КВАНТОВАЯ КРИПТОГРАФИЯ

О квантовой криптографии на когерентных состояниях с использованием псевдослучайных генераторов

А.С.Аванесов, Д.А.Кронберг

Квантовое распределение ключей играет важную роль в современной криптографии, поскольку секретность передаваемых ключей гарантируется фундаментальными законами природы. Рассмотрен способ использования в квантовой криптографии псевдослучайных генераторов, хорошо известных из классической криптографии. Показано, что их использование позволяет увеличить скорость генерации ключа при очень слабых предположениях о возможностях перехватчика. Предложена практическая схема протокола квантового распределения ключей на когерентных состояниях, использующая псевдослучайные последовательности. Рассмотрена криптографическая стойкость предложенного протокола против атаки светоделителем.

Ключевые слова: *квантовая криптография, квантовая информация, когерентные состояния, псевдослучайные генераторы.*

1. Введение

Квантовая криптография, появившаяся более 30 лет назад [1], стремительно развивается в последние годы. Существует ряд коммерческих схем квантового распределения ключей, работает передача ключей между городами [2] и между Землей и спутниками [3].

Ключевым преимуществом квантового распределения ключей перед классическим является то, что стойкость ключей гарантируется фундаментальными законами природы и не сводится к предположениям об ограниченных возможностях перехватчика. Классическая же криптография основывается главным образом на предположении о том, что некоторые вычислительные задачи не могут быть решены быстро. Однако это предположение до сих пор не доказано, что влечет за собой потенциальную уязвимость классических криптографических схем как из-за развития вычислительных способностей перехватчика, так и из-за разработки новых алгоритмов. Так, в 1998 г. было создано вычислительное устройство EFF DES cracker, подбирающее ключ к схеме шифрования DES за несколько суток, что обусловлено стремительным развитием мощности вычислительной техники за два десятилетия после принятия стандарта DES в 1977 г.

А.С.Аванесов. Математический институт им. В.А.Стеклова РАН, Россия, 119991 Москва, ул. Губкина, 8; Московский физико-технический институт (национальный исследовательский университет), Россия, Московская обл., 141701 Долгопрудный, Институтский пер., 9; e-mail: avanesov@phystech.edu

Д.А.Кронберг. Математический институт им. В.А.Стеклова РАН, Россия, 119991 Москва, ул. Губкина, 8; Российский квантовый центр, Россия, 1213353 Москва, Сколковское ш., 45; Московский физико-технический институт (национальный исследовательский университет), Россия, Московская обл., 141701 Долгопрудный, Институтский пер., 9; e-mail: dmitry.kronberg@gmail.com

Поступила в редакцию 30 апреля 2019 г., после доработки – 28 июня 2019 г.

Кроме того, как было показано еще в 1994 г. Шором [4], создание квантового компьютера может сделать ряд важных классических схем полностью несекретными, в том числе теряет секретность вся информация, зашифрованная к этому времени. Это приводит к утверждению, что информация, для которой важна секретность в течение долгого времени, должна уже сейчас шифроваться с помощью схем, стойких к появлению у перехватчика квантового компьютера в будущем [5]. Схемы классической криптографии, устойчивые к появлению квантового компьютера, называют постквантовой криптографией [6].

В этом контексте важное преимущество квантовой криптографии заключается в том, что она позволяет сохранять секретность передаваемых ключей бесконечно долго, и у перехватчика нет возможности получить дополнительную информацию о ключе при решении вычислительных задач или при появлении у него новых технологических средств. При этом следует отметить, что реализация протоколов квантовой криптографии, как правило, имеет свои недостатки, что ведет к возможности атак, использующих несовершенство оборудования или целенаправленное повреждение перехватчиком отдельных элементов схем легитимных пользователей [7, 8]. Однако все атаки подобного рода относятся к атакам реального времени и не дают возможности получить секретный ключ после окончания сеанса его генерации.

Важная цель научных и экспериментальных групп, работающих над квантовым распределением ключей, – передача ключей с большой скоростью и на большие расстояния. При этом практические схемы шифрования, даже основанные на квантовой криптографии для генерации ключа, могут в ряде случаев для увеличения скорости использовать элементы классической криптографии, такие как схемы AES, что делает систему уже не абсолютно стойкой, поскольку длина ключа оказывается меньше длины шифруемого сообщения. Такой подход может оказаться целесообразным для приложений, где использование абсолютно стойкого одноразового шифр-блокнота

практически не оправдано из-за быстрого расходования ключа. Для подобных приложений актуальной является задача увеличения скорости генерации ключа в протоколах квантовой криптографии при использовании ряда технологий классической криптографии, пусть и ценой отказа от полной теоретической стойкости.

Важным понятием классической криптографии, которое может быть использовано и в квантовых технологиях, является псевдослучайный генератор [9], т. е. функция, которая по данному начальному ключу длиной K (иногда называемому зерном псевдослучайной последовательности) строит строку большей длины $q(K)$ (псевдослучайную последовательность). Эту строку сложно (с вычислительной точки зрения) отличить от случайной строки, т. е. по выходной строке сложно вычислить начальный ключ и предугадать следующие символы псевдослучайной последовательности [10]. Такой генератор можно получить из классических систем шифрования, таких как AES, если запустить их в режиме гаммирования (OFB) [11].

Примером применения псевдослучайных генераторов в квантовой криптографии является протокол Y-00 [12–14], который использует когерентные состояния, хорошо различимые при знании псевдослучайной последовательности, но плохо различимые без него. Этот протокол далее будет рассмотрен подробно. Псевдослучайные последовательности было предложено также применять при выборе базисов в однофотонных протоколах квантовой криптографии [15], что позволяет увеличить скорость генерации ключа при сохранении безусловной стойкости. При этом было показано, что квантовый поточный шифр на основе псевдослучайной последовательности уже не способен обеспечить теоретическую стойкость [16]. Помимо этого, заслуживает упоминания «квантовая Энигма» [17] – метод, который позволяет передать секретное сообщение произвольной длины при наличии ключа ограниченной длины между легитимными пользователями. Правда, этот метод требует от легитимных пользователей возможности совершать преобразования над квантовыми состояниями в пространствах больших размерностей, что затрудняет его практическое применение.

В настоящей работе предлагается схема, которая использует псевдослучайные генераторы как составную часть и поэтому требует предположений относительно вычислительных способностей перехватчика. Будем использовать предположение о том, что перехватчик не может вычислить зерно псевдослучайной последовательности в течение сеанса связи, который, как правило, не превышает по длительности нескольких минут. В то же время при выполнении этого слабого предположения распределяемые ключи остаются секретными в течение неограниченного времени, что сохраняет важное преимущество квантовой криптографии перед классической.

Работа организована следующим образом. Раздел 2 посвящен протоколам квантовой криптографии на симметричных когерентных состояниях. В нем вводится общая схема таких протоколов, обобщающая два предложенных к настоящему времени протокола, и предлагается оптическая схема измерения. В разделе 3 описывается основной протокол с псевдослучайным выбором базисов. В разделе 4 рассматривается атака светоделителем и приводятся рассуждения, почему эта атака близка к оптимальной для предлагаемого протокола. Раздел 5 посвящен возможным модификациям протокола в различных практических условиях. В Заключении приводятся основные выводы работы.

2. Использование симметричных когерентных состояний в квантовой криптографии

Ослабленное лазерное излучение является одним из наиболее доступных на практике источников квантовых состояний, поэтому протоколам квантовой криптографии на когерентных состояниях уделяется большое внимание. Когерентное состояние, задаваемое комплексным числом α, записывается как

$$|\alpha\rangle = \mathrm{e}^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \tag{1}$$

где $|n\rangle$ – n-фотонное состояние. Параметр α связан с интенсивностью светового пучка:

$$\mu = |\alpha|^2. \tag{2}$$

Схема с четырьмя геометрически однородными когерентными состояниями [18] является одним из первых предложенных протоколов квантовой криптографии на когерентных состояниях. Эта конфигурация состояний близка к протоколу BB84, т. к. при знании базиса повышается вероятность различить состояния. Однако поскольку когерентные состояния неортогональны, состояния в одном базисе также не являются ортогональными, и протокол имеет сходство и с протоколом B92 на двух неортогональных состояниях [19], из-за чего его также называют протоколом 4 + 2.

В данном протоколе задействованы состояния $|\alpha\rangle$, $|\mathrm{i}\alpha\rangle$, $|-\alpha\rangle$ и $|-\mathrm{i}\alpha\rangle$, образующие два базиса $\{|\alpha\rangle, |-\alpha\rangle\}$ и $\{|\mathrm{i}\alpha\rangle, |-\mathrm{i}\alpha\rangle\}$. При описании квантовых протоколов распределения ключей действующих агентов, между которыми и осуществляется распределение ключей, принято называть Алисой и Бобом. Канал связи между ними может прослушиваться злоумышленником, которого называют Евой. Обозначим используемый базис с помощью параметра $b \in \{0, 1\}$, а отправляемый бит сообщения как k. Тогда Алиса в каждой посылке отправляет состояние $|(-1)^k \mathrm{i}^b \alpha\rangle$. Для измерения Боб использует интерферометр Маха – Цендера. Изменяя фазу на нижнем плече интерферометра, Боб проводит измерение в случайно выбранном им базисе. С вероятностью 1/2 он верно угадывает базис, тогда с вероятностью $1 - \mathrm{e}^{-\mu}$ происходит срабатывание одного из детекторов. Затем, как в протоколе BB84, Алиса и Боб общаются по открытому каналу и отбрасывают посылки, где их базисы не совпали, после чего проводят коррекцию ошибок и усиление секретности для получения совпадающего ключа, информация перехватчика о котором мала.

При использовании этого протокола и при отсутствии затухания в линии связи Ева не знает выбранного базиса в момент пересылки состояний и вносит ошибку при попытке получить информацию из сигнала (в простейшем случае – при попытке угадать базис и провести измерение, но это не лучшая стратегия). Однако из-за неортогональности состояний внутри базиса и затухания в канале связи Боб ожидает срабатывания детекторов не во всех позициях, что дает Еве новые возможности для подслушивания. В частности, она может блокировать часть

посылок, для которых не смогла получить всю информацию. Это приводит к атаке измерением с определенным исходом (иначе называемой USD-атакой) [20]. При такой атаке перехватчик проводит безошибочное измерение (unambiguous state discrimination), которое дает либо полную информацию о передаваемом состоянии, либо неопределенный результат. В последнем случае перехватчик блокирует посылку, иначе отправляет состояние без ошибок, при необходимости с увеличенной интенсивностью. При достаточно больших потерях в линии связи эта стратегия атаки позволяет перехватчику получать полную информацию о ключе, не будучи обнаруженным.

Состояния протокола 4+2 обладают симметрией, а именно могут быть получены действием преобразования $U\colon |\alpha_{i+1}\rangle = U|\alpha_i\rangle$, $U^N = I$. Важным результатом для симметричных когерентных состояний (иногда их также называют геометрически однородными) является оценка вероятности их безошибочного различения [21, 22], которая дает ограничение на применение атаки измерением с определенным исходом, – при фиксированной интенсивности чем больше состояний используют легитимные пользователи, тем сложнее их безошибочно различить. Протокол 4+2 использует лишь два базиса, что делает применение USD-атаки достаточно простым. Тогда естественным предложением является использование большего числа базисов, т. к. Еве будет сложнее их различить. Однако это помешает также и легитимным пользователям, поскольку скорость генерации ключа будет уменьшаться с ростом числа базисов из-за частого их несовпадения у Алисы и Боба.

Следует также упомянуть протокол на геометрически однородных когерентных состояниях [23], в котором передаваемое сообщение кодируется в $2M$ когерентных состояний, образующих M базисов, с фазовым сдвигом между базисными состояниями $\delta = \pi/M$. Отметим также протокол [24, 25], использующий аналогичный набор симметричных когерентных состояний с фазовым сдвигом π внутри базиса, однако применяющий иную (по сравнению с протоколами 4+2 и упомянутым выше протоколом на геометрически однородных состояниях) схему измерения на стороне Боба, использующую боковые частоты.

Наше предложение заключается в том, что использование большого числа базисов M позволяет выбирать их псевдослучайным образом, т. е. в соответствии с псевдослучайной последовательностью, задаваемой общим начальным ключом, имеющимся в распоряжении Алисы и Боба. Можно также использовать произвольный фазовый сдвиг между состояниями внутри базиса, вместо $\delta = \pi$ в протоколе 4+2 и $\delta = \pi/M$ в протоколе с геометрически однородными состояниями. Таким образом, можно построить целое семейство схем квантового распределения ключей, частными случаями которого будут два указанных выше протокола.

Рассмотрим случай произвольных значений δ и M и опишем действия легитимных пользователей. Отдельно рассматриваются два случая, т. к. для них используются разные схемы измерения.

1. Пусть $\delta = \pi$, тогда выбираем базисы вида $\{|e^{i\pi b/M}\alpha\rangle, |-e^{i\pi b/M}\alpha\rangle\}$, $b = 0,..., M-1$.

2. Если $\delta \neq \pi$, то потребуем дополнительно, чтобы $\delta \neq 2\pi k/M$, где $k \in Z$. Соответствующие базисы будем выбирать в виде $\{|e^{i2\pi b/M}\alpha\rangle, |e^{i\delta}e^{i2\pi b/M}\alpha\rangle\}$, $b = 0,..., M-1$.

На рис.1 представлены изображения передаваемых в протоколе состояний в фазовой плоскости в случае использования восьми базисов; рассмотрены два варианта: $\delta = 3\pi/8$ и $\delta = \pi$.

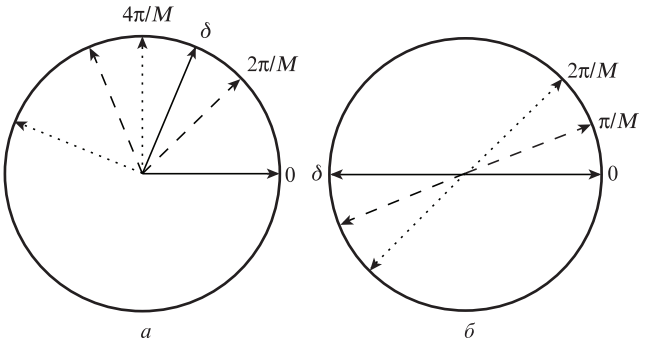

Рис.1. Примеры передаваемых Алисой состояний для $M = 8$. Изображены состояния первых трех базисов ($b \in \{0, 1, 2\}$) для $\delta = 3\pi/8$ (*а*) и $\delta = \pi$ (*б*). Одинаковые типы линий обозначают состояния одного базиса.

Пошаговое описание протокола выглядит следующим образом.

1. Алиса и Боб выбирают целое число M, соответствующее числу базисов, и фазовый сдвиг δ.

2. Далее N раз повторяются следующие действия:

а) Алиса случайным образом выбирает базис $b \in \{0, 1,..., M-1\}$ и значение бита $k \in \{0, 1\}$;

б) Алиса отправляет состояние $|\alpha_k^{(b)}\rangle = |\alpha e^{i\theta_b} e^{ik\delta}\rangle$, где

$$\theta_b = \frac{\pi b}{M}(1 + [\delta \neq \pi]) \qquad (3)$$

(здесь $[\delta \neq \pi]$ – индикатор того, что $\delta \neq \pi$);

в) Боб случайным образом выбирает базис $b' \in \{0, 1,..., M-1\}$ и проводит измерение с определенным исходом, различающее состояния $|\alpha_0^{(b)}\rangle$ и $|\alpha_0^{(b')}\rangle$. В результате измерения Боб получает либо неопределенный исход, либо число k', соответствующее состоянию $|\alpha_{k'}^{(b')}\rangle$.

3. Алиса и Боб по открытому каналу раскрывают базисы b и b'. Посылки с несовпадающими b и b' отбрасываются. Кроме того, отбрасываются все посылки, где измерение на стороне Боба дало неопределенный исход.

4. Алиса и Боб раскрывают часть своих последовательностей k и k' для оценки вероятности ошибки. Если ошибка оказывается больше критической, выполнение протокола прерывается. В противном случае через открытый канал проводится коррекция ошибок.

5. Алисой и Бобом проводится процедура усиления секретности, в результате которой они получают битовую строку меньшей длины, информация Евы о которой мала.

Схема измерения на стороне Боба приведена на рис.2. Алиса в каждой посылке отправляет опорный сигнал $|\alpha\rangle$ и следом, с фиксированной задержкой относительно опорного сигала, информационное состояние $|\alpha_k^{(b)}\rangle$. На приемной стороне используется интерферометр Маха–Цендера. Для наблюдения интерференции части опорного сигнала, проходящей по нижнему пути, и части информационного состояния, идущей по верхнему пути, осуществляется задержка на нижнем пути, равная задержке при отправке состояний. Кроме того, на нижнем пути с помощью фазового модулятора Боб «подкручивает» фазу опорного состояния в соответствии с b' и k' для получения информации о переданном бите Алисы.

Светоделитель СД1 на входе интерферометра делит состояние $|\alpha\rangle$ на две части: $|\alpha/\sqrt{2}\rangle$ на верхнем пути и

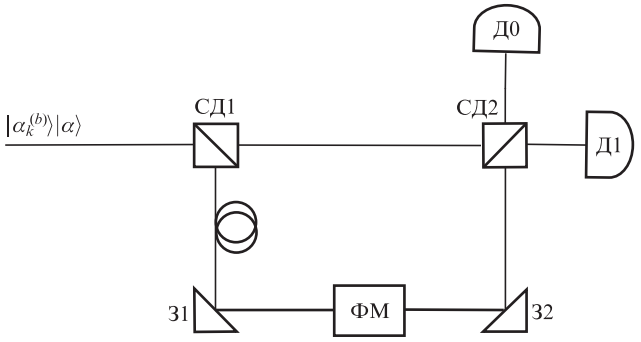

Рис.2. Схема измерения на стороне Боба:
СД1 и СД2 – светоделители; 31 и 32 – зеркала; Д0 и Д1 – детекторы. Часть опорного сигнала $|\alpha\rangle$ проходит по нижнему пути через линию задержки и на фазовом модуляторе ФМ изменяет свою фазу в соответствии с выбранными Бобом параметрами $b' \in \{0,...,M-1\}$ и $l \in \{0,1\}$. Получившееся состояние $|-i\alpha_l^{(b')}/\sqrt{2}\rangle$ после прохождения через СД2 интерферирует с прошедшей по верхнему пути частью сигнального состояния $|i\alpha_k^{(b)}/\sqrt{2}\rangle$. Возможны варианты: если $\delta = \pi$, то l всегда устанавливается равным нулю, а b' выбирается случайным образом, срабатывания детекторов Д0 и Д1 соответствуют $k' = 0$ и $k' = 1$; при $\delta \neq \pi$ параметры b' и l выбираются случайно, показания детектора Д0 игнорируются, а в случае срабатывания детектора Д1 параметру k' присваивается значение $k' = l \oplus 1$.

$|i\alpha/\sqrt{2}\rangle$ на нижнем пути. Два зеркала 31 и 32 на нижнем пути изменяют фазу в сумме на 2π, а фазовый модулятор ФМ преобразует входящий в него сигнал $|\alpha\rangle$ в $|e^{i\theta}\alpha\rangle$, выбор θ осуществляется Бобом.

В случае $\delta = \pi$ преобразование опорного сигнала между началом и концом нижнего пути принимает вид

$$\left|\frac{i\alpha}{\sqrt{2}}\right\rangle \to \left|\frac{ie^{i\theta_{b'}}\alpha}{\sqrt{2}}\right\rangle. \quad (4)$$

Далее оба пучка проходят через светоделитель СД2. Рассмотрим временной момент, когда к детекторам придет часть информационного состояния, прошедшая по верхнему пути. Положим, базис угадан верно, т.е. $b' = b$. Тогда после светоделителя СД2 на вход детектора Д0 приходит состояние $|^1\!/_2 e^{i\pi b/M}(e^{i\pi k}+1)\alpha\rangle$, а на вход детектора Д1 – состояние $|^1\!/_2 e^{i\pi b/M}(e^{i\pi k}-1)\alpha\rangle$. В случае посылки состояния $|\alpha_0^{(b)}\rangle$ имеется ненулевая вероятность срабатывания детектора Д0, который указывает, что отправлялся классический бит 0, а значит, $k' = 0$. Срабатывание второго детектора не должно происходить, и это событие рассматривается как ошибка. Если же Алиса отправила состояние $|\alpha_1^{(b)}\rangle$ и базис угадан верно, то с некоторой ненулевой вероятностью срабатывает детектор Д1, тогда $k' = 1$. Срабатывание обоих детекторов трактуется как ошибка. В итоге вероятность того, что Боб угадал базис и сработал один из его детекторов, принимает вид

$$p = \frac{1 - e^{-\mu}}{M}. \quad (5)$$

Теперь рассмотрим вариант $\delta \neq \pi$. В этом случае Боб не только пытается угадать базис, но и подстраивает схему под каждое информационное состояние, т.е. выбирает случайный бит l и с помощью фазового модулятора осуществляет преобразование

$$\left|\frac{i\alpha}{\sqrt{2}}\right\rangle \to \left|\frac{ie^{i\theta_{b'}}e^{i\delta l}\alpha}{\sqrt{2}}\right\rangle = \left|\frac{i\alpha_l^{(b')}}{\sqrt{2}}\right\rangle. \quad (6)$$

Снова допустим, что базис был угадан верно, т.е. $b' = b$, и рассмотрим момент прихода части информационного состояния по верхнему пути. После светоделителя СД2 на вход детектора Д1 приходит состояние $|^1\!/_2 e^{i\pi b/M}(e^{i\delta k} - e^{i\delta l})\alpha\rangle$. Срабатывание детектора Д1 возможно, только если $l \oplus 1 = k$, поэтому Боб полагает $k' = l \oplus 1$. В прочих случаях Боб получает неопределенный исход. Будем игнорировать возможные срабатывания детектора Д0, в этом случае от него можно отказаться вовсе. Для вероятности определенного исхода имеем выражение

$$p = \frac{1 - \exp[-|(\alpha - e^{i\delta}\alpha)/2|^2]}{2M} = \frac{1 - \exp(-\mu \sin^2(\delta/2))}{2M}. \quad (7)$$

Скорость генерации ключа есть величина, пропорциональная вероятности p успешного получения информации о посланном состоянии.

3. Выбор базиса с использованием генератора псевдослучайных чисел

Можно заметить, что при фиксированном δ вероятность определенного исхода оказывается обратно пропорциональной числу используемых в протоколе базисов. Это, в свою очередь, приводит к ограничениям для скорости генерации ключа.

Базис b в описанном выше протоколе выбирался случайным образом. Имеет смысл рассмотреть возможность использования генератора псевдослучайной последовательности для выбора значений параметра b. Иными словами, Алиса и Боб исходно имеют некоторый общий секрет – это начальный ключ псевдослучайной последовательности. Используя эту информацию, они детерминированно могут получить идентичные последовательности базисов b. В таком случае приводимые ниже схемы уже не будут безусловно стойкими протоколами квантового распределения ключей, однако при выполнении определенных предположений можно говорить об их стойкости. Важным протоколом, использующим псевдослучайную последовательность для выбора базисов, является протокол Y-00 [12, 13]. В этом протоколе используется рассмотренная выше конфигурация состояний при большом числе базисов ($M \gg 1$) с фазовым сдвигом между базисными состояниями $\delta = \pi$. Протокол также использует высокую интенсивность передаваемых когерентных состояний ($\mu \gg 1$), что делает возможным применение гомодинного детектирования, которое при высокой интенсивности и знании базиса Бобом дает малую ошибку.

Протокол Y-00 имеет высокую скорость генерации ключа при относительно простой реализации [14], однако обеспечивает лишь практическую стойкость, когда перехватчик ограничен текущим технологическим уровнем и не может, к примеру, долго хранить состояния в квантовой памяти и совершать коллективные измерения над квантовыми состояниями в пространстве большой размерности.

Мы предлагаем генерировать номера базисов b псевдослучайным образом, как в протоколе Y-00, но при этом полагаем, что Боб использует однофотонный детектор. Это позволяет использовать при передаче когерентные состояния малой интенсивности. Отметим, что при малых μ базисные состояния становятся хуже различимыми,

это существенно затрудняет подслушивание даже при отсутствии предположений о технологических возможностях перехватчика: даже после расчета начального ключа псевдослучайной последовательности Ева не может получить достаточно информации о ключе вследствие неразличимости измеряемых состояний. Однако если Ева посчитает начальный ключ псевдослучайной последовательности до окончания пересылки квантовых состояний, то описываемый нами протокол оказывается уязвимым перед USD-атакой, т. к. Ева может провести в каждой позиции безошибочное измерение в известном ей базисе, после чего, согласно сценарию USD-атаки, заблокировать состояние при неопределенном исходе или усилить его интенсивность при получении всей информации. В итоге протокол оказывается секретным в предположении, что время вычисления начального ключа псевдослучайной последовательности больше времени сеанса связи между Алисой и Бобом, и это слабое вычислительное предположение является единственным предположением о возможностях перехватчика в предлагаемой схеме.

Ниже будет показано, что протокол не теряет секретность при вычислении начального ключа псевдослучайной последовательности после сеанса связи, т. к. Ева уже не имеет возможности блокировать посылки, из которых ей не удалось извлечь информацию. Поскольку помимо начального ключа нет информации, которая способна помочь Еве получить секретный ключ, секретность ключа не меняется со временем, что является важным преимуществом квантового распределения ключей. Между сеансами связи Алиса и Боб изменяют начальный ключ псевдослучайного генератора, беря часть распределенного между ними секретного ключа, поэтому вычисление начального ключа предыдущих сеансов оказывается не актуальным при перехвате ключа, распределяемого во время следующих сеансов связи.

Наконец, можно рассматривать целое семейство протоколов, каждый представитель которого определяется выбранными значениями параметров μ, δ, M. Поскольку выбор базисов производится в соответствии с псевдослучайной последовательностью, в предлагаемых нами протоколах вероятность определенного исхода у Боба не будет зависеть от числа используемых базисов и согласно (6) и (7) оказывается равной $1 - e^{-\mu}$ и $(1 - e^{-\mu\sin^2(\delta/2)})/2$ для $\delta = \pi$ и $\delta \neq \pi$ соответственно.

Таким образом, увеличение параметра M не сказывается на скорости генерации ключа. Использование же большого числа базисов делает протокол более устойчивым к USD-атаке.

4. Атака с использованием светоделителя

Рассмотрим для протокола (μ, M, δ) одну из базовых атак на протоколы на когерентных состояниях в условиях линии связи с затуханием – атаку светоделителем. При такой атаке для каждого посланного Алисой состояния $|\alpha_k^{(b)}|$ Ева использует светоделитель, с помощью которого разделяет пучок на два (рис.3). Одна часть ($|t\alpha_k^{(b)}|$) отправляется Бобу, а над другой ($|r\alpha_k^{(b)}|$, где $|t|^2 + |r|^2 = 1$) осуществляется оптимальное коллективное измерение для получения максимальной информации о значении бита k. Отметим, что Ева имеет возможность хранить состояния в квантовой памяти и проводить измерения над отложенной частью состояния после того, как она вычислит псевдослучайную последовательность. Это означает, что в момент измерения базис будет известен перехватчику и ему потребуется различить состояния $|r\alpha_0^{(b)}|$ и $|r\alpha_1^{(b)}|$.

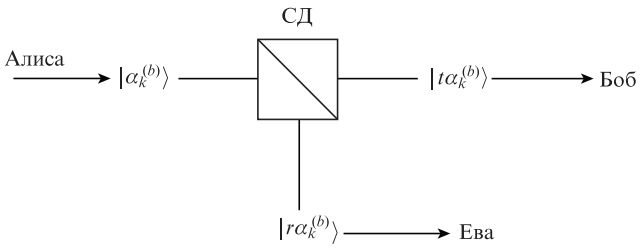

Рис.3. Атака с использованием светоделителя:
СД – светоделитель; $|t|^2$ и $|r|^2$ – коэффициенты пропускания и отражения соответственно.

Наибольшая информация, которая может быть извлечена, ограничена величиной Холево [26], имеющей для двух равновероятных чистых состояний следующий вид:

$$\chi(|r\alpha_0^{(b)}\rangle, |r\alpha_1^{(b)}\rangle) = H\left(\frac{|r\alpha_0^{(b)}\rangle\langle r\alpha_0^{(b)}| + |r\alpha_1^{(b)}\rangle\langle r\alpha_1^{(b)}|}{2}\right)$$
$$= h_2\left(\frac{1 - |\langle r\alpha | e^{i\delta} r\alpha\rangle|}{2}\right), \quad (8)$$

где $H(\hat{\rho}) = \mathrm{Tr}(\hat{\rho}\log\hat{\rho})$ – энтропия фон Неймана, а $h_2(x) = -x\log x - (1-x)\log(1-x)$ – бинарная энтропия.

Ожидаемая интенсивность сигнала на приемной стороне в канале связи с затуханием равна $\mu 10^{-\kappa L/10}$, где L – длина канала, а $\kappa > 0$ – параметр затухания. В дальнейшем будем полагать $\kappa = 0.2$ дБ/км, что соответствует параметрам оптоволокна. По предположению, Ева может заменить канал между Алисой и Бобом на идеальный канал без затухания, и тогда, чтобы на приемную сторону приходили сигналы ожидаемой интенсивности, параметры светоделителя Евы должны определяться соотношениями

$$|r|^2 = 1 - 10^{-\frac{\kappa L}{10}}, \; |t|^2 = 10^{-\frac{\kappa L}{10}}. \quad (9)$$

Обозначим исходное скалярное произведение состояний Алисы внутри базиса как ε, тогда

$$\varepsilon = |\langle \alpha | e^{i\delta} \alpha\rangle| = |e^{\mu(e^{i\delta} - 1)}| = e^{-2\mu\sin^2(\delta/2)}, \quad (10)$$

и через эту величину выразим вероятность определенного исхода на стороне Боба (эта вероятность не зависит от того, была проведена атака или нет, а зависит от длины линии связи L, т. к. светоделителем Ева моделирует затухание в канале):

$$p(\varepsilon, L) = \frac{1 - \varepsilon^{|t|^2/2}}{2^s} = \frac{1 - \varepsilon^{1/2\,10^{-\kappa L/10}}}{2^s}, \quad (11)$$

где в соответствии с описанными в предыдущем разделе схемами измерений $s = 0$, если $\delta = \pi$, в противном случае $s = 1$.

Для информации, которую Ева может извлечь из своих состояний, получаем

$$\chi(\varepsilon, L) = \chi(|r\alpha_0^{(b)}\rangle, |r\alpha_1^{(b)}\rangle)$$
$$= h_2\left(\frac{1 - \varepsilon^{|r|^2}}{2}\right) = h_2\left(\frac{1 - \varepsilon^{1 - 10^{-\kappa L/10}}}{2}\right). \quad (12)$$

Таким образом, как наибольшая информация, извлекаемая Евой при измерении, так и вероятность получения определенного исхода на стороне Боба зависит только от исходного скалярного произведения состояний внутри базиса $\varepsilon = |\langle\alpha|e^{i\delta}\alpha\rangle|$ и длины линии связи L.

Для скорости генерации секретного ключа [27] с учетом вероятности определенного исхода у Боба имеем

$$R(\varepsilon, L) = p(\varepsilon, L)[1 - h_2(q) - \chi(\varepsilon, L)], \quad (13)$$

где q – средняя наблюдаемая вероятность ошибки в канале между Алисой и Бобом (quantum bit error rate, QBER). Критическая ошибка Q, при которой скорость генерации ключа обращается в нуль, определяется выражением

$$h_2(Q) = 1 - \chi(\varepsilon, L). \quad (14)$$

Решив уравнение

$$\frac{\partial R(\varepsilon, L)}{\partial \varepsilon} = 0, \quad (15)$$

можно найти зависимость оптимального скалярного произведения $\varepsilon_{opt}(L)$ состояний Алисы внутри базиса, дающего наибольшую скорость генерации ключа, от длины линии связи L. В случае нулевого уровня ошибок ($q = 0$) эта зависимость представлена на рис.4.

Заданное значение величины ε можно получить путем варьирования параметров μ и δ. Иными словами, для оптимальной работы протокола необходимо выбрать такие значения фазового сдвига и интенсивности передаваемых сигналов, чтобы выполнялось соотношение

$$\mu \sin^2 \frac{\delta}{2} = -\frac{1}{2}\ln(\varepsilon_{opt}). \quad (16)$$

Предположим, что один из параметров δ или μ должен оставаться неизменным вне зависимости от текущей длины линии связи L. Допустим, мы используем световые сигналы только определенной интенсивности. Тогда оптимальное значение ε может достигаться путем изменения величины фазового сдвига между базисными состояниями δ. Это также означает, что на стороне Боба используется схема измерения с одним детектором. Если же технически возможно изменение интенсивности сигнала, то выгоднее использовать схему с двумя детекторами, положив $\delta = \pi$. В этом случае значение интенсивности используемых сигналов должно совпадать с оптимальным значением параметра ε для данной длины линии связи, т. е.

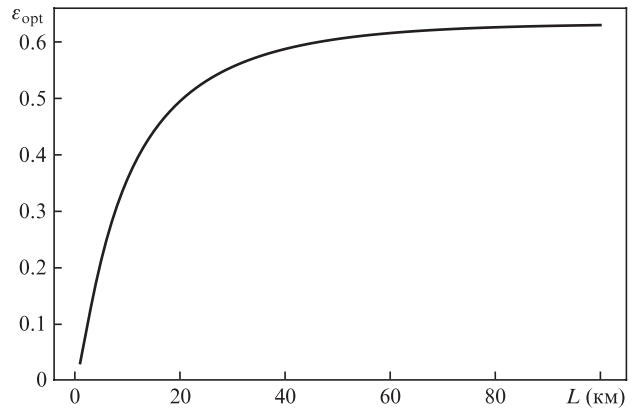

Рис.4. Зависимость оптимального скалярного произведения базисных векторов ε_{opt} от длины линии связи L при $q = 0$.

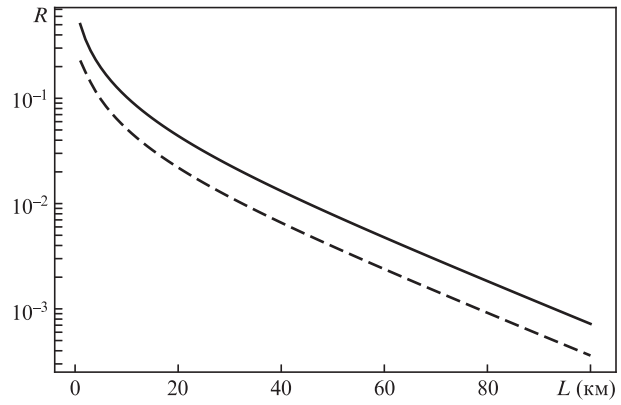

Рис.5. Зависимость скорости генерации ключа R от длины линии связи L при $q = 0$ и оптимальном выборе ε. Рассматривались два случая: интенсивность μ зависит от длины линии связи, $\delta = \pi$ (сплошная кривая); фазовый сдвиг δ зависит от длины линии связи, а $\mu = 1.0$ (штриховая кривая).

$$\mu(L) = -\frac{1}{2}\ln(\varepsilon_{opt}(L)). \quad (17)$$

Полученная зависимость скорости генерации ключа от L для обоих случаев представлена на рис.5.

При большом числе используемых базисов M и больших потерях в канале (что соответствует передаче ключей на большое расстояние) атака светоделителем близка к оптимальной атаке. Действительно, поскольку, по нашему предположению, Ева не знает базиса на момент передачи сигнала (т. к. не может вычислить зерно псевдослучайной последовательности), она не может применить USD-измерение, дающее полную информацию о передаваемых состояниях, а попытка выполнить такое измерение без знания базиса приведет к желаемому результату только с очень малой вероятностью, что и показано в работе [21]. Далее, в связи с тем, что затухание в канале связи велико, Ева после светоделителя отправляет Бобу состояния очень малой интенсивности, из которых нельзя извлечь много информации (т. к. величина Холево для этих состояний очень мала), поэтому попытка применить к ним когерентную атаку, вносящую ошибку, не приведет к сколь-нибудь заметному увеличению информации перехватчика.

5. Возможные модификации протокола

Выше была рассмотрена атака светоделителем, которая требует от перехватчика возможности хранить состояния в квантовой памяти в течение всего времени вычисления начального ключа псевдослучайной последовательности, и единственным ограничением, накладываемым на перехватчика, была невозможность вычислить начальный ключ псевдослучайной последовательности за время сеанса связи. Можно рассмотреть другое практическое ограничение перехватчика: подверженность его квантовой памяти декогеренции. В этом случае его информация о состояниях будет меньше, чем $\chi(\varepsilon, L)$ в (12), что означает увеличение скорости генерации ключа при еще одном предположении о возможностях перехватчика – не-

идеальности его квантовой памяти. В этом случае оптимальное значение скалярного произведения состояний внутри базиса на стороне Алисы может стать меньше значения, посчитанного в предположении идеальной квантовой памяти Евы, что также означает увеличение длины секретного ключа за счет большего числа определенных исходов у Боба из-за большей различимости состояний. Таким образом, используя предположение о техническом ограничении на квантовую память Евы, можно увеличить скорость генерации ключа в предложенной схеме.

Приведем еще одну модификацию построенного семейства протоколов. Итак, схема с параметрами (μ, δ, M) оказывалась секретной в предположении, что перехватчик не в состоянии вычислить псевдослучайную последовательность за время передачи сигналов и проведения измерений на приемной стороне τ_{session}. Если обозначить время вычисления начального ключа псевдослучайной последовательности как τ_{calc}, то получим, что секретность обеспечивается в случае справедливости неравенства

$$\tau_{\text{calc}} > \tau_{\text{session}}. \tag{18}$$

Если же последнее условие не выполняется, протокол оказывается уязвимым перед USD-атакой. Чтобы избежать потери стойкости, необходимо увеличить время τ_{calc}. Очевидная возможность сделать это – вернуться к истинно случайной генерации базисов. В этом случае Ева в принципе не может детерминированным образом узнать, в каком базисе осуществляется передача сигналов. Так мы возвращаемся к исходным квантовым протоколам распределения ключа, в которых скорость генерации обратно пропорциональна числу используемых базисов.

Чтобы избежать большого падения скорости генерации ключа, рассмотрим промежуточный вариант между истинно случайной и псевдослучайной генерациями базисов. Число бит, необходимых для кодировки базиса в одной посылке, равно $[\log(M)]$. Будем выбирать некоторое число бит $m < [\log(M)]$ случайным образом, а остальные – с использованием генератора псевдослучайной последовательности. В этом случае Еве необходимо будет при вычислениях осуществлять дополнительный перебор 2^m вариантов, что, в свою очередь, увеличивает τ_{calc}. Таким образом, величину m мы подбираем так, чтобы выполнялось условие (18). Тогда для вероятности определенного исхода имеем

$$p = \frac{1 - \mathrm{e}^{-\mu}}{2^m},\ \delta = \pi, \tag{19}$$

$$p = \frac{1 - \mathrm{e}^{-\mu \sin^2(\delta/2)}}{2^{m+1}},\ \delta \neq \pi. \tag{20}$$

С учетом нового параметра m расширим введенное нами семейство протоколов. Теперь каждый представитель будет иметь свой набор значений интенсивности используемых сигналов, числа базисов, фазового сдвига между состояниями одного базиса и числа случайных бит в кодировке базисного номера b. С учетом введенных обозначений будем использовать для соответствующего протокола запись (μ, M, δ, m). Измерения на стороне Боба также будут описываться схемой, изображенной на рис.2.

6. Заключение

Предложено семейство протоколов, которые комбинируют использование случайного и псевдослучайного выбора базисов и которые можно рассматривать как обобщение предложенных ранее протоколов 4+2 и протокола на геометрически однородных состояниях, а также протокола Y-00. Показана стойкость этого семейства относительно двух базовых атак – USD-атаки и атаки со светоделителем – при слабом вычислительном предположении о возможностях перехватчика. Однако на данный момент преждевременно говорить о стойкости построенного семейства протоколов против произвольной атаки, т.к. даже для полностью случайного выбора базисов стойкость протокола против атак общего вида не доказана. Так, существуют более эффективные атаки на протоколы квантовой криптографии на когерентных состояниях, обобщающие атаку светоделителем [28–30], хотя для построенного семейства протоколов выгода от их применения невелика из-за большого числа базисов. В целом же доказательство стойкости построенного семейства протоколов против произвольной атаки остается открытой проблемой.

Важно отметить, что это семейство протоколов позволяет сохранить главное преимущество квантовой криптографии, а именно секретность ключа в течение неограниченного времени, что отличает эту схему от схем классической криптографии и протокола Y-00.

Предложенное семейство протоколов позволяет регулировать скорость генерации ключа при различных предположениях о возможностях перехватчика. Так, при предположении об ограничении на квантовую память это может быть схема с хорошо различимыми состояниями внутри базиса, которая обеспечивает более высокую скорость генерации ключа за счет уменьшения вероятности неопределенного исхода на приемной стороне. В ситуациях, когда к секретности ключа применяются более жесткие требования, схема позволяет использовать мало различимые состояния внутри базиса и увеличить долю истинной случайности в выборе базиса, что означает приближение к схемам истинно квантового распределения ключей. Такое регулирование может осуществляться одним лишь изменением программной части (без изменения аппаратной реализации), при этом возможно быстрое переключение между режимами генерации ключа.

Предложены две схемы для практической реализации: с двумя детекторами на приемной стороне и с одним детектором, что уменьшает скорость генерации ключа, но удешевляет схему. Переключение между разными режимами скорости и секретности во второй схеме не требует изменения интенсивности, что можно отнести к ее преимуществам.

Настоящую работу можно рассматривать как добавление классической технологии псевдослучайных генераторов к двум существующим протоколам квантового распределения ключей. Однако по схожему принципу этот подход может быть применен и к другим протоколам квантовой криптографии для увеличения скорости генерации ключа и сохранения стойкости против USD-атаки. Это одна из тем следующих исследований.

Авторы выражают благодарность А.С.Трушечкину, Д.В.Сычу, И.В.Чижову и Кентаро Като за многочисленные обсуждения.

Работа поддержана грантом Российского научного фонда (проект № 18-71-00074).

1. Bennett Ch.H., Brassard G. *Proc. Int. Conf. Comput., Syst. Signal Process. (Bangalore, India)* (New York: IEEE, 1984, pp 175–179).
2. Boaron A., Boso G., Rusca D., et al. *Phys. Rev. Lett*., **121**, 190502 (2018).
3. Liao S.-K., Yong H.-L., Liu C., et al. *Nature Photon.*, **11**, 509 (2017).
4. Shor P.W. *Proc. 35th Ann. Symp. Found. Comput. Sci.* (Los Alamos, 1994, pp 124–134).
5. Mosca M. *IEEE Secur. Priv.*, **16**, 38 (2018).
6. Bernstein D.J. *Post-Quantum Cryptography* (Berlin, Heidelberg: Springer, 2009, pp 1–14).
7. Lydersen L., Wiechers C., Wittmann C., Elser D., Skaar J., Makarov V. *Nat. Photonics*, **4** (10), 686 (2010).
8. Bugge A.N., Sauge S., Ghazali A.M.M., Skaar J., Lydersen L., Makarov V. *Phys. Rev. Lett*., **112** (7), 070503 (2014).
9. Blum M., Micali S. *SIAM J. Comput.*, **13** (4), 850 (1984).
10. Ященко В.В., Варнавский Н.П., Нестеренко Ю.В. и др. *Введение в криптографию* (М.: МЦНМО, 2012).
11. Смарт Н. *Криптография* (М.: Техносфера, 2005).
12. Yuen H.P. arXiv:quant-ph/0311061 (2003).
13. Hirota O., Sohma M., Fuse M., Kato K. *Phys. Rev. A*, **72**, 02335 (2005).
14. Futami F., Guan K., Gripp J., Kato K., Tanizawa K., Chandrasekhar S., Winzer P.J. *Opt. Express*, **25** (26), 33338 (2017).
15. Trushechkin A.S., Tregubov P.A., Kiktenko E.O., Kurochkin Y.V., Fedorov A.K. *Phys. Rev. A*, **97**, 012311 (2018).
16. Трегубов П.А., Трушечкин А.С. *Итоги науки и техники. Сер. «Современная математика и ее приложения. Тематические обзоры»*, **151**, 91 (2018).
17. Guha S., Hayden P., Krovi H., Lloyd S., Lupo C., Shapiro J.H., Takeoka M., Wilde M.M. *Phys. Rev. X*, **4** (1), 011016 (2014).
18. Huttner B., Imoto N., Gisin N., Mor T. *Phys. Rev. A*, **51**, 1863 (1994).
19. Bennet C.H. *Phys. Rev. Lett.*, **68**, 3121 (1992).
20. Dušek M., Jahma M., Lütkenhaus N. *Phys. Rev. A*, **62** (2), 022306 (2000).
21. Chefles A., Barnett S.M. *Phys. Lett. A*, **250**, 223 (1998).
22. Chefles A. *Phys. Lett. A*, **239**, 339 (1998).
23. Молотков С.Н. *Письма в ЖЭТФ*, **95**, 361 (2012).
24. Miroshnichenko, G.P., Kozubov A.V., Gaidash A.A., Gleim A.V., Horoshko D.B. *Opt. Express*, **26** (9), 11292 (2018).
25. Kozubov A., Gaidash A., Miroshnichenko G. arXiv:1903.04371 (2019).
26. Holevo A.S. *IEEE Trans. Inform. Theory*, **44** (1), 269 (1998).
27. Devetak I., Winter A. *Proc. Roy. Soc. A: Math., Phys., Eng. Sci*., **461** (2053), 207 (2005).
28. Кронберг Д.А., Киктенко Е.О., Федоров А.К., Курочкин Ю.В. *Квантовая электроника*, **47** (2), 163 (2017). [*Quantum Electron*., **47** (2), 163 (2017)].
29. Кронберг Д.А., Курочкин Ю.В. *Квантовая электроника*, **48** (9), 843 (2017) [*Quantum Electron*., **48** (9), 843 (2017)].
30. Avanesov A.S., Kronberg D.A., Pechen A.N. *Ultramet. Anal. Appl.*, **10** (3), 222 (2018).