\rangle = \tfrac{1}{\sqrt{2}}\left[|0^{\bar{b}}\rangle + |1^{\bar{b}}\rangle\right]$$

получаем

$$U|0^E\rangle|0^{\bar{b}}\rangle = \tfrac{1}{2}\left[|E_{00}^b\rangle + |E_{10}^b\rangle + |E_{01}^b\rangle + |E_{11}^b\rangle\right]|0^{\bar{b}}\rangle + \\ + \tfrac{1}{2}\left[\left(|E_{00}^b\rangle - |E_{11}^b\rangle\right) + \left(|E_{10}^b\rangle - |E_{01}^b\rangle\right)\right]|1^{\bar{b}}\rangle \quad (13)$$

$$U|0^E\rangle|1^{\bar{b}}\rangle = \tfrac{1}{2}\left[|E_{00}^b\rangle - |E_{11}^b\rangle - |E_{10}^b\rangle - |E_{01}^b\rangle\right]|0^{\bar{b}}\rangle + \\ + \tfrac{1}{2}\left[|E_{00}^b\rangle - |E_{10}^b\rangle - |E_{01}^b\rangle + |E_{11}^b\rangle\right]|1^{\bar{b}}\rangle \quad (14)$$

где члены для $|E_{01}^{\bar{b}}\rangle$ и $|E_{10}^{\bar{b}}\rangle$ заключены в скобки, так что очевидно, что

$$p_\epsilon^{\bar{b}} = \tfrac{1}{2}\left[\langle E_{01}^{\bar{b}}|E_{01}^{\bar{b}}\rangle + \langle E_{10}^{\bar{b}}|E_{10}^{\bar{b}}\rangle\right] = \tfrac{1}{4}\left[\left(\langle E_{00}^b| - \right.\right. \\ - \langle E_{11}^b|\rangle\left(|E_{00}^b\rangle - |E_{11}^b\rangle\right) + \left(\langle E_{10}^b| - \right. \\ \left.\left. - \langle E_{01}^b|\rangle\left(|E_{10}^b\rangle - |E_{01}^b\rangle\right)\right)\right].$$

Расширим этот результат, используя тождества $\langle\phi|\psi\rangle = \overline{\langle\psi|\phi\rangle}$ и $z + \bar{z} = 2Re(z)$ для $z \in C$ (здесь над чертой обозначается комплексное сопряжение [8]).

Используя равенства (3) и (4), получаем следующие выражения:

$$p_e^{\bar{b}} = \frac{1}{4}\left[2 - \langle E_{00}^b|E_{11}^b\rangle - \langle E_{11}^b|E_{00}^b\rangle - \right. \\ \left. - \langle E_{01}^b|E_{10}^b\rangle - \langle E_{10}^b|E_{01}^b\rangle\right]$$

$$p_e^{\bar{b}} = \tfrac{1}{2}\left[1 - Re\left(\langle E_{00}^b|E_{11}^b\rangle + \langle E_{01}^b|E_{10}^b\rangle\right)\right]. \quad (15)$$

Эта формула будет использоваться для связи возмущения, вызванного Евой, когда Алиса кодирует в базисе $\bar{b}_j$ биты i_j, так что $s_j = 1$, с информацией, которую Ева может получить, когда Алиса кодирует их в базисе. Следуя принципу «Информация против возмущения» [9], чем больше информации получает Ева, когда кодирование осуществляется в базисе b, тем больше помех она вызывает, когда биты кодируются и проверяются в сопряженном базисе. Следовательно, можно ограничить знания Евы о ключе, ограничив допустимую частоту ошибок в протоколе.

Результаты исследований и их анализ

Доказательство защищённости протокола BB84 от коллективных атак

Выберем код

$$\frac{d_{r,m}}{2n} > p_a + \epsilon$$

для некоторого ϵ; тогда

$$2m\sqrt{P\left[\left(\frac{|C_I|}{n} \geq \frac{d_{r,m}}{2n}\right) \wedge \left(\frac{|C_T|}{n} \leq p_a\right)\right]}$$

окажется меньше, чем значение

$$P\left[\left(\frac{|C_I|}{n} > p_a + \epsilon\right) \wedge \left(\frac{|C_T|}{n} \leq p_a\right)\right],$$

что само по себе экспоненциально мало по n. Можно применить выборку Хёффдинга из [3] (теорема 10) для каждой конкретной строки $c_1 \ldots c_{2n}$, соответствую-

щей измерению всех кубитов в некотором допустимом координатном базисе b. Пусть

$$\overline{X} = \frac{|C_I|}{n} —$$

среднее значение выборки, соответствующее ошибочным информационным битам; а

$$\mu = \frac{|C_I|+|C_T|}{2n} —$$

математическое ожидание $\overline{X}$, которое эквивалентно выражению $2\mu - \bar{X} \leq p_a$, или тождественно неравенству $\bar{X} - \mu \geq \mu - p_a$.

Для строк $\left(\frac{|C_I|}{n} > p_a + \epsilon\right)$ и $\left(\frac{|C_T|}{n} \leq p_a\right)$ перепишем условия, как

$$(\bar{X} - \mu > \epsilon + p_a - \mu) \wedge (\bar{X} - \mu \geq \mu - p_a) \quad (16)$$

откуда следует, что используя теорему Хёффдинга [10], получается соотношение:

$$P\left[\left(\frac{|C_I|}{n} > p_a + \epsilon\right) \wedge \left(\frac{|C_T|}{n} \leq p_a\right)\right] \leq$$
$$\leq P\left[\bar{X} - \mu > \frac{\epsilon}{2}\right] \leq e^{-\frac{1}{2}n\epsilon^2} \quad (17)$$

Нужно быть уверенным, в том, что частота ошибок в информационных битах будет меньше максимальной скорости, с которой эти ошибки может обработать код с исправлением ошибок. Это условие необходимо для доказательства надёжности ключа.

Доказательство защищённости протокола BB84-Info-Zот коллективных атак

Общая коллективная атака Евы

Допустим, что перед выполнением протокола квантового распределения ключей (КРК), Ева выбирает коллективную атаку [3].

Дан j–й кубит, отправленный Алисой Бобу. Ева присоединяет состояние зонда, и применяет некоторый унитарный оператор U_J к составной квантовой системе.

Затем, Ева держит у себя в квантовой памяти подсистему E_j, которая является её состоянием зонда; далее, она посылает Бобу подсистему T_j, которая является кубитом, отправленным от Алисы к Бобу (возможно, эта подсистема была изменена атакой Евы унитарным оператором U_J).

Наиболее общей коллективной атакой U_J Евы на j–й кубит, представленный на ортонорматической основе, является атака, описываемая, выражениями:

$$U_j|0^E\rangle E_j|0^{b_j}\rangle T_j = |E_{00}^{b_j}\rangle E_j|0^{b_j}\rangle T_j + |E_{01}^{b_j}\rangle E_j|1^{b_j}\rangle T_j \quad (18)$$

$$U_j|0^E\rangle E_j|0^{b_j}\rangle T_j = |E_{10}^{b_j}\rangle E_j|0^{b_j}\rangle T_j + |E_{11}^{b_j}\rangle E_j|1^{b_j}\rangle T_j, \quad (19)$$

где $|E_{00}^{b_j}\rangle E_j$, $|E_{01}^{b_j}\rangle E_j$, $|E_{10}^{b_j}\rangle E_j$, и $|E_{11}^{b_j}\rangle E_j$ —

ненормированные состояния в системе зонда Евы E_j, прикрепленные к j–му кубиту.

Таким образом, очевидно, что описанная атака может изменить исходное состояние составной системы,

$$|0^E\rangle E_j \left|i_j^{b_j}\right\rangle T_j,$$

и привести его в запутанное состояние, что означает, что атака Евы может вызвать запутывание своего зонда с зондом Боба.

С одной стороны, это даёт некоторую информацию о состоянии Боба; с другой стороны, это вызывает нарушение, которое может быть обнаружено им же. Информация, полученная накануне, и возмущение, вызванное Евой, по своей природе устанавливает их взаимосвязь. По этой причине протоколы квантового распределения ключей являются безопасными.

Доказательство безопасности протокола BB84-Info-Z от коллективных атак

Как упоминалось ранее [3], случайная величина $\tilde{C}_I$ соответствует битовой строке ошибок в битах INFO, если они были закодированы в базисе X. Биты TEST–X также кодируются в базисе X, а случайная величина C_{TX} соответствует строке битов ошибок на этих битах. Следовательно, выбор индексов n–битов INFO и n_x–битов TEST–X можно рассматривать как случайную выборку (после того, как числа n, n_z и n_x; и индексы битов TEST–Z уже выбраны) и использовать теорему Хёффдинга [4].

Таким образом, для каждой битовой строки $c_1 \ldots c_{n+nx}$, состоящей из ошибок в $n + n_x$ битах INFO и TEST–X, если биты INFO были закодированы в базисе X, можно применить теорему Хёффдинга. Для этого следует взять образец размера n без замены из совокупности $c_1, \ldots, c_{n+nx}$. Фактически, доказывается следующая теорема [3]:

Теорема. Пусть даны $\delta > 0$, $R > 0$, и для бесконечного числа значений n семейство линейно независимых векторов $\{v_1^n, \ldots, v_{r_n+m_n}^n\}$ таково, что

$$\delta < \frac{d_{r_n,m_n}}{n} \text{ и } \frac{m_n}{n} \leq R.$$

Тогда, для любых $p_{a,z}, p_{a,x} > 0$, таких, что

, и для любых $n, n_z, n_x > 0$, а также двух m_n–битовых финальных ключей $k,\ k'$, расстояние между состояниями Евы, соответствующими k и k', удовлетворяет следующей границе:

$$\langle \Delta_{Eve}^{(p_{a,z},p_{a,x})}(k,k') \rangle \leq 2Rne^{-\left(\frac{n_x}{n+n_x}\right)^2 n\epsilon_{sec}^2}. \quad (20)$$

Надежность протокола BB84-Info-Z

Сама по себе безопасность квантового протокола недостаточна; также необходимо, чтобы надёжным был ключ (а именно, чтобы он был одинаковым для Алисы и Боба) [11]. Это означает, что нужно убедиться, что количество ошибок в битах INFO меньше максимального количества ошибок, которое может быть исправлено кодом исправления ошибок. Для этого необходимо, чтобы код исправления ошибок был способен исправить ошибки. Отсюда следует, что надёжность финального ключа, с экспоненциально малой вероятностью отказа, гарантируется неравенством:

$$P\left[\left(\frac{|c_l|}{n} > p_{a,z} + \epsilon_{rel}\right) \wedge \left(\frac{|c_{T_z}|}{n_z} \leq p_{a,z}\right)\right] \leq e^{-2\left(\frac{n_z}{n+n_z}\right)^2 n\epsilon_{rel}^2} \quad (21)$$

Выбор индексов INFO–битов и битов TEST–Z –это случайное разделение $n + n_z$ битов на два подмножеств, размеров n и n_z(при условии, что индексы битов TEST–X уже были выбраны), что т соответствует выборке Хёффдинга.

Разработка квантового протоколаCSLOE-2022 как новой модификации BB84

Теперь предлагаем читателю ознакомится с новой модификацией, предложенной авторами и получившей наименование CSLOE-2022, для старого, но всё ещё результативного квантового протокола BB84, использующего квантовое распределение ключей.

В протоколе BB84 можно, в значительной мере, улучшить криптостойкость и степень запутываемости атакующего хакера–прослушивателя, что способно усложнить возможность перехвата информации в результате кибератаки, нацелившейся на конфиденциальные сообщения.

Известно [11], что после согласования базисов в классическом протоколе BB84, перехватчик может получить точную информацию о передаваемом состоянии.

Конечной целью описываемой модификации является усложнение процесса подслушивания, до состояния его бесполезности, в плане затрачивания времени и ресурсов, а также подтверждения гипотезы о реальной возможности использования этого метода.

Идея состоит в следующем: известно, что процесс репликации состояния, записываемый как ψ ψ ψ, и известный, как клонирование, может быть выполнен идеально с вероятностью 1 тогда и только тогда, когда известен базис, которому принадлежит ψ [12]. В противном случае, идеальное клонирование невозможно, так как копии получаются не идеальными. Таковы содержание и следствия теоремы о запрете клонирования квантовой информации.

Это обстоятельство может оказаться полезным. При невозможности воспроизвести точный клон фотона, для того чтобы получить информацию из него, необходимо провести измерение характеристик оригинала. Единственным способом измерить характеристики фотона является использование детектора одиночных фотонов. Но как только фотон попадает на детектор, он передаёт энергию и исчезает, то есть измерение уничтожает сам фотон [4]. Нужно учитывать, что каждый фотон уникален [13]. Однако можно создать некое подобие фотона. Известно, что благодаря квантовой телепортации можно получить точную копию фотона [12], которую, в свою очередь, также можно использовать для конструирования такого подобия. Для просты назовём его *псевдо–фотоном*. Перехватчик будет воспринимать такой псевдо–фотон либо как настоящий фотон со своим специфичным набором характеристик, либо как искажение в канале. А для обнаружения и опознавания такого клона в канале связи необходимо приложить немалые усилия.

Теоретически, на первом этапе, как и в классическом протоколе BB84, Алиса будет общаться с Бобом по квантовому каналу связи. В свою очередь, Алиса будет передавать Бобу изменённую последовательность, состоящую из клонированных псевдо–фотонов, и формирующую словарь для каждого бита с соответствующей поляризацией. Как упоминалось ранее, псевдо–фотон представляет собой некое подобие фотона, созданного искусственно [4]. В каждом конкретном случае возможно формирование новых последовательностей, формирующих динамический словарь, тем самым снижая повтор при шифровании, учитывая уникальность каждого фотона [13]. Для каждого бита может быть использован не один псевдо–фотон, а целая группа, с определённым диапазоном значений, который будет корректироваться, смещаться или расширяться [14]. Каждый бит, или их последовательность, даже если они повторяются, будут иметь случайные псевдо–фотоны из определённого диапазона значений, которые приписаны биту или битовой последовательности.

При отправке словаря для декодирования можно пересылать его частями, во избежание полного рассекречивания словаря. При обнаружении прослушива-

Таблица 1. Просеянный ключ

Бит Алисы	0	1	1	0		1	0	0	1
Базис Алисы	x	+	+	x		+	x	+	x
Поляризация Алисы	↗	↑	→	↖		→	↖	↑	↗
Базис Боба	x	x	x	+		+	x	+	+
Измерение Боба	↗	↖	↗	→		→	↖	↑	→
Обсуждение	x	+	+	*		+	x	+	*
Просеянный ключ	0					1	0	0	

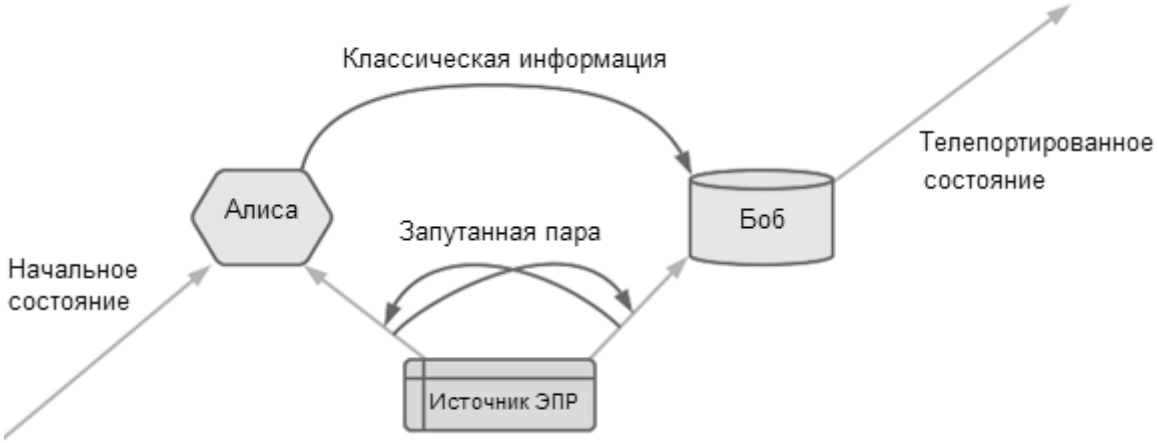

Рис. 3. Результаты работы протокола CSLOE-2022, где источник ЭПР представляет собой источник фотонов, предложенный Эйнштейном–Подольским–Розеном

ния, на данном этапе словарь можно расширить, а перехваченную часть не использовать [15], или временно прекратить передачу данных и сформировать новый словарь. После успешной передачи словаря, можно начать отправку закодированных сообщений по каналу связи, в котором настоящие фотоны, как и созданные их копии, будут чередоваться, и иметь абсолютно случайные позиции в последовательности. Стоит отметить, что данный протокол можно дополнительно усложнить.

Например, можно использовать четыре квантовых состояния для кодирования битов в двух базисах, что соответствует протоколу BB84(4+2) [16]. Далее, такой протокол работает по классическому сценарию, но с использованием словаря.

Каждый раз, когда Боб получает кубит, он сообщает об этом Алисе, но не измеряет его. Впоследствии, для каждого фотона и псевдо–фотона, который получает Боб, он будет измерять поляризацию на случайно выбранной основе, применяя её к своему состоянию. Если для конкретного фотона Боб выбрал ту же базу состояния, то, когда он выполняет H^{b}, что и Алиса, то он переходит в то же состояние. Боб должен измерить ту же поляризацию в i^{B} строкеи, таким образом, он может правильно вывести бит, который Алиса намеревалась послать, в случае если, в канале связи нет шума и признаков подслушивания.

На втором этапе Боб должен уведомить Алису, по любому незащищенному каналу связи, какой базис он использовал для измерения каждого фотона. Алиса сообщает Бобу, какие фотоны были настоящими, путём отправки зашифрованных диапазонов, а также ставит его в известность, правильно ли он выбрал базис для каждого оригинального фотона. На этом этапе Алиса и Боб отбрасывают биты, соответствующие псевдо–фотонам, и биты, которые Боб измерял с другим базисом. При условии, что ошибок не произошло, и никто не манипулировал фотонами, Боб и Алиса должны получить одинаковую строку битов, являющуюся *просеянным ключом*. В приведенном примере (рис. 3, табл. 1) показаны биты, выбранные Алисой; базисы, в которых она их закодировала; а также базисы, которые Боб использовал для измерения. Показан полученный просеянный ключ, после того как Боб и Алиса отбросили свои биты, упомянутые выше.

Принцип неидеальной репликации часто применяется в практике телекоммуникаций. Информация, пере-

даваемая в оптоволокне, кодируется в состоянии света, поэтому этот процесс является *квантовым кодированием* [17]. Эта информация усиливается в несколько раз от источника до приёмника, поэтому её качество со временем неминуемо ухудшается.

Однако телекоммуникационный сигнал состоит из большого количества фотонов, приготовленных в одном и том же квантовом состоянии. Усиление в телекоммуникациях сводится к созданию некоторых новых копий ψ из ψ⊗N. Иначе говоря, теорема о запрете клонирования применима к усилению телекоммуникационных сигналов, потому что в усилителях всегда присутствует спонтанное излучение. Копия почти идеальна, потому что стимулированное излучение является доминирующим эффектом. Чувствительность современных устройств достаточно высока, и на данном этапе такова, что квантовый предел может быть достигнут в обозримом будущем.

Таким образом, кодирование информации, подчиняющееся теореме о запрете клонирования, может быть полезно и для протоколов квантового распределения ключей [18]. Невозможность точного копирования квантовой информации не отменяет всей концепции квантовой информации. Напротив, он служит иллюстрацией его силы. Невозможно полностью скопировать состояние квантовой системы для умного кодирования информации, которое использует набор не ортогональных состояний. Следовательно, если такая система доходит до приёмника невозмущенной, то это доказывает, что она не была скопирована ни одним перехватчиком. Это означает, что, из-за теоремы о запрете клонирования, квантовая информация предоставляет средства для выполнения некоторых задач, которые были бы невозможны при использовании только обычной информации. Например, обнаружение любого подслушивающего устройства на канале связи возможно только с применением идей квантовой криптографии.

Методы клонирования

Рассмотрим возможные методы неидеального клонирования дискретных квантовых систем, чем и является протокол BB84.Существует несколько вариантов таких машин:

1. Оптимальная симметричная универсальная квантовая копировальная машина (УККМ), предложенная Владимиром Бужеком–Марком Хиллери (БХ) в 1996 г.;
2. Симметричная УККМ, предложенная Никола Гизеном– Сержем Массаром в 1997 году;
3. Ассиметричная универсальная квантовая копировальная машина — УККМ.

Симметричная УККМ для 1 2 клонирования кубитов, разработанная Бужеком и Хиллери, принимает клонируемый кубит на вход, и использует отдельный кубит в качестве вспомогательного кубита [19]. Действие такой машины в вычислительной базе исходного кубита описывается выражением:

$$|0\rangle|R\rangle|M\rangle \to \sqrt{\frac{2}{3}}|0\rangle|0\rangle|1\rangle -$$

$$-\sqrt{\frac{1}{3}}|\psi^+\rangle|0\rangle(-|1\rangle)|E\rangle|M\rangle \to$$

$$\to \sqrt{\frac{2}{3}}|1\rangle|1\rangle|0\rangle - \sqrt{\frac{1}{6}}|\psi^+\rangle|1\rangle \quad (22)$$

с $\left|\psi^+\right\rangle = \frac{1}{\sqrt{2}}[|1\rangle|0\rangle + |0\rangle|1\rangle]$. По линейности, эти два соотношения индуцируют следующее действие на наиболее общее входное состояние $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:

$$|\psi\rangle|R\rangle|M\rangle \to$$

$$\to \sqrt{\frac{2}{3}}|\psi\rangle|\psi\rangle|\psi^\perp\rangle - \sqrt{\frac{1}{6}}[|\psi\rangle|\psi^\perp\rangle + |\psi^\perp\rangle|\psi\rangle]|\psi\rangle \quad (23)$$

где $|\psi^\perp\rangle = \alpha * |1\rangle - \beta * |0\rangle$.

Как видно из уравнения (23), α и β можно поменять местами. Кроме того, преобразование имеет одинаковую форму для всех входных состояний $|\psi\rangle$.

Таким образом, такая квантовая копировальная машина (ККМ)является симметричной и универсальной. Её частичные состояния для оригинала и копии:

$$\rho_\alpha = \rho_\beta = \frac{5}{6}|\psi\rangle\langle\psi| + \frac{1}{6}|\psi^\perp\rangle\langle\psi^\perp| = \frac{1}{2}\left(1 + \frac{2}{3}\hat{m} + \vec{\sigma}\right). \quad (24)$$

Симметричная УККМ для $N \to M$ кубитов была открыта Гизеном и Массаром в 1997 году. Она обобщает УККМ Бужека–Хиллери, и её правильность определяется выражением:

$$F_{N\to M} = \frac{MN+M+N}{M(N+2)}\ (d = 2), \quad (25)$$

которое воспроизводит $F_{1\to 2} = \frac{5}{6}$ для $N = 1$ и $M = 2$. Гизен и Массар дали численные доказательства оптимальности своей универсальной квантовой копировальной машины. Позже аналитическое доказательство оптимальности было дано Дагмаром Брюссом, Артуром Эккертом и Киаром Маккиавелли в 1998 году, которые предположили, что выходное состояние принадлежит симметричному подпространству из M кубитов. Результат далее был обобщен Рейнхардом Вернером для систем любой размерности [20].

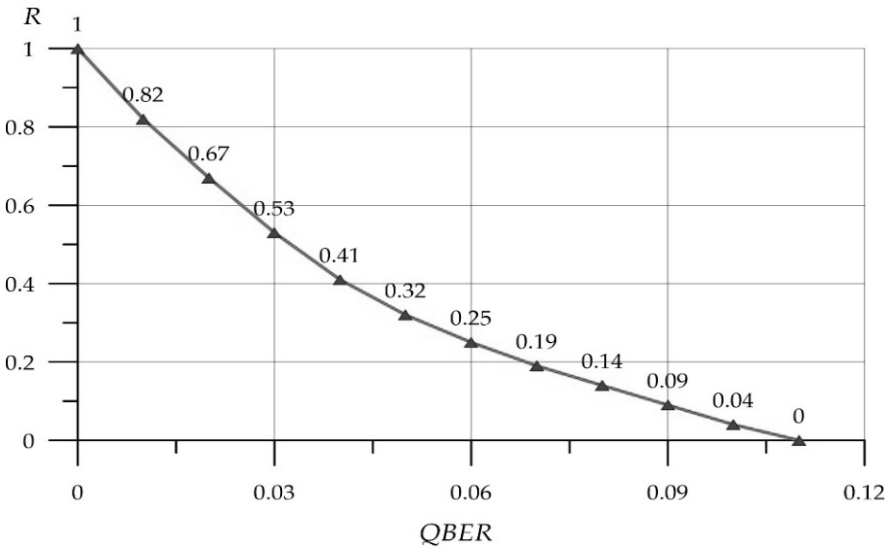

Рис. 4. Порог ошибок для BB84

Асимметричное универсальное клонирование относится к ситуации, когда выходные клоны могут иметь разную точность воспроизведения.

Здесь следует сосредоточиться на универсальном клонировании $1 \to 1+1$. Изучение более общих случаев было предпринято несколькими исследователями в 2004–2005 г.г.

Рассмотрим некоторые из этих идей ниже вместе с их экспериментальной реализацией. В своем всестороннем исследовании клонирования $1 \to 1+1$, Чи–Шенг Ниу и Роберт Гриффитс в 1998 г. получили, в частности, оптимальную асимметричную УККМ $1 \to 1+1$.

Тот же результат независимо получил Николас Серф в 1998–2000 г.г., который использовал алгебраический подход, а также Владимир Бужек и Марк Хиллери в 1998 г. [21], которые разработали подход квантовых схем, улучшенный по сравнению с предыдущей конструкцией для симметричного клонирования. Оптимальность демонстрируется путём доказательства того, что верность двух клонов, F_α и F_β, насыщает неравенство не клонирования:

$$\sqrt{(1-F_\alpha)(1-F_\beta)} \geq \frac{1}{2} - (1-F_\alpha) - (1-F_\beta). \quad (26)$$

Тем же авторам удалось расширить разработку своих схем далеко за пределы отдельного случая кубита, и распространить на любое их количество. Исходя из вышесказанного, для улучшения крипто стойкости протокола BB84 лучше всего подходит УККМ Бужека–Хиллери, как наиболее простая в реализации квантовая копировальная машина из рассмотренных выше.

Сравнение протоколов

Поскольку квантовые протоколы BB84, BB84–INFO–Z и предложенная авторами модификация CSLOE-2022имеют много общего, то можно выделить ряд параметров для их сравнения. Начнём со сравнения порога ошибок. Данный параметр необходим, чтобы определить, был ли осуществлён перехват информации, или попытка подслушивания. В практической реализации протокола квантового распределения ключа всегда будут проявляться недостатки отдельных компонентов, и некоторые кубиты будут непригодны для формирования секретного ключа. Помимо этого, попытки прослушивания квантового канала вносят изменения в передаваемые кубиты, что также не позволяет использовать их при формировании секретного ключа.

В случае с классическим протоколом BB84, пороговое значение частоты ошибок составляет 11% [22]. Для идеальной модели, количество битов окончательного секретного ключа (R) на один бит просеянного ключа выражается формулой

$$R = 1 - 2\,H(QBER), \quad (27)$$

где H — двоичная Шенноновская энтропия, а $QBER$– количество ошибок, измеренных Бобом. Зависимость R от QBER представлена на рис. 4: Она не обязательно должна быть такой. Качество исполнения аппаратуры, реализующей протокол, позволит снизить порог в меньшую сторону.

В протоколе BB84–INFO–z, помимо информационных кубитов, отвечающих за генерацию ключа, исполь-

Таблица 2. Сравнительные характеристики протоколов по порогу ошибок

Протокол	Порог ошибок
BB84	11%
BB84–INFO–Z	7,56%
CSLOE-2022	~11%

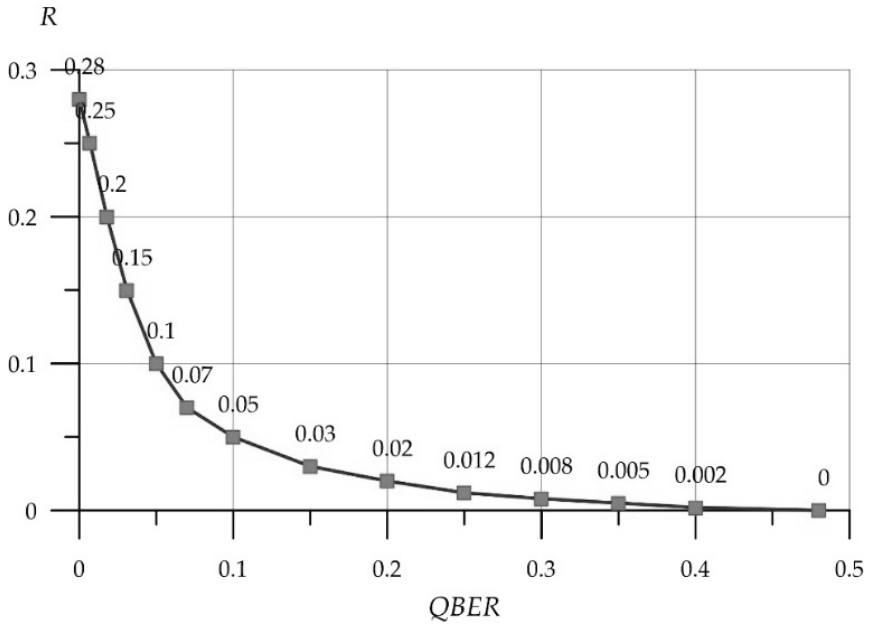

Рис. 5. Безопасная зона асимптотических скоростей ошибок для BB84–INFO–Z

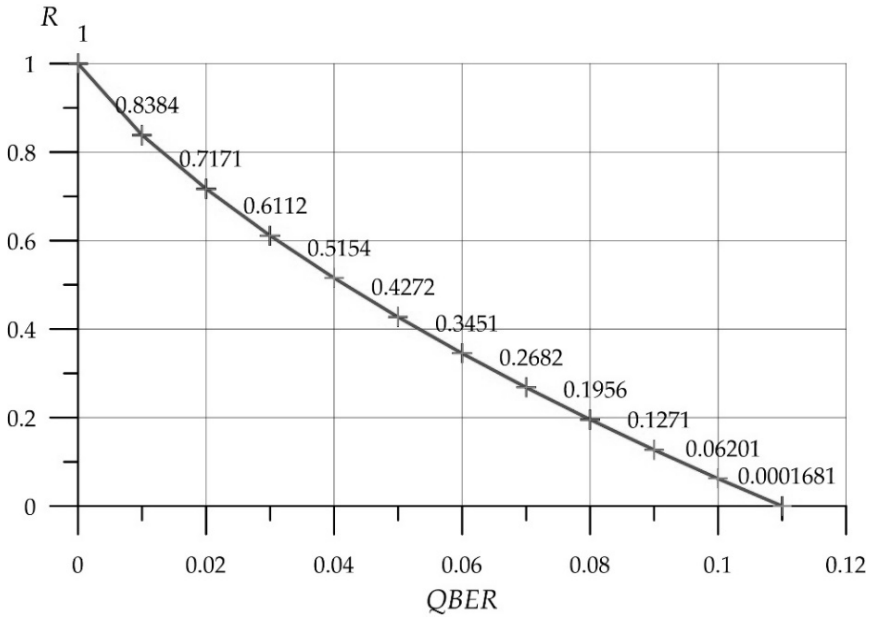

Рис. 6. Порог ошибок для протокола CSLOE-2022

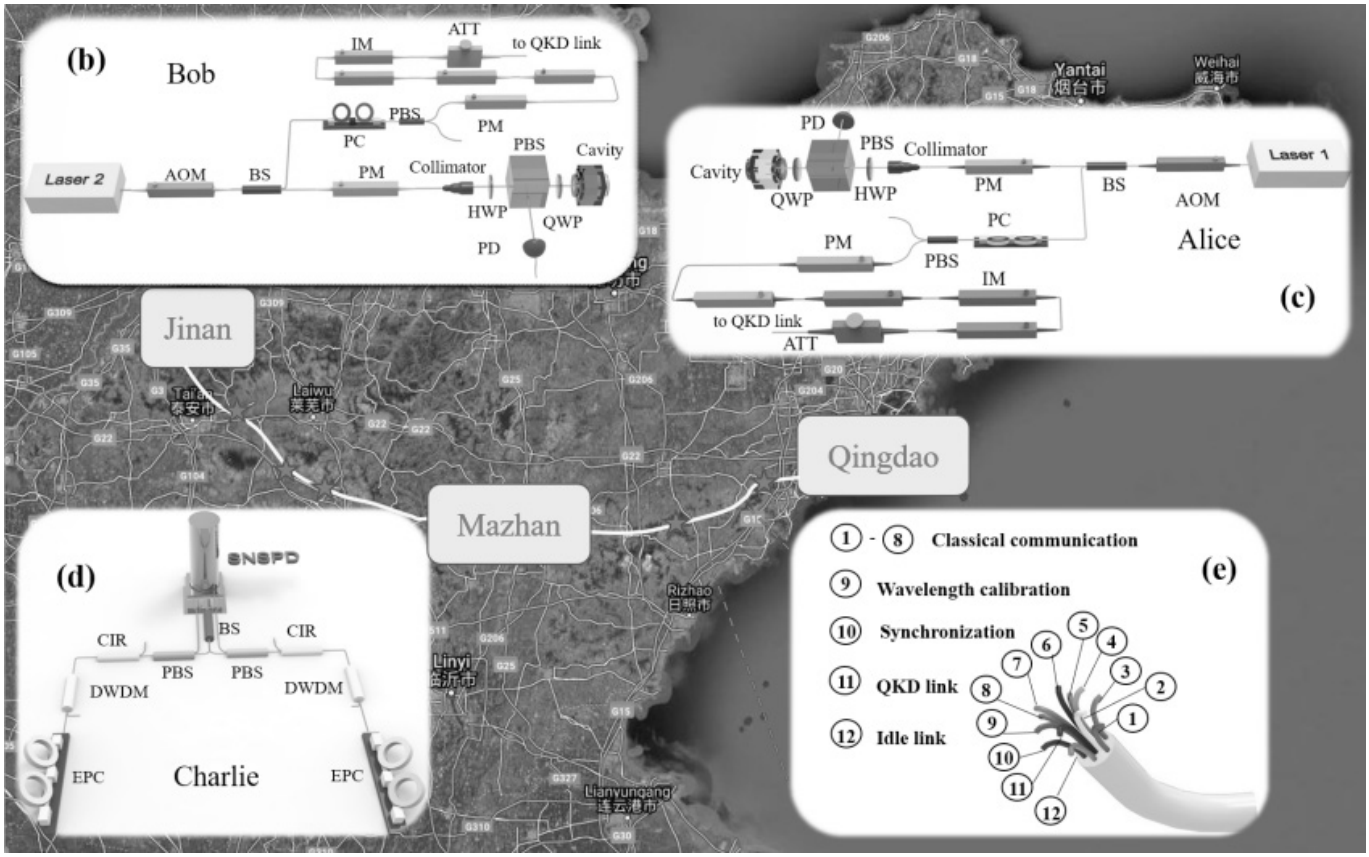

Рис. 7. Провинции Китая, соединенные оптоволоконной сетью протяженностью 430 км.

зуются тестовые кубиты Xи Z [2], необходимые для проверки на попытки перехвата — прослушивания. Порог ошибок для этой модификации иной, и отличается в меньшую сторону. Он составляет не более 7,56% [4], как показано на рис. 5.

Для предлагаемой авторами модификации (CSLOE-2022), порог ошибок, теоретически, аналогичен оригинальному, поскольку в ходе формирования ключа неидеальные копии фотонов, используемые для запутывания прослушивающего перехватчика, отбрасываются и далее проверяются оригиналы, как в классическом протоколе. С другой стороны, при попытке прослушивания искажение именно фотонов маловероятно, поскольку их значительно меньше, чем их копий, псевдо–фотонов. Из работы [12] известно, что код Стина (CSS) позволяет на практике закодировать

$$[1 - 2 * H(\delta)]n \tag{28}$$

кубитов, где δ — количество измеренных ошибок, а n — длина последовательности кубитов. Если записать формулу (28) как: $f(x) = 1 - 2 * H(x)$, то график пересечёт ось X в точке 0,11, что и даёт порог ошибок в 11% в классическом квантовом протоколе BB84 [23].

Для протокола CSLOE-2022 зависимость количества битов окончательного секретного ключа R от количества зафиксированных ошибок QBER сохраняется, как показано на рис. 6, поскольку искажению при передаче подвергнутся все фотоны: и оригинальные, и их копии в виде псевдо–фотонов.Сравнение протоколов по порогу ошибок можно наблюдать в табл. 2:

Квантовый протокол BB84–INFO–Z отличается в лучшую сторону от остальных исследуемых протоколов, поскольку более низкий порог ошибок позволяет перехватчику Еве получить значительно меньше информации о просеянном секретном ключе.

Ещё одним немаловажным параметром является рабочее расстояние. Протоколы квантового распределения ключа оперируют одиночными фотонами, которые при передаче могут исказиться. Поэтому рабочее расстояние относительно невелико.

Например, для BB84 это расстояние составляет около 70 км [24]. При реализации протоколов DPS и COW удалось достичь 250 и 307 км соответственно, однако их безопасность ещё не доказана. В свою очередь, команде китайских физиков: Цзю-Пэн Чен, Чи Чжани др.

Таблица 3. Рабочее расстояние протоколов.

Протокол	Рабочее расстояние
BB84	70 км
BB84–INFO–Z	70 км
CSLOE-2022	511 км

удалось передать секретный квантовый ключ на расстояние 511 километров в реальных условиях[19]. Они смогли реализовать квантовую линию передачи данных не в лабораторных условиях, а в реальных между двумя городами. Схема квантовой линии представлена на рис. 7.

Физики продолжают искать разные способы увеличить расстояние до сотен и тысяч километров, занимаясь разработкой повторителей для существующих протоколов, а также разрабатывают новые, например, протокол полей–близнецов TF (TwinField). В отличие от стандартного протокола BB84, в котором Алиса напрямую отправляет Бобу фотоны, протокол TF [25] включает в себя дополнительный узел Чарли, который находится между Алисой и Бобом.

Предварительное моделирование квантовой линии связи показало, что производительность метода может превзойти ограничение по ёмкости секретного ключа, и при этом сохранить как безопасность, так и эффективность. Сам эксперимент SNS–TF–QKD с полевым оптоволокном показывает, что между китайскими провинциями Циндао, который выступает в качестве Алисы, и Цзинань, выступающим в качестве Боба, были расположены экспериментальные установки.

На соответствующих станциях, килогерцовый волоконный лазер с непрерывной волной накачки был подключен к резонатору со сверхнизким коэффициентом расширения. В свою очередь, источником света является акустический оптический модулятор. Лазер был синхронизирован по частоте, и применялся для выполнения кодирования с помощью двух фазовых модуляторов и трёх модуляторов интенсивности.

Закодированные импульсы при помощи аттенюатора ослабляются до однофотонного состояния, а затем отправляются на измерительную станцию с контролером поляризации.

На промежуточной станции (Мажан, выступающей в роли Чарли) производится настройка для двух контролеров поляризации, а также ведётся обратная связь в режиме реального времени, с данными о поляризации импульсов между станциями Циндао (Алиса) и Цзинань (Боб). Для фильтрации утечек в канале и нелинейных рассеиваний импульсов используются мультиплексоры. В рамках эксперимента использовался оптоволоконный кабель, состоящий из 12 волокон, для передачи сигнала однофотонного состояния линии связи, для синхронизации и фиксации оптической частоты между лазерами станций Алиса и Боб соответственно. Разделяя излучение на две части, где одна часть предназначена для передачи квантового сигнала, а другая — для захвата длины волны, в рамках эксперимента фиксируются 2 лазера на расстоянии более 400км в оптоволоконном канале на 84,1 дБ с 6 оптическими усилителями EDFA между ними. Условный дрейф частоты между двух источников составляет примерно 0,1 Гц/с, что даёт суммарную разность фаз около π/60 в час. Следовательно, вместо калибровки длины волны, более значительным является калибровка разницы длин волн в час, что является вполне приемлемой характеристикой для показательного эксперимента. Соответственно, при более подходящих настройках достигается результат вплоть до расстояния в 511 километров.

В этом случае Алиса и Боб осуществляют передачу по слабому когерентному импульсу Чарли, который сравнивает их и объявляет, совпали ли полученные биты или нет. Но у Чарли отсутствует информация о пришедших к нему битах, и он может только сравнивать их и объявлять, совпали они в данный момент или нет, поэтому Чарли оказывается не доверенным узлом.

Такой подход позволяет превысить известный предел скорости генерации ключей без повторителей. Он использует два источника, стабилизировать фазы которых, как и сотен километров волокна между ними, оказывается непростой задачей.

Можно подытожить сравнение квантовых протоколов по рабочему расстоянию (табл. 3:

Вывод

Авторы показали, что квантовый протокол BB84–INFO–Z полностью защищен от коллективных атак. Обнаружено, что результаты работы протокола BB84–INFO–Z имеют много общего с протоколом BB84, за двумя существенными исключениями:

1. Частота ошибок должна проверяться отдельно, чтобы она была ниже пороговых значений $p_{a,z}$

и $p_{a,x}$ для битов TEST–Z и TEST–X, соответственно, в то время как в протоколе BB84 пороговое значение частоты ошибок p_a применяется ко всем битам TEST совместно [2].

2. Показатели информации Евы (безопасность) и вероятности отказа исправляющего ошибки кода (надёжность) отличаются от показателей в случае с классическим BB84 [3].

Можно сделать вывод, что даже если изменить квантовый протокол BB84, чтобы биты INFO были только в основе Z, то это не ослабит его безопасность и надёжность (по крайней мере, против коллективных атак) и не поменяет порога асимптотической частоты ошибок [3].

Протокол BB84–INFO–Z можно безопасно использовать для распространения просеянного секретного ключа; его безопасность имеет идеальную реализацию против возможных коллективных атак перехватчиков, прослушивающих каналы связи.

Показано, что предлагаемая авторами модификация классического квантового протокола BB84 (CSLOE-2022) вполне могла бы применяться для квантового распределения ключей, поскольку применяемый принцип неидеального копирования не нарушает законов физики, но позволяет значительно повысить крипто стойкость протокола.

Пока что эта модификация является гипотезой, и её необходимо доказать серией практических экспериментов с использованием специфического оборудования. Известно, что принцип неидеального копирования уже давно экспериментально применяется в каналах связи, что описано в публикациях [26–40], что позволяет передавать информацию на значительно большие расстояния. Однако для квантового распределения ключей существуют иные требования по качеству исполнения отдельных компонентов. Поэтому, специалистами в области квантовой физики выдвигаются новые идеи и гипотезы, а перед инженерами ставятся специфические и конкретные задачи проверки и доказательства справедливости подобных гипотез.

Далее авторы ставят перед собой задачу исследования квантовой оптической памяти на основе фотонов и псевдо–фотонов, на предмет возможности записи в них информации. Основываясь на полученных данных, необходимо выявить теоретические ограничения, а также найти способы их нивелирования и нейтрализации, соответственно, как для фотонов, так и для воссозданных копий на их основе — псевдо–фотонов.

ЛИТЕРАТУРА

1. Bennett, C.H.; Brassard, G. Quantum Cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing 1984.
2. Park J. The Concept of Transition in the Quantum Mechanics. (1970).
3. Boyer M.; Liss R.; Mor T. Compo sable Security against Collective Attacks of Modified BB84 QKD Protocol with Information Only in One Basis. Theoretical Computer Science. 2019.
4. Biham, E.; Mor, T. Security of quantum cryptography against collective attacks. Physical Review Letters 1997.
5. Boyer M.; Gelles R.; Mor T. Security of the Bennett–Brassard Quantum Key Distribution Protocol against Collective Attacks. 2009.
6. Vercruysse D.; Sapra N., Yang K., etc. Inverse–Designed Photonic Crystal Devices for Optical Beam Steering. E.L. Ginzton Laboratory, Stanford University. 2021.
7. Buckley S., Radulaski M., Zhang J., etc. Nonlinear Frequency Conversion Using High Quality Modes in GaAs Nanobeam Cavities. Ginzton Lab., Spilker Engineering and Applied Sciences Building, Stanford University, 2014.
8. Cerf N., Ipe A., Rottenberg X. Cloning of Continuous Quantum Variables. Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 2000.
9. Fuchs C.; Peres, A. Quantum–State Disturbance versus Information Gain: Uncertainty Relations for Quantum Information. Physical Review. 1996. 53. 2038–2045.
10. Skoric B.; Wolfs Z. Diagrammatic Security Proof for 8–State Encoding. arXiv:2103.01936v1. 2021.
11. Morimae T. Quantum Randomized Encoding, Verifification of Quantum Computing, No-Cloning, and Blind Quantum Computing. Yukawa Institute for Theoretical Physics, Kyoto University/ 2020.
12. Schimpf C., Reindl M., Huber D., etc. Quantum Cryptography with Highly Entangled Photons from Semiconductor Quantum Dots. arXiv:2007.12726v1. 2020.
13. Tan X. Introduction to Quantum Cryptography, (2013). DOI:10.5772/56092.
14. Shor P. and Preskill J., Simple Proof of Security of the BB84 Quantum Key Distribution Protocol (2000). AT&T Labs Research, Florham Park, New Jersey 07932.
15. Huttner B.; Imoto N., GisinN., etc. Quantum Cryptography with Coherent States (1995). https://doi.org/10.1103/PhysRevA.51.1863.
16. Djordjevic I. Quantum Information Processing, Quantum Computing, and Quantum Error Correction.2021.
17. Quantum Teleportation — Overview | ScienceDirect Topics.
18. Quantum Teleportation of Particles in an Environment.
19. Chen J.; Zhang C.; Liu Y. et al. Twin–Field Quantum Key Distribution over 511 km Optical Fiber Linking two Distant Metropolitans, 2021.

20. This is Condensed Version of Report from Live Science. https://www.nbcnews.com/science/weird-science/scientists-are-beaming-over-quantum-teleportation-record-n264726
21. Жизан Н. Квантовая случайность. Не локальность, телепортация и другие квантовые чудеса. М: Альпина нон–фикшн, 2018, 208 с.
22. Родина О.В. Волоконно–оптические линии связи. М: «Горячая линия–Телеком». 2018.
23. Atom–to–Photon State Mapping by Quantum Teleportation.
24. Козубов А.В., Гайдаш А.А., Кынев С.М. и др. Основы квантовой коммуникации: Ч. 1. 2019.
25. Lucamarini M., Yuan Z., Dynes J., et al. Overcoming the Rate–Distance Limit of Quantum Key Distribution without Quantum Repeaters, 2018.
26. Probabilistic and Controlled Teleportation of Unknown Quantum States. Phys. Lett. A (2003).
27. Quantum Hyper Entanglement and its Applications in Quantum Information Processing. Sci. Bull. (2017).
28. Quantum Teleportation of Three and Four-Qubit State Using Multi-Qubit Cluster States. International Journal of Theoretical Physics (2016)
29. Blunt N.S., Camps J., Crawford O., et al. Perspective on the Current State-of-the-art of Quantum Computing for Drug. Discovery Applications, 2022.
30. Chamberland C., Noh K., Arrangoiz-Arriola P., et al., Building the Fault-Tolerant Quantum Computer Using Concatenated Cat Codes, PRX Quantum 3, 2022.
31. Chamber land C. and Campbell E.T., Universal Quantum Computing with Twist–Free and Temporally Encoded Lattice Surgery, PRX Quantum 3, 2022.
32. Kivlichan I.D., GidneyC., Berry D.W., et al. Improved Fault–Tolerant Quantum Simulation of Condensed-Phase Correlated Electrons via Trotterization, Quantum 4, 2020.
33. Bacon D., Software of QIP, by QIP, and for QIP, QIP Plenary Talk 2022.
34. Hermans, S.L. et al. Qubit Teleportation between Non-Neighbouring Nodes in the Quantum Network. Nature 605, 663–668 2022.
35. Sun, Q.— C. et al. Quantum Teleportation with Independent Sources and Prior Entanglement Distribution over a Network. Nature Photonics 10, 671–675 2016.
36. Wang Y, Hu M–L. Quantum Teleportation and Dense Coding in Multiple Bosonic Reservoirs. Entropy. 2022.
37. Wu, H.; Liu, X.; Zhang, H.; etc. Performance Analysis of Continuous Variable Quantum Teleportation with Noiseless Linear Amplifier in Seawater Channel. Symmetry.2022.
38. Cardoso–Isidoro, C., and Delgado F. Shared Quantum Key Distribution Based on Asymmetric Double Quantum Teleportation.Symmetry14, 2022.
39. Lu, D., Zhihui L., Jing Yu, and Zhaowei H. Verifiable Arbitrated Quantum Signature Scheme Based on Controlled Quantum Teleportation" Entropy24, 2022.
40. Короченцев Д.А. и др. Квантовые вычислительные системы информационной безопасности: основы алгоритмического, программного и аппаратного обеспечения.— 2021.