О возможностях использования практических ограничений перехватчика в квантовой криптографии

А.С.Аванесов, Д.А.Кронберг

Важным преимуществом квантовой криптографии перед классической является то, что секретность передаваемых ключей не связана с предположениями о возможностях перехватчика и гарантируется законами природы. Тем не менее в ряде ситуаций имеет смысл рассмотреть некоторые разумные предположения о возможностях перехватчика, позволяющие увеличить скорость распределения секретного ключа. Предлагаются методы использования легитимными пользователями некоторых практических ограничений, а также строятся атаки, которые перехватчик может применить в условиях этих ограничений.

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

1. Введение

Важнейшим свойством квантовой криптографии, впервые предложенной в работе [1], является то, что она не использует предположения о вычислительных способностях перехватчика, а опирается на фундаментальный запрет на извлечение полной информации из неортогональных квантовых состояний.

Тем не менее квантовая криптография всё-таки использует ряд предположений, таких как наличие у легитимных пользователей генераторов случайных чисел и корректная работа устройств на передающей и приёмной сторонах. Если перехватчик использует не известные легитимным пользователям несовершенства аппаратуры (в том числе вызванные такими действиями перехватчика, как лазерный урон), квантовая криптография теряет свою стойкость [2–6]. Это также может произойти при вмешательстве перехватчика в работу генераторов случайных чисел, вследствие чего перехватчик получает информацию о генерируемых последовательностях. Кроме того, безусловная секретность передаваемых данных возможна только при использовании ключа в режиме одноразового шифроблокнота [7], что вследствие существующих ограничений на скорость генерации ключа не всегда эффективно реализуется на практике. В большинстве случаев для получения секретных сообщений распределённые ключи используются в классических шифровальных алгоритмах, таких как AES.

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

Д.А.Кронберг. Математический институт им. В.А.Стеклова РАН, Россия, 119991 Москва, ул. Губкина, 8; Российский квантовый центр, Россия, 121353 Москва, Сколковское ш., 45: Московский физико-технический институт (национальный исследовательский университет), Россия, Московская обл., 141701 Долгопрудный, Институтский пер., 9; e-mail: dmitry.kronberg@gmail.ru

Поступила в редакцию 28 февраля 2020 г.

С одной стороны, в квантовой криптографии имеется тенденция к сокращению числа предположений. Так, популярна концепция квантовой криптографии, криптографическая стойкость которой не использует предположений о свойствах измерительных приборов [8], в том числе находящихся во власти перехватчика, т. к. именно атакам на измерительные приборы посвящена значительная часть работ по «взлому» систем квантовой криптографии. Следующим шагом является концепция квантовой криптографии, чья стойкость не зависит от каких бы то ни было устройств [9–11]. В этом случае единственным требованием является наличие у легитимных пользователей генераторов случайных чисел, работа по достижению аппаратной независимости которых также ведётся в настоящее время [12]. Однако учёт подобного рода возможностей злоумышленника или неидеальностей составляющих элементов протокола приводит к уменьшению скорости генерации ключа.

Представляет интерес движение в обратном направлении – исследование возможности увеличения скорости генерации ключей в квантовой криптографии при осознанном использовании ряда новых предположений. Подобный подход открывает перед легитимными пользователями новые возможности, такие как использование псевдослучайного генератора для согласования базисов [13], что требует довольно слабого предположения о невозможности быстрого решения некоторых вычислительных задач. Важным является то, что при выполнении этого предположения ключ оказывается секретным в течение неограниченного времени, что сохраняет важное преимущество квантовой криптографии перед классической. Следует отметить, что предлагаемый подход не обязательно ухудшает систему квантового распределения ключей, а связан, скорее, с выбором параметров секретности: как более жёстких, относящихся к традиционной квантовой криптографии, так и обеспечивающих более высокую скорость распределения ключей при меньшей стойкости.

В настоящей работе рассмотрены новые методы использования вычислительных ограничений, а также возможности использования других ограничений перехватчика – неидеальности линии связи и ограничения на ка-

чество квантовой памяти; кроме того, рассматриваются действия перехватчика в условиях этих ограничений.

2. Ограничения на качество линии связи

Традиционно при изучении секретности протоколов квантового распределения ключа полагается, что злоумышленник (его обычно называют Евой) имеет доступ к идеальной линии связи, в которой отсутствуют потери. Сами же легитимные пользователи (Алиса и Боб, где Алиса передает сообщения Бобу) могут использовать только доступные им на сегодняшний день технологии. В частности, в канале связи между Алисой и Бобом имеются потери. При исходной интенсивности μ_A сигнала, передаваемого между легитимными пользователями, интенсивность μ_B на выходе такова:

$$\mu_B = 10^{-\kappa_B L/10}\mu_A,$$

где κ_B – параметр затухания линии связи, а L – её длина. В сценарии атаки светоделителем [14] Ева использует возможность отвести себе часть сигнала, заменив канал между Алисой и Бобом своим каналом без потерь, а затем измерить отведённую часть оптимальным образом после объявления базисов. Возможность Евы по отведению части сигнала зависит от того, насколько малы потери в линии связи, на которую она заменяет канал между Алисой и Бобом: традиционно полагается, что Ева может использовать идеальный канал без потерь.

Тем не менее, как было отмечено в [15], потери в оптоволоконной линии связи являются не технологическими, а физическими, тогда как альтернативные технологии передачи данных (телепортация и переход на другую длину волны) в настоящее время не выглядят реализуемыми. Поэтому разумно предполагать, что канал, имеющийся в распоряжении Евы, также имеет потери. Обозначим соответствующий параметр затухания как κ_E, в этом случае часть f состояния, которую может отвести Ева, должна быть такой, чтобы на стороне Боба не наблюдалось излишнего падения интенсивности приходящего сигнала, т. е. должно выполняться условие

$$10^{-\kappa_B L/10}\mu_A = 10^{-\kappa_E L/10}(1-f)\mu_A.$$

В итоге Ева будет производить измерения над состояниями интенсивности:

$$\mu_E = f\mu_A = (1 - 10^{-(\kappa_B - \kappa_E)L/10})\mu_A.$$

В пределе большой длины линии связи L интенсивность μ_E будет стремиться к μ_A в любом канале, потери в котором меньше, чем в канале между Алисой и Бобом. Следовательно, ограничения на оптоволокно хоть и, по всей видимости, являются неустранимыми даже для технически очень продвинутого перехватчика, не дают большого преимущества легитимным пользователям. Поскольку наиболее востребованные случаи квантового распределения ключей соответствуют большим потерям, предположение о том, что Ева не обладает идеальным каналом, не ведёт к существенному улучшению ситуации для легитимных пользователей, и представляется разумным традиционное предположение о том, что перехватчик обладает идеальным каналом.

3. Ограниченные вычислительные возможности

В классических криптографических системах традиционно полагается, что вычислительные возможности перехватчика ограничены. Так, популярнейший алгоритм асимметричного шифрования RSA опирается на сложность разложения неизвестного числа на простые сомножители, а схема Диффи–Хеллмана удалённого распределения ключей предполагает сложность задачи дискретного логарифмирования [7].

Более точное предположение классической криптографии заключается в том, что перехватчик не нашёл эффективных алгоритмов быстрого решения задач и не располагает вычислительными мощностями, способными решить их за актуальное для секрета время с использованием известных в настоящее время алгоритмов.

В этом контексте важной угрозой для классической криптографии является появление у перехватчика квантового компьютера, что не только сделает невозможным использование ряда важных технологий классической криптографии, но и позволит дешифровать все данные, зашифрованные с помощью таких алгоритмов к этому времени [16]. Это ведёт к увеличению интереса к постквантовой криптографии: разработке алгоритмов, криптографическая стойкость которых не зависит от наличия у перехватчика квантового компьютера [17].

Актуальной темой представляется использование методов классической криптографии для увеличения скорости генерации ключа в квантовой криптографии с сохранением ключевого преимущества последней – неизменной криптографической стойкости ключа после его получения. Роль классических технологий в этом случае сводится к противодействию ряду атак реального времени.

В работе [13] была рассмотрена возможность использования псевдослучайных генераторов для увеличения скорости генерации ключа за счет совпадения базисов во всех посылках. Это предложение использует ряд предлагавшихся ранее идей [18–20]. Большое число базисов позволяет бороться с такой важной атакой реального времени, как атака с однозначным различением состояний (USD-атака) [21].

Рассмотрим другие возможности использования псевдослучайных генераторов на примере протоколов распределения ключей на когерентных состояниях; это протоколы COW, DPS и B92 с интенсивным опорным состоянием. Они не используют согласование базисов, поэтому псевдослучайная последовательность будет применяться не для выбора базисов, а для противодействия ряду атак путём установки псевдослучайной фазы.

Начнём с протокола COW [22], схема работы которого приведена на рис.1. В исходной версии протокола Алиса кодирует каждый передаваемый Бобу бит последовательностью из двух состояний: бит 0 соответствует паре $|\alpha\rangle|0\rangle$, а бит 1 – паре $|0\rangle|\alpha\rangle$. Здесь $|0\rangle$ – вакуумное состояние, а $|\alpha\rangle$ – когерентное состояние, задаваемое комплексным числом $\alpha = \sqrt{\mu}\exp(i\varphi)$, где μ – интенсивность состояния, а φ – его фаза. Кроме последовательностей, несущих информацию, посылаются также контрольные последовательности вида $|\alpha\rangle|\alpha\rangle$. Боб разделяет каждое пришедшее состояние на две части. Одна часть отправляется на детектор D_B, где фиксируется время прихода сигнала, другая – на интерферометр, имеющий задержку на одном плече и с помощью которого Боб наблюдает интерференцию меж-

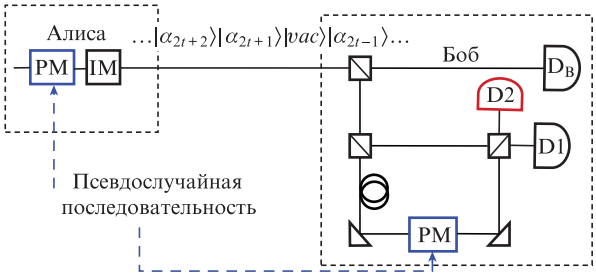

Рис.1. Схема протокола COW с использованием генератора псевдослучайных чисел; PM – фазовый модулятор, IM – модулятор интенсивности.

ду двумя последовательными невакуумными сигналами. При этом срабатывание детектора D2 говорит о потере когерентности и трактуется как присутствие Евы. В протоколе полагается, что фаза φ каждого состояния одинакова и известна злоумышленнику.

Все детекторы, рассматриваемые в этом разделе, являются однофотонными и описываются наблюдаемой

$$\left\{M_0 = |0\rangle\langle 0|,\ M_1 = \sum_{n=1}^{+\infty}|n\rangle\langle n|\right\}.$$

Вероятность их срабатывания на когерентном состоянии интенсивности μ равна $1 - \exp(-\mu)$.

В качестве модификации можно рассматривать схему, в которой Алиса выбирает фазу каждого состояния φ_t в соответствии с псевдослучайной последовательностью. В этом случае Боб использует ту же псевдослучайную последовательность и фазовый модулятор на одном из плеч интерферометра для согласования фазы и получения интерференционной картины.

Теперь Ева не знает не только интенсивность каждого состояния (0 или μ), но и его фазу φ_t (в случае отправки невакуумного состояния). Если Ева не успевает за время сеанса связи вычислить начальный ключ псевдослучайной последовательности, то она не может знать фазы пересылаемых сигналов, что не даёт ей возможности совершать атаки с отличением вакумного состояния от невакуумного [23, 24].

Покажем, как именно незнание фазы состояния мешает перехватчику детектировать вакуумные состояния. При известной фазе измерение, детектирующее вакуумные состояния, описывается наблюдаемой (разложением единицы)

$$M_0 = I - |\alpha\rangle\langle\alpha|, \quad M_? = |\alpha\rangle\langle\alpha|,$$

$$p(0|0) = 1 - |\langle 0|\alpha\rangle|^2 = 1 - \exp(-\mu).$$

В то же время задача отличения вакуумного состояния $|0\rangle$ от набора из N состояний вида

$$\{|\alpha_k\rangle\}_{k=1}^N = \{|\sqrt{\mu}\ \exp(\mathrm{i}2\pi k/N)\rangle\}_{k=1}^N$$

является более сложной. Оператор M_0^N детектирования вакуумного состояния должен обладать свойством

$$\langle\alpha_k|\, M_0^N|\alpha_k\rangle = 0\ \forall k,$$

поэтому в силу симметрии состояний $\{|\alpha_k\rangle\}_{k=1}^N$ он имеет вид $M_0^N = \lambda I - G$, где $G = N^{-1}\sum_{k=1}^N |\alpha_k\rangle\langle\alpha_k|$ – оператор Грама системы векторов $\{|\alpha_k\rangle\}_{k=1}^N$, а $\lambda = \langle\alpha_k|G|\alpha_k\rangle \leqslant \lambda_{\max}(G)$ – величина, не зависящая от конкретного вектора, но не превышающая максимальное собственное значение G. Для вероятности детектирования вакуума имеем

$$p(0|0) = \langle 0|M_0^N|0\rangle = \lambda - \langle 0|G|0\rangle \leqslant \lambda_{\max}(G) - \exp(-\mu).$$

Эта величина тем меньше, чем больше N, т. е. чем больше состояний неизвестной перехватчику фазы используют легитимные пользователи.

Такая модификация даёт возможность увеличить скорость генерации секретного ключа за счёт увеличения интенсивности состояний, испускаемых Алисой. При этом используется предположение, что Ева не может вычислить псевдослучайную последовательность за время сеанса связи и провести атаку с детектированием вакуумных состояний.

Аналогично выбор фазы пересылаемого состояния с помощью генератора псевдослучайных чисел можно использовать и в протоколе DPS [25] (рис.2). В исходной схеме данного протокола Алиса отправляет Бобу кортеж из l последовательных по времени когерентных состояний вида $|\pm\alpha\rangle$. Логические биты кодируются относительной фазой между двумя последовательными сигналами. Разность фаз 0 соответствует биту 0, а разность фаз π – биту 1. При этом Боб использует интерферометр с задержкой в одном плече для наблюдения интерференции двух последовательно идущих когерентных состояний. Срабатывание детектора D0 соответствует приёму состояний с одинаковой фазой (бит 0), а срабатывание детектора D1 – приёму состояний с противоположной фазой (бит 1).

Теперь снова положим, что Алиса приготавливает кортеж состояний вида $|\pm\alpha\exp(\mathrm{i}\varphi_t)\rangle$, причём величина φ_t для каждого элемента кортежа генерируется псевдослучайно. Бобу известен начальный ключ псевдослучайной последовательности, поэтому он может при помощи фазового модулятора согласовать фазы между двумя идущими подряд сигналами кортежа, интерференцию которых он измеряет.

При неизвестной фазе каждого состояния Ева уже не может, в частности, использовать схему, аналогичную используемой на приемной стороне, чтобы перенаправлять лишь часть кортежей, как это происходит при USD-атаке. Также затруднена атака активным светоделителем [26], при которой Ева стремится усилить интенсивность каждого состояния кортежа для возможности получения большего количества информации о ключе и блокирует весь кортеж, если многие из таких попыток потерпели неудачу.

Аналогично модификации протокола COW такая модификация позволяет увеличить скорость генерации ключа за счёт использования сигналов большей интенсивности, т. к. часть эффективных атак оказывается неприменимой.

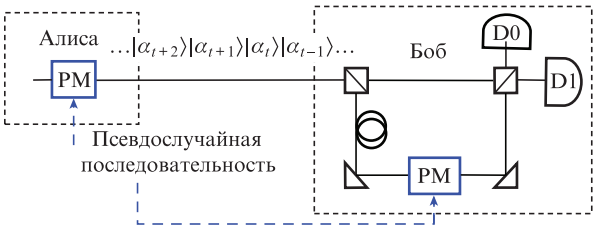

Рис.2. Схема протокола DPS с использованием генератора псевдослучайных чисел.

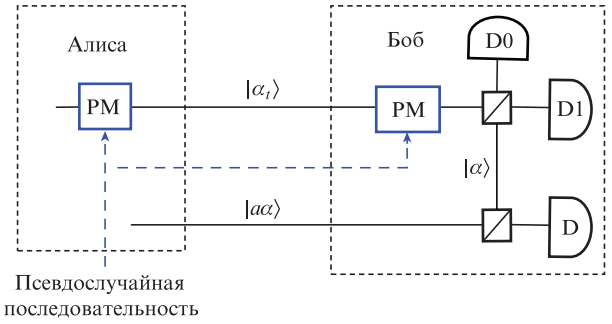

Рис.3. Схема модификации протокола с интенсивным опорным состоянием при использовании генератора псевдослучайных чисел.

Третьим протоколом, допускающим модификацию по подобному сценарию, является протокол B92 с интенсивным опорным состоянием [27, 28]. Схема протокола изображена на рис.3. Полагается, что в каждой посылке Алиса отправляет Бобу два состояния: сигнальное, $|\alpha_t\rangle$, и вспомогательное высокой интенсивности, $|a\alpha\rangle$ (т.е. $|a| \gg 1$), причём $|\alpha_t\rangle = |\alpha\rangle = |\sqrt{\mu}\,\rangle$ соответствует биту 0, а $|\alpha_t\rangle = |-\sqrt{\mu}\,\rangle$ – биту 1. На приёмной стороне вспомогательный импульс разделяется на две части при помощи светоделителя, параметры которого подобраны такими, чтобы одна из частей представляла собой состояние $|\alpha\rangle = |\sqrt{\mu}\,\rangle$ (рис.3), а другая шла на детектор D, по срабатываниям которого оценивается интенсивность пришедшего контрольного состояния. Далее наблюдается интерференция первой части вспомогательного импульса $|\alpha\rangle$ с сигнальным состоянием $|\alpha_t\rangle$. Срабатывание детектора D0 Боб интерпретирует как переданный бит 0, а срабатывание детектора D1 – как бит 1.

Использование генератора псевдослучайных чисел, как и в случаях протоколов COW и DPS, даёт возможность модификации рассматриваемого протокола посредством использования большего числа фаз при генерации сигнальных состояний, причём выбор фазы осуществляется псевдослучайно и согласованно между Алисой и Бобом. Неизвестная перехватчику фаза позволит сделать невозможным преобразование вероятностного усиления информационного состояния, которое встречается в атаках, разобранных в работах [24, 26, 29].

4. Ограничения на качество квантовой памяти

Наличие идеальной квантовой памяти позволяет Еве отводить часть пересылаемого Алисой сигнала и хранить его до момента объявления Алисой базисов, в которых были приготовлены передаваемые состояния, или до объявления кодовых слов, использующихся для исправления ошибки между легитимными пользователями. Однако в реальности квантовая память обладает ограничениями, и с течением времени состояния в ней могут как теряться, так и изменяться по сравнению с исходными состояниями, что ухудшает их различимость после извлечения из квантовой памяти.

Простейшей реализацией квантовой памяти может служить моток оптоволокна. Вследствие процессов затухания интенсивность извлекаемого сигнала будет падать. Так, для оптоволокна с параметром затухания 0.15 дБ/км снижение интенсивности составляет 50% при времени хранения 100 мкс (с учётом меньшей скорости распространения света в оптоволокне). Характеристики данной реализации квантовой памяти являются отправными при разработке других её видов и оценке их работы. Например, в работе [30] была реализована схема памяти, которая демонстрировала лучшее поведение, чем схема на основе оптоволокна, в том смысле, что интенсивность извлекаемого сигнала снижалась в два раза за время, превышающее 100 мкс. В той же работе представлены характеристики существующих реализаций квантовой памяти.

Отметим, что рассмотрение задачи с учётом неидеальности квантовой памяти Евы не совсем корректно при допущении о наличии у Евы коммуникационного канала без потерь. Действительно, в этом случае у перехватчика имеется возможность задержать отведённый сигнал на произвольное время, подобрав длину канала. Так как при передаче нет потерь, извлекаемое состояние не будет претерпевать затухания. Таким образом, предположение об ограниченности времени хранения квантовых состояний автоматически требует учёта затухания в коммуникационных каналах, доступных перехватчику.

Легитимным пользователям очень просто использовать ограничения перехватчика на квантовую память, поскольку, как отмечено в [15], они могут просто задержать время объявления базисов на время, за которое состояния Евы в квантовой памяти окончательно потеряют связь с состояниями Алисы. Такая задержка в условиях непрерывной пересылки квантовых состояний в системе квантового распределения ключей практически не влияет на скорость их генерации и требует лишь увеличения объёма классической памяти для хранения сырого ключа, поскольку его классическая обработка может начинаться лишь непосредственно в момент необходимости получения нового секретного ключа.

Таким образом, пользуясь предположением о неидеальности квантовой памяти перехватчика, Алиса и Боб могут при выборе адекватного времени задержки считать, что к моменту объявления классической информации перехватчик уже не обладает состояниями в квантовой памяти и не может совершить над ними необходимое измерение, дающее максимум возможной информации. В работе [31] была рассмотрена ситуация отсутствия квантовой памяти у перехватчика и показано, что в этом случае оптимальной атакой является перехват-перепосыл. Мы же используем более слабое предположение о том, что перехватчик обладает квантовой памятью и может совершать коллективные измерения, но не способен хранить в квантовой памяти состояния до момента объявления классической информации.

Важным следствием этого ограничения является то, что информацию перехватчика следует оценивать не из величины Холево его состояний, а из пропускной способности за один шаг [32]. В самом деле, классическая взаимная информация между отправителем и получателем квантовых состояний в общем случае демонстрирует супераддитивность, когда получатель может извлечь больше информации в результате коллективных измерений над всей передаваемой последовательностью; в этом случае информация получателя ограничена величиной Холево [32]. Тем не менее такой эффект достигается только при надлежащем выборе кодовых слов на передающей стороне и измерении в соответствии с этим кодированием: так, теорема 2 в [33] утверждает, что если измеряемый ансамбль состояний распадается на произведение ансамблей, относящихся к подсистемам, то взаимная информация даже при коллективном измерении такого ансамбля даётся суммой

пропускных способностей при измерении каждой подсистемы в отдельности, что соответствует аддитивному случаю. Информация, раскрываемая легитимными пользователями при исправлении ошибок, фактически представляет собой набор кодовых слов. Если же набор кодовых слов в момент измерения неизвестен, перехватчик имеет дело с измерением любой возможной строки исходных состояний, и в этом случае взаимная информация между передающей и принимающей сторонами строго аддитивна и в пересчёте на одну посылку равна пропускной способности за один шаг. Эта пропускная способность определяется как максимальная взаимная информация при индивидуальных измерениях квантовых состояний:

$$C_1 = \max_{\{p_i\},\Gamma} I_1(\{p_i\},\Gamma),$$

где $I_1(\{p_i\},\Gamma)$ – взаимная информация при вероятностях состояний на передающей стороне $\{p_i\}$ и применении наблюдаемой Γ на приёмной стороне. Нахождение оптимальной наблюдаемой Γ для произвольного ансамбля состояний является нетривиальной задачей, однако можно привести значения двух неортогональных чистых состояний, таких как когерентные состояния $|\pm\alpha\rangle$, для которых величина Холево χ и пропускная способность за один шаг C_1 известны [32]:

$$C_1 = 1 - h_2\left(\frac{1-\sqrt{1-|\langle -\alpha|\alpha\rangle|^2}}{2}\right) = 1 - h_2\left(\frac{1-\sqrt{1-\exp(-4\mu)}}{2}\right),$$

$$\chi(|\pm\alpha\rangle) = h_2\left(\frac{1-|\langle -\alpha|\alpha\rangle|}{2}\right) = h_2\left(\frac{1-\exp(-2\mu)}{2}\right),$$

где $\mu = |\alpha|^2$ – интенсивность; $h_2(x) = -(1-x)\log_2(1-x) - x\log_2 x$ – бинарная энтропия Шеннона. Так, если в канале не было ошибок, а перехватчик смог отвести себе состояния интенсивности $\mu = 0.2$ фотона на импульс, длина секретного ключа при оценке информации перехватчика по величине Холево [34] равна $1-\chi \approx 0.354$ бит на посылку, а при оценке информации по пропускной способности за один шаг она составляет $1 - C_1 \approx 0.555$ бит на посылку, что существенно выгоднее легитимным пользователям. При интенсивности отведенных перехватчиком состояний 0.5 эти величины составят приблизительно 0.1 и 0.219 бит на посылку, что означает выгоду более чем в два раза. Ещё раз отметим: здесь используется лишь предположение, что Ева совершает измерения, не зная набора кодовых слов, при этом у Евы есть возможность иметь квантовую память и совершать коллективные измерения, однако же выигрыша от их использования она не получит.

Также из предположения об ограниченности квантовой памяти у Евы следует, что Ева будет проводить измерения состояний без знания базиса, в котором они были приготовлены. Это обстоятельство накладывает дополнительные ограничения на величину информации, получаемой Евой при помощи измерений.

В целом, легитимные пользователи могут использовать состояния большей интенсивности с целью увеличения скорости генерации ключа. Однако Алиса и Боб всё равно не могут делать пересылаемые состояния сколь угодно различимыми, даже при использовании очень большого числа базисов. Действительно, в случае передачи сигналов большой интенсивности Ева может отвести себе часть состояния и провести над ним измерение, сохранив его классический результат в памяти. После процедуры согласования базисов между легитимными пользователями Ева использует результаты своих измерений и новую информацию для определения переданного бита. В качестве иллюстрации рассмотрим конфигурацию симметричных когерентных состояний из [13] и атаку, где перехватчиком отводится часть состояния, над которым затем производится гомодинирование, т. е. измеряется квадратура $\hat{X}_\phi = \hat{a}\exp(i\phi) + \hat{a}^\dagger\exp(-i\phi)$. Положим $\phi = 0$, тогда функция плотности распределения вероятностей исходов x такого измерения в случае когерентного состояния $|\alpha\rangle$ имеет вид

$$P(x|\alpha) = \sqrt{\frac{2}{\pi}}\exp[-2(x - \mathrm{Re}\,\alpha)^2].$$

Рассмотрим конфигурацию, в которой фазовый сдвиг между базисными состояниями есть $\delta\pi$. Пусть b – номер базиса, k – передаваемый бит, а M – число базисов. Тогда Алиса отсылает состояния вида

$$|\alpha_{b,k}\rangle = |\sqrt{\mu}\exp(i\varphi_{b,k})\rangle,$$

где μ – интенсивность; $\varphi_{b,k} = \pi(b/M + k)$ – фаза.

Таким образом, плотность распределения исходов измерения Евы при условии выбора Алисой базиса b и бита k имеет вид

$$P(x|k,b) = \sqrt{\frac{2}{\pi}}\exp\left\{-2\left[x - \sqrt{\mu}\cos\left(\frac{\pi b}{M} + \pi k\right)\right]\right\}.$$

Используя формулу Байеса, можно получить апостериорную вероятность того, что Алиса отправляла бит k при условии получения результатов измерения Евой и того, как базис объявлен. Биты выбираются равновероятно, т. е. $P(k|b) = 1/2$ для всех значений k и b. Параметр k может принимать два значения: 0 или 1. Имеем

$$P(0|x,b) = \frac{1}{1+\exp[-8x\sqrt{\mu}\cos(\pi b/M)]}.$$

Для условной взаимной информации между Алисой и Евой получаем

$$I(\mathrm{A}:\mathrm{B}|x,b) = 1 - h_2(P(0|x,b)),$$

где $h_2(q) = -q\log_2(q) - (1-q)\log_2(1-q)$. Интегрируя по x и суммируя по b, получаем величину взаимной информации

$$I(\mathrm{A}:\mathrm{E}) = 1 - \frac{1}{M}\int_{-\infty}^{+\infty} dx \sum_{b=0}^{M-1} P(x|b)h_2(P(0|x,b)) = 1 - \int_{-\infty}^{+\infty} dx\,\mathcal{L}(x),$$

где

$$\mathcal{L}(x) = \frac{1}{M}\sqrt{\frac{1}{2\pi}}\sum_{b=0}^{M-1}\{\exp[-2(x+f(b))^2] \times \log_2[1+\exp[8f(b)x]] + \exp[-2(x-f(b))^2] \times \log_2[1+\exp[-8f(b)x]]\};$$

$$f(b) = \sqrt{\mu}\cos(\pi b/M).$$

При таком измерении сам по себе результат x без знания базиса b не несёт информации о сигнале k, но эту информацию можно получить после объявления базиса, при этом большое число базисов M хоть и снижает вероятность достоверного различения всех состояний [35], почти не усложняет проведение описанного измерения. Из этого следует вывод, что даже в отсутствие у перехватчика квантовой памяти и незнания базиса в момент передачи сигналов состояния внутри базиса, вообще говоря, нельзя делать сколь угодно различимыми.

Отметим, что при высоких интенсивностях в случае использования легитимными пользователями нечётного числа базисов взаимная информация оказывается близкой к единице, т. е. $I(\mathrm{A}:\mathrm{E}) \sim 1$. Однако в случае использования чётного числа базисов это не так: $I(\mathrm{A}:\mathrm{E}) \sim 1 - M^{-1}$. Уменьшение информации связано с тем, что в рассматриваемой схеме атаки Ева будет иметь проблемы с различением состояний $|\pm \mathrm{i}\alpha\rangle$, проекции которых на ось гомодинирования совпадают. Для того чтобы сделать извлекаемую информацию близкой к единице, перехватчику следует повернуть ось гомодинирования в фазовой плоскости на угол $\varphi = -\pi/(2M)$ так, чтобы относительно неё не было состояний одного базиса с совпадающими проекциями. При $\varphi = -\pi/(2M)$ величина $f(b)$ модифицируется как $f(b) \to \sqrt{\mu}\cos[\pi b/M + \pi/(2M)]$ и для всех $b \in \{0,\ldots,M-1\}$ функция $f(b)$ становится ненулевой. В итоге, при высоких интенсивностях $I(\mathrm{A}:\mathrm{E}) \sim 1$. Зависимость величины $I(\mathrm{A}:\mathrm{E})$ от значений μ представлена на рис.4.

В связи с желанием использовать большое число базисов (выбираемых случайным или псевдослучайным образом) для противодействия перехватчику, не обладающему квантовой памятью, можно сформулировать следующую теоретическую задачу: нахождение ансамбля состояний R, разбитых на набор базисов B так, чтобы при знании базиса и проведении измерения Γ_{B}, зависящего от него, информация о ключе K была бы велика, при незнании же базиса любое измерение Γ, не зависящее от B, давало бы малую информацию о ключе, даже когда базис становится известен:

$$I(K,\Gamma|B) \ll I(K,\Gamma_{\mathrm{B}}|B).$$

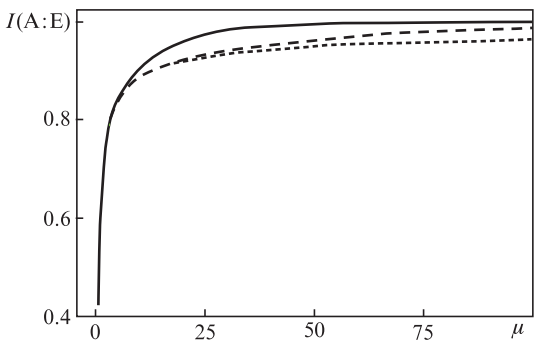

Рис.4. Зависимости функции взаимной информации $I(\mathrm{A}:\mathrm{E})$ от интенсивности передаваемых Алисой состояний при гомодинировании вдоль оси $\varphi = -\pi/(2M)$. Рассматривается протокол на симметричных когерентных состояниях с фазовым сдвигом векторов внутри базиса $\delta = \pi$. Сплошная кривая отвечает числу базисов $M = 8$, штриховая – $M = 16$, пунктирная – $M = 64$.

Наличие такого ансамбля состояний означало бы возможность использования его в квантовой криптографии: Боб мог бы использовать выбор базиса (случайным или псевдослучайным образом), после чего при случайном выборе базисов пользователи отбрасывали бы посылки с несовпавшими значениями и измеряли величину $I(K,\Gamma_{\mathrm{B}}|B)$ в качестве взаимной информации; в то же время перехватчик ограничен измерениями, которые не зависят от выбора базиса, хоть и его взаимная информация вычисляется при последующем знании базиса.

Как было показано выше, конфигурация симметричных когерентных состояний большой интенсивности плохо подходит для этой цели, т. к. перехватчик может совершить измерение и после раскрытия базисов получить из результатов измерений много информации о ключе.

Эта задача имеет сходство с классической задачей построения функции с секретом [7], т. е. функции $F_k(x)$, для которой легко вычислить $y = F_k(x)$, зная x, и так же легко вычислить x, зная y и k; в то же время нет эффективных алгоритмов вычисления x по y без знания k. Такие функции используются в ряде классических алгоритмов, в частности RSA, однако до сих пор остается открытым вопрос об их существовании, и для построенных функций утверждение, что x по y действительно сложно вычислить, является лишь предположением, опирающимся на то, что для ряда задач за продолжительное время не удалось найти эффективных алгоритмов решения.

Для ансамблей квантовых состояний роль подобного «секрета» играет знание базиса. Задача построения «ансамбля с секретом» нетривиальна, т. к. само по себе построение оптимальной наблюдаемой является сложной задачей для пространств высоких размерностей, в то время как в задаче требуется оптимальность наблюдаемой с учетом последующего получения дополнительной информации.

Отметим, что поставленную задачу можно также обобщить на случай, когда перехватчику доступна блокировка части состояний. Такие измерения [21], как правило, дают больше информации перехватчику, что улучшает его возможности. Важным является то, что решение о блокировке должно быть принято без знания секрета, и построенное выше измерение в принципе это позволяет, т. к. информация о ключе зависит от значения x, полученного при измерении: при больших значениях x информации больше. Это даёт возможность обобщить атаку на случай, когда перехватчик блокирует часть состояний. Обычно протоколы квантовой криптографии используют методы защиты от блокирования части состояний, к которым относят упомянутые выше распределённое кодирование, отправку интенсивного опорного состояния, а также использование состояний-ловушек [36].

5. Заключение

Рассматриваемые в работе ограничения возможностей перехватчика, в первую очередь его вычислительных ресурсов и времени хранения квантовых состояний, позволяют легитимным пользователям согласовывать базисы при помощи генератора псевдослучайных чисел и увеличивать интенсивности используемых в протоколе сигналов. Это приводит к увеличению скорости генерации ключей. В качестве примеров рассматривались протоколы на когерентных состояниях.

Предположение о вычислительных возможностях Евы позволяет использовать большее число базисов, что делает рассматриваемые в работе протоколы более устойчивыми к некоторым атакам. При этом согласование базисов при помощи генератора псевдослучайных чисел позволяет не уменьшать скорость генерации ключей.

Предположение об ограниченности времени хранения квантового состояния даёт возможность использовать состояния более высокой интенсивности, что также увеличивает скорость генерации ключей. Однако протоколы, в которых используются состояния слишком высокой интенсивности, оказываются уязвимыми. На примере протокола на геометрически однородных когерентных состояниях была вычислена информация Евы о ключе, которую она может получить посредством гомодинирования и последующего использования информации, раскрытой Алисой при согласовании базисов (при рассмотрении проблемы об ограничениях квантовой памяти полагалось, что базисы выбираются случайно).

Основным выводом работы является то, что в системы квантовой криптографии должна быть встроена возможность увеличения скорости генерации ими ключа при некоторых реалистичных предположениях о возможностях перехватчика, чтобы наряду с полностью защищенным режимом была возможность более быстрой генерации ключа, обладающего практической стойкостью, в частности против атак реального времени, с сохранением ключевого преимущества квантовой криптографии: неизменной стойкости ключа после его генерации. Такая схема представляется более стойкой, чем система с медленной генерацией полностью секретного ключа методами «чистой» квантовой криптографии, после которой ключ используется в классической симметричной системе для шифрования большого объема данных. Этот вопрос актуален, пока не разработаны системы квантовой криптографии, способные обеспечить скорость генерации ключа, достаточную для шифрования в режиме одноразового шифроблокнота.

В связи с этим представляются осмысленными следующие задачи: строгое обоснование формулы для скорости генерации ключа при практических ограничениях, а также разработка конфигурации квантовых состояний, для которых максимальная взаимная информация при не зависящем от базиса измерении будет ограничена небольшой величиной, в то время как при измерении с известным базисом есть возможность извлечь большой объем информации, в том числе после отбрасывания неопределенных исходов.

Авторы выражают благодарность А.С.Трушечкину за многочисленные обсуждения.

Исследование выполнено за счет гранта Российского научного фонда (проект №18-71-00074).

1. Bennett Ch.H., Brassard G., in *Proc. Int. Conf. Comput., Syst. Sign. Proces*. (Bangalore, India, 1984, pp 175–179).
2. Qi B., Fung C.H.F., Lo H.K., Ma X.; arXiv preprint quant-ph/0512080 (2005).
3. Gisin N., Fasel S., Kraus B., Zbinden H., Ribordy G. *Phys. Rev. A*, **73** (2), 022320 (2006).
4. Makarov V., Anisimov A., Skaar J. *Phys. Rev. A*, **74** (2), 022313 (2006).
5. Lydersen L., Wiechers C., Wittmann C., Elser D., Skaar J., Makarov V. *Nature Photon*., **4** (10), 686 (2010).
6. Bugge A.N., Sauge S., Ghazali A.M.M., Skaar J., Lydersen L., Makarov V. *Phys. Rev. Lett*., **112** (7), 070503 (2014).
7. Ященко В.В., Варнавский Н.П., Нестеренко Ю.В. и др. *Введение в криптографию* (М.: МЦНМО, 2012).
8. Lo H.K., Curty M., Qi B. *Phys. Rev. Lett*., **108** (13), 130503 (2012).
9. Acín A., Massar S., Pironio S. *New J. Phys*., **8** (8), 126 (2006).
10. Acín A., Brunner N., Gisin N., Massar S., Pironio S., Scarani V. *Phys. Rev. Lett*., **98** (23), 230501 (2007).
11. Vazirani U., Vidick T. *Commun. ACM*, **62** (4), 133 (2019).
12. Liu Y., Zhao Q., Li M.H., Guan J.Y., Zhang Y., Bai B., Li H. *Nature*, **562** (7728), 548 (2018).
13. Аванесов А.С., Кронберг Д.А. *Квантовая электроника*, **49** (10), 974 (2019) [*Quantum Electron*., **49** (10), 974 (2019)].
14. Bennett C.H., Bessette F., Brassard G., Salvail L., Smolin J. *J. Cryptology*, **5** (1), 3 (1992).
15. Gisin N., Ribordy G., Tittel W., Zbinden H. *Rev. Mod. Phys*., **74**, 145 (2002).
16. Shor P.W., in *Proc. 35th Ann. Symp. Foundati. Comput. Sci*. (Santa Fe, 1994, p. 124).
17. Bernstein D.J., Buchmann J., Dahmen E. (Eds) *Post-Quantum Cryptography* (Berlin, Heidelberg: Springer, 2009).
18. Hirota O., Sohma M., et al. *Phys. Rev. A*, **72** (2), 022335 (2005).
19. Kurochkin Y. *Quantum Inform*., **5833**, 213 (2004).
20. Trushechkin A.S., Tregubov P.A., Kiktenko E.O., Kurochkin Y.V. Fedorov A.K. *Phys. Rev. A*, **97** (1), 012311 (2018).
21. Dušek M., Jahma M., Lütkenhaus N. *Phys. Rev. A*, **62** (2), 022306 (2000).
22. Stucki D., Brunner N., Gisin N., Scarani V., Zbinden H. *Appl. Phys. Lett*., **87** (19), 194108 (2005).
23. Branciard C., Gisin N., Lütkenhaus N., Scarani V. *Appl. Phys. Lett*., **87**, 194108 (2005).
24. Kronberg D.A., Nikolaeva A.S., Kurochkin Y.V., Fedorov A.K. *Phys. Rev. A*, **101** (3), 032334 (2020).
25. Inoue K., Waks E., Yamamoto Y. *Phys. Rev. Lett*., **89** (3), 037902 (2002).
26. Avanesov A.S., Kronberg D.A., Pechen A.N. *p-Adic Numbers, Ultrametric Analys, Applicat*., **10** (3), 222 (2018).
27. Bennett C.H. *Phys. Rev. Lett*., **68** (21), 3121 (1992).
28. Tamaki K., Lütkenhaus N., Koashi M., Batuwantudawe J. *Phys. Rev. A*, **80** (3), 032302 (2009).
29. Кронберг Д.А., Курочкин Ю.В. *Квантовая электроника*, **48** (9), 843 (2018) [*Quantum Electron*., **48** (9), 843 (2018)].
30. Cho Y.-W., Campbell G.T., Everett J.L., Bernu J., Higginbottom D.B., Cao M.T., Geng J., Robins N.P., Lam P.K., Buchler B.C. *Optica*, **3** (1), 100 (2016).
31. Bechmann-Pasquinucci H. *Phys. Rev. A*, **73** (4), 044305 (2006).
32. Холево А.С. *Квантовые системы, каналы, информация* (М.: МЦНМО, 2010, с. 327).
33. Sasaki M., Kato K., Izutsu M., Hirota O. *Phys. Rev. A*, **58** (1), 146 (1998).
34. Devetak I., Winter A. *Proc. Royal Soc. A*, **461**(2053), 207 (2005).
35. Chefles A., Barnett S.M. *Phys. Lett. A*, **250** (4-6), 223 (1998).
36. Lo H. K., Ma X., Chen K. *Phys. Rev. Lett*., **94** (23), 230504 (2005),