КВАНТОВАЯ КРИПТОГРАФИЯ

Анализ уязвимости когерентного протокола квантовой криптографии к атаке методом активного светоделителя

Д.А.Кронберг, Е.О.Киктенко, А.К.Федоров, Ю.В.Курочкин

Рассмотрен новый тип атаки на когерентный протокол квантового распределения ключа (протокол COW). Основная идея атаки состоит в индивидуальном измерении части перехваченных состояний и пересылке остальной их части в неизмененном виде. Рассчитаны оптимальные значения параметров атаки для произвольной длины канала связи, а также проведено ее сравнение со стандартной атакой со светоделителем.

Ключевые слова: *квантовая криптография, квантовая теория информации.*

1. Введение

Развитие средств управления индивидуальными квантовыми системами играет ключевую роль во внедрении квантовых технологий. В свою очередь, квантовые технологии обладают огромным потенциалом для развития современных вычислительных устройств [1 – 3] и средств коммуникаций [4]. В частности, использование квантовых систем в качестве элементарных структурных элементов для компьютеров позволяет добиться колоссального выигрыша в производительности в ряде задач [3], например при поиске по неупорядоченной базе данных [5], а также в задачах факторизации и дискретного логарифмирования [6]. Последние задачи имеют особо важное значение для криптографии с открытым ключом [7, 8], которая базируется на сложности их решения для классических компьютеров. С появлением квантовых вычислительных устройств такие задачи могут решаться гораздо быстрее, что ставит под угрозу существующие методы защиты информации с использованием криптографических средств. Кроме того, не доказано отсутствие эффективных неквантовых алгоритмов для решения таких задач.

Появление квантовых компьютеров ограничивает спектр возможных решений для криптографии фактически двумя возможными методами. Первый из них состоит в использовании в качестве основы для новых систем с открытым ключом задач, для которых отсутствуют как классические, так и квантовые эффективные алгоритмы. Совокупность таких методов составляет основу постквантовой криптографии [9]. Однако поскольку доказательство отсутствия эффективного алгоритма является чрезвычайно сложной задачей, подобные методы, по всей видимости, еще долго будут потенциально уязвимыми.

Другим возможным решением является использование криптографии с закрытым ключом. С одной стороны, такие системы (при определенных условиях) являются абсолютно стойкими [10]. Если легитимные пользователи (передатчик Алиса и приемник Боб) обладают идентичными случайными закрытыми ключами, которые используются только один раз, а размер ключей равен или превышает размер сообщения, то по теореме Шеннона [10] сообщения, зашифрованные таким ключом по схеме одноразового блокнота (one-time pad) [11], принципиально не могут быть дешифрованы злоумышленником (Евой). Однако распространение ключей, удовлетворяющих этим требованиям, является сложной задачей.

Для решения задачи распространения ключей можно использовать ресурс квантовых систем [4]. При передаче информации с помощью индивидуальных квантовых объектов (например, одиночных фотонов) конфиденциальность будет гарантироваться принципами квантовой физики [12, 13]. Во-первых, произвольное квантовое состояние не может быть скопировано в соответствии с теоремой о запрете клонирования (no-cloning theorem) [14]. Во-вторых, пара состояний, которым отвечают некоммутирующие эрмитовы операторы, не может быть гарантированно различима. Наконец, любое измерение вносит возмущение или уничтожает квантовое состояние. Таким образом, при распределении ключа с помощью одиночных фотонов получается схема, которая позволяет достоверно обнаружить факт вмешательства в процесс генерации ключа. Следовательно, метод квантового распределения ключа потенциально позволит построить новую архитектуру информационно-телекоммуникационных систем, в которых конфиденциальность передаваемой информации будет гарантироваться фундаментальными законами физики. Тем не менее, несовершенства технической реализации систем квантового распределения ключа, такие как поглощение фотонов в оптоволокне, эффективность детекторов одиночных фотонов, а также действия

Д.А.Кронберг. Математический институт им. В.А.Стеклова РАН, Россия, 119991 Москва, ул. Губкина, 8; Московский государственный университет им. М.В.Ломоносова, Россия, 119991 Москва, Воробьевы горы; e-mail: dmitry.kronberg@gmail.com
Е.О.Киктенко. ООО «ДЕФАН», Россия, 143025 Москва, д. Сколково, ул. Новая, 100; Московский государственный технический университет им. Н.Э.Баумана, Россия, 105005 Москва, 2-я Бауманская ул., 5, стр. 1
А.К.Федоров. Российский квантовый центр, Россия, 143025 Москва, д. Сколково, ул. Новая, 100А; ООО «Акронис», Россия, 127566 Москва, Алтуфьевское ш., 44; LPTMS, CNRS, Univ. Paris-Sud, Universite Paris-Saclay, Orsay 91405, France
Ю.В.Курочкин. Российский квантовый центр, Россия, 143025 Москва, д. Сколково, ул. Новая, 100А

Поступила в редакцию 19 октября 2016 г., после доработки – 12 декабря 2016 г.

злоумышленника, использующего эти несовершенства, могут привести к возможным атакам. В частности, если длина квантового канала превышает некоторую критическую величину, то гарантировать конфиденциальность распределенных ключей становится невозможно [13].

Стоит отметить, что атаки на системы квантового распределения ключа можно условно разделить на два класса. Первый класс – это атаки на протоколы распределения ключа. Под протоколом квантового распределения ключа принято понимать общую схему приготовления и измерения квантовых состояний, а также процедуру получения из результатов измерений квантовых состояний ключа на стороне Алисы и Боба. Первым протоколом квантового распределения ключа является протокол BB84. При рассмотрении атак данного класса традиционно предполагается [12, 13], что злоумышленник обладает всеми технологическими ресурсами, которые не противоречат законам физики [12], например квантовым компьютером, квантовой памятью и идеальными каналами передачи квантовых состояний. Безусловно, практическая реализация рассматриваемых атак существенно зависит от требуемых технологических ресурсов. Второй класс предполагает атаки на техническую реализацию квантово-криптографических систем (так называемый «квантовый хакинг») [15–17]. Например, это атаки на определенный тип детекторов одиночных фотонов [17].

Устройства для квантового распределения ключа доступны на рынке. Тем не менее, на пути к их внедрению имеется ряд технологических трудностей. Один из наиболее перспективных методов работы с квантовыми системами, который применяется в устройствах квантовой криптографии, – это использование ослабленных когерентных состояний вместо одиночных фотонов и, следовательно, когерентных протоколов квантового распределения ключа, например протокола coherent one-way (COW) [18–20]. Данные протоколы восходят к классическим средствам коммуникаций с использованием оптоволоконных систем [20]. Наиболее значимым преимуществом протокола COW является простота его реализации [13, 18–20], связанная с достаточно несложной оптической схемой. Данный протокол легко реализуется экспериментально и был использован в проекте по построению европейской сети квантового распределения ключа SECOQC [21]. Однако, несмотря на распространенность данного метода и его несомненную практическую значимость, анализ возможности атак, позволяющих злоумышленнику получить информацию о ключе, остается актуальной задачей [18–26].

Отметим также, что системы квантового распределения ключа не являются в полном смысле системами связи или коммуникаций. Квантовый ресурс в виде одиночных фотонов используется не для передачи информации, а для генерации случайной идентичной для легитимных пользователей последовательности бит (ключа). Типичная скорость генерации ключа в таких системах составляет величины порядка 10 кбит/с на расстояниях 50–80 км. Некоторым ограничением таких систем является то обстоятельство, что для генерации ключа легитимным пользователям требуется выделенный прямой канал (т.е. используется топология сети «точка-точка»). После того как ключ распределен, он может использоваться для шифрования в режиме одноразовых блокнотов или в качестве источника энтропии. Конечная скорость передачи информации зависит в этом случае от системы связи, передающей зашифрованную информацию.

В настоящей работе мы рассматриваем новый тип атаки на протокол квантового распределения ключа COW. Основная идея атаки заключается в индивидуальном измерении части перехваченных состояний и пересылке остальной их части в неизмененном виде. Предлагаемая атака относится к первому классу (к атакам на протокол). Одним из ее преимуществ, однако, является тот факт, что реализация данной атаки не требует использования квантовой памяти или сложных элементов, а ограничивается распространенным предположением о наличии у злоумышленника канала без потерь. В остальном же предлагаемая атака имеет достаточно простую оптическую схему для реализации, позволяя добиться преимущества по сравнению с известной атакой со светоделителем при определенных ограничениях на параметры системы распределения ключа.

2. Когерентный протокол квантового распределения ключа (COW)

В протоколе квантового распределения ключа COW Алиса и Боб используют два информационных состояния [18–20], в которых значение бита (0 или 1) кодируется через когерентное состояние $|\alpha\rangle$ в одном из двух временных окон, в то время как в другом временном окне находится вакуумное состояние. Следовательно, состояния, соответствующие 0 и 1, могут быть представлены в следующем виде:

$$|\psi_0\rangle = |\alpha\rangle\otimes|0\rangle,\ |\psi_1\rangle = |0\rangle\otimes|\alpha\rangle, \tag{1}$$

где интенсивность когерентного состояния $|\alpha\rangle$ мы обозначим как $\mu = |\alpha|^2$.

Одним из наиболее простых сценариев атаки на протокол COW является атака «перехват-пересылка». В ней Ева пытается измерить состояние в каждом временном окне с последующей пересылкой полученного состояния (с увеличением интенсивности для компенсации потерь). Для того чтобы обнаружить злоумышленника, использующего подобную атаку, помимо информационных состояний Алиса и Боб используют контрольные состояния вида

$$|\psi_c\rangle = |\alpha\rangle\otimes|\alpha\rangle. \tag{2}$$

Контрольные состояния используются для детектирования попытки различения информационных состояний. При атаке перехватчик будет время от времени посылать информационные состояния вместо контрольных, что позволит его обнаружить. Долю контрольных состояний обозначим как f, обычно она составляет $\sim$10% [13, 18–20].

3. Атака светоделителем на протокол COW

В реальных оптоволоконных линиях имеется затухание сигнала, которое приводит к тому, что Боб получает состояния меньшей интенсивности. Интенсивность получаемого Бобом состояния имеет следующий вид:

$$\mu_B = 10^{-\delta l/10}\mu, \tag{3}$$

где l – длина линии в километрах, а δ – коэффициент затухания (типичное значение коэффициента затухания для оптоволоконных линий в спектральной области 1.5 мкм составляет 0.2 дБ/км).

При анализе атак на протокол квантового распределения ключа предполагается, что Ева обладает неограниченными технологическими ресурсами. Поэтому одним из возможных сценариев атаки является использование светоделителя в сочетании с идеальным каналом связи. Поскольку на светоделителе, как и в линии связи с затуханием, состояния преобразуются самоподобным образом, Ева может отвести себе на светоделителе часть каждого состояния, отправив остальную часть Бобу, заменив канал на идеальный (канал без потерь).

Максимальная интенсивность излучения, которое может перехватить Ева, имеет вид

$$\mu_{\mathrm{E}}^{\max} = \mu - \mu_{\mathrm{B}} = (1 - 10^{-\delta l/10})\mu. \quad (4)$$

Такой отвод состояний с использованием светоделителя с точки зрения Боба ничем не отличается от затухания в канале и никак не детектируется. Дальнейшие действия Евы с отведенными состояниями могут различаться для разных атак.

Рассмотрим сценарий атаки со светоделителем, при котором Ева сохраняет у себя отведенные состояния, чтобы затем извлечь из них информацию [25]. Конфигурация состояний и измерения на приемной стороне таковы, что в отсутствие Евы (а также при отводе ею части состояний с пересылкой оставшейся части по идеальному каналу) Боб не имеет ошибки, и его взаимная информация с Алисой после отбрасывания несовместных исходов равна единице. Так как Ева имеет меньше информации, она при такой атаке вносит ошибку, чтобы ее информация сравнялась с информацией Боба. Таким образом, информационные состояния Евы при этой атаке

$$|\psi_0^{\mathrm{E}}\rangle = |\sqrt{\mu_{\mathrm{E}}^{\max}}\rangle\otimes|0\rangle,\ |\psi_1^{\mathrm{E}}\rangle = |0\rangle\otimes|\sqrt{\mu_{\mathrm{E}}^{\max}}\rangle. \quad (5)$$

Информация, которую Ева может извлечь из таких состояний при коллективном измерении, дается величиной Холево (χ-величиной) [27]:

$$I_{\mathrm{AE}} = \chi(\{|\psi_0^{\mathrm{E}}\rangle, |\psi_1^{\mathrm{E}}\rangle\}). \quad (6)$$

При этом несложно найти критическую величину ошибки QBER, которую Ева должна добавить, чтобы ее информация совпадала с информацией Боба. Критическая величина ошибки выражается через бинарную энтропию вносимой ошибки следующим образом:

$$I_{\mathrm{AB}} = 1 - h_2(\mathrm{QBER}), \quad (7)$$

где $h_2(\mathrm{QBER})$ – бинарная функция энтропии.

Сильная сторона атаки со светоделителем состоит в том, что она использует коллективные измерения над всей передаваемой последовательностью. Это позволяет благодаря квантовой супераддитивности достичь χ-величины и получить теоретический максимум информации из квантовых состояний. Однако недостатком такой атаки можно назвать то, что при больших длинах линии связи критическая ошибка протокола не стремится к нулю, так как информация Евы в пределе ограничена χ-величиной исходных состояний. В то же время, поскольку при увеличении длины линии связи до Боба доходит все меньше посылок, естественным требованием к атаке является то, чтобы она пользовалась возможностью, например, заблокировать некоторые из посылок, из которых не получилось извлечь достаточно информации.

4. Атака на протокол COW с активным светоделителем

В настоящей работе предлагается альтернативный сценарий атаки на протокол COW. Его отличие от атаки со светоделителем проявляется в следующих аспектах. Во-первых, в рассматриваемой атаке Ева отводит себе меньшую часть состояний, чем в атаке со светоделителем. Во-вторых, злоумышленник проводит измерение сразу же, над каждым состоянием индивидуально. При несовместном исходе измерения (т. е. при детектировании вакуумных состояний в обеих позициях) Ева может заблокировать посылку, так как информация о состоянии оказалась ей недоступна. В то же время блокировать все такие посылки Ева в общем случае не может, потому что тогда интенсивность на приемной стороне будет меньше ожидаемой, что выдаст Еву. Поэтому для оценки эффективности данной атаки рассмотрим ту же идею, что и при атаке со светоделителем: если длина канала не позволяет Еве заблокировать все посылки, из которых не удалось извлечь информацию, она вносит в передаваемые состояния ошибку, чтобы информация Боба сравнялась с информацией Евы. Назовем такую атаку атакой с активным светоделителем, потому что его использование зависит от того, смогла ли Ева получить информацию из отведенных состояний.

Опишем подробнее действия Евы с учетом всех параметров. Ева отводит себе часть состояний с интенсивностью μ_{E}, после чего измеряет каждое временное окно своего состояния. Ее измерение в каждом временном окне описывается наблюдаемой величиной

$$M_0 = |0\rangle\langle 0|,\ M_1 = \sum_{i=0}^{\infty} |i\rangle\langle i|. \quad (8)$$

Вероятность получить исход 1 при измерении состояния интенсивности μ_{E} есть

$$p_{\mathrm{conc}}^{\mathrm{inf}} = 1 - \exp(-\mu_{\mathrm{E}}). \quad (9)$$

Это выражение дает вероятность получить совместный исход при измерении информационного состояния (1), но с меньшей интенсивностью. При передаче же контрольного состояния вероятность получить совместный исход есть

$$p_{\mathrm{conc}}^{\mathrm{cont}} = 2\exp(-\mu_{\mathrm{E}})(1 - \exp(-\mu_{\mathrm{E}})) + (1 - \exp(-\mu_{\mathrm{E}}))^2. \quad (10)$$

Таким образом, общая вероятность совместного исхода Евы с учетом доли контрольных состояний

$$p_{\mathrm{conc}}^{\mathrm{E}} = (1 - f)\, p_{\mathrm{conc}}^{\mathrm{inf}} + f p_{\mathrm{conc}}^{\mathrm{cont}}. \quad (11)$$

Следует обратить внимание, что использование контрольных состояний не позволяет детектировать Еву, так как она все равно отправляет часть исходного состояния, не затронутую ее измерениями. Возможная ошибка Евы, когда контрольное состояние принимается за информационное, не ведет к уменьшению ее информации, т. к. по-

сылки с контрольными состояниями отбрасываются легитимными пользователями.

В случае несовместного исхода измерения Евы, вероятность которого равна $1 - p_{\mathrm{conc}}^{\mathrm{E}}$, Ева стремится заблокировать состояние, направляемое к Бобу. В общем случае, Ева может так сделать не всегда, а лишь для доли посылок, достаточно небольшой, чтобы эта блокировка не была заметна по большему затуханию на приемной стороне. Посчитаем долю посылок, доступных для блокировки.

Боб ожидает состояния с интенсивностью (3). Для этих состояний вероятность получения совместного исхода для информационных состояний равна $1 - \exp(-\mu_{\mathrm{B}})$. В реальности, при использовании светоделителя Ева имеет возможность оставить Бобу состояния большей интенсивности, чтобы иметь возможность заблокировать «неудобные» посылки, поэтому интенсивность состояний Боба $\mu'_{\mathrm{B}} = \mu - \mu_{\mathrm{E}}$. Следовательно, допустимая доля блокируемых Евой посылок b может быть получена из соотношения

$$(1 - b)(1 - \exp(-\mu'_{\mathrm{B}})) = 1 - \exp(-\mu_{\mathrm{B}}). \tag{12}$$

Эту долю блокируемых посылок можно определить для данной длины канала и данных настроек атаки Евы, а именно из того, какую часть состояния она отводит себе. Эта часть может варьироваться от части нулевой интенсивности до $\mu_{\mathrm{E}}^{\max}$, определяемой соотношением (4). Для каждой длины канала Ева должна выбирать долю отводимых состояний, дающую ей наибольшую информацию.

Информация Евы вычисляется следующим образом. В тех позициях, где Ева получила определенный исход, ее информация равна единице. В то же время для произвольной длины канала Ева не может блокировать все посылки, где она не получила полной информации, и иногда ей придется все равно отправлять их Бобу. Для вероятности совместного исхода (9) и вероятности блокирования посылки b, определяемой из (12), имеем

$$I_{\mathrm{AE}} = p_{\mathrm{conc}}^{\mathrm{inf}}/(1 - b). \tag{13}$$

Видно, что если Ева имеет возможность блокировать все посылки с несовместным исходом (т.е., если $b = 1 - p_{\mathrm{conc}}^{\mathrm{inf}}$), то ее информация равна единице. Значения параметра b, превышающие вероятность несовместного исхода, рассматривать не имеет смысла, а при меньших значениях информация Евы уменьшается и в отсутствие блокировок достигает минимума, равного вероятности совместного исхода, что и является пропускной способностью канала с затуханием.

Рассмотрим вопрос о выборе Евой оптимальной величины отводимой интенсивности μ_{E}, обеспечивающей максимум перехватываемой информации I_{AE}. Используя выражения для вероятности $p_{\mathrm{conc}}^{\mathrm{inf}}$ (9) и тождество (12), определяющее допустимую долю блокируемых Евой сообщений b, перепишем (13) в виде

$$I_{\mathrm{AE}} = \frac{(1 - \exp(-\mu + \mu_{\mathrm{E}}))(1 - \exp(-\mu_{\mathrm{E}}))}{1 - \exp(-\mu_{\mathrm{B}})}. \tag{14}$$

Нетрудно убедиться, что I_{AE} является вогнутой функцией по аргументу μ_{E}, достигающей максимума при $\mu_{\mathrm{E}} = \mu/2$. Однако в связи с тем, что интенсивность μ_{E} ограничена величиной $\mu_{\mathrm{E}}^{\max}$, максимум информации достигается при величине перехватываемой интенсивности

$$\mu_{\mathrm{E}} = \min(\mu_{\mathrm{E}}^{\max}, \mu/2). \tag{15}$$

Отметим, что в случае $\mu_{\mathrm{E}} = \mu_{\mathrm{E}}^{\max}$ мы имеем $\mu_{\mathrm{E}}^{\max} = \mu'_{\mathrm{E}}$ и $b = 1$.Таким образом, при $\mu_{\mathrm{E}}^{\max} \leqslant \mu/2$ Еве лучше всего никогда не блокировать состояния, а пересылать все сообщения Бобу.

Критическая длина l_0, при которой Еве целесообразно начать блокировать состояния, определяется тождеством

$$(1 - 10^{-\delta l_0/10}) = 1/2 \tag{16}$$

и вычисляется как

$$l_0 = 10\log_{10}2/\delta \approx 3/\delta. \tag{17}$$

Для типичного значения $\delta = 0.2$ дБ/км мы, следовательно, получаем $l_0 \approx 15$ км.

5. Обсуждение результатов

Итак, еще раз кратко опишем сценарий рассматриваемой атаки и метод поиска критической ошибки протокола. Для заданной длины канала Ева считает максимальную интенсивность состояний, которые она может отвести. Затем она рассматривает возможность отведения состояний разной интенсивности – от нуля до максимальной. Для каждой из них можно явно посчитать долю посылок, которые Ева может заблокировать, а также информацию Евы. Чем большей интенсивности состояния достались Бобу, тем больше посылок можно заблокировать. Ева выбирает интенсивность, при которой ее информация максимальна. Если она может заблокировать все посылки, где она получила несовместный исход, Ева может произвести атаку, не внося никакой ошибки, и протокол оказывается полностью несекретным. Если же доля состояний, которые можно заблокировать, оказывается меньше, Ева вносит ошибку в канал между Алисой и Бобом, чтобы нивелировать разницу между его информацией и своей. Минимальная величина ошибки, при которой их информации сравниваются, и есть критическая величина ошибки протокола против данной атаки. На рис.1 показаны критическая ошибка обычной атаки со светоделителем и рассматриваемой атаки с активным светоделителем для трех значений интенсивности.

Может возникнуть вопрос о том, какая интенсивность исходных состояний является оптимальной для легитимных пользователей в предположении, что перехватчик использует именно эту атаку. С одной стороны, для увеличения критической ошибки им нужно, очевидно, брать наименьшую интенсивность исходных состояний. С другой стороны, малая интенсивность ведет к малой скорости генерации ключа из-за слишком большой доли посылок, не достигших приемной стороны.

Будем искать оптимальную интенсивность следующим образом. Пусть Ева лишь отводит себе максимальную долю состояний, допустимую атакой, и извлекает из них всю информацию, не внося, однако, ошибки в канал между Алисой и Бобом (так как величина ошибки уже не показатель). Длина секретного ключа между Алисой и Бобом в пересчете на одну отправленную посылку дается разностью информаций между Алисой и Бобом I_{AB} и между Алисой и Евой I_{AE}. Первая равна пропускной способности канала связи с затуханием, равным вероятно-

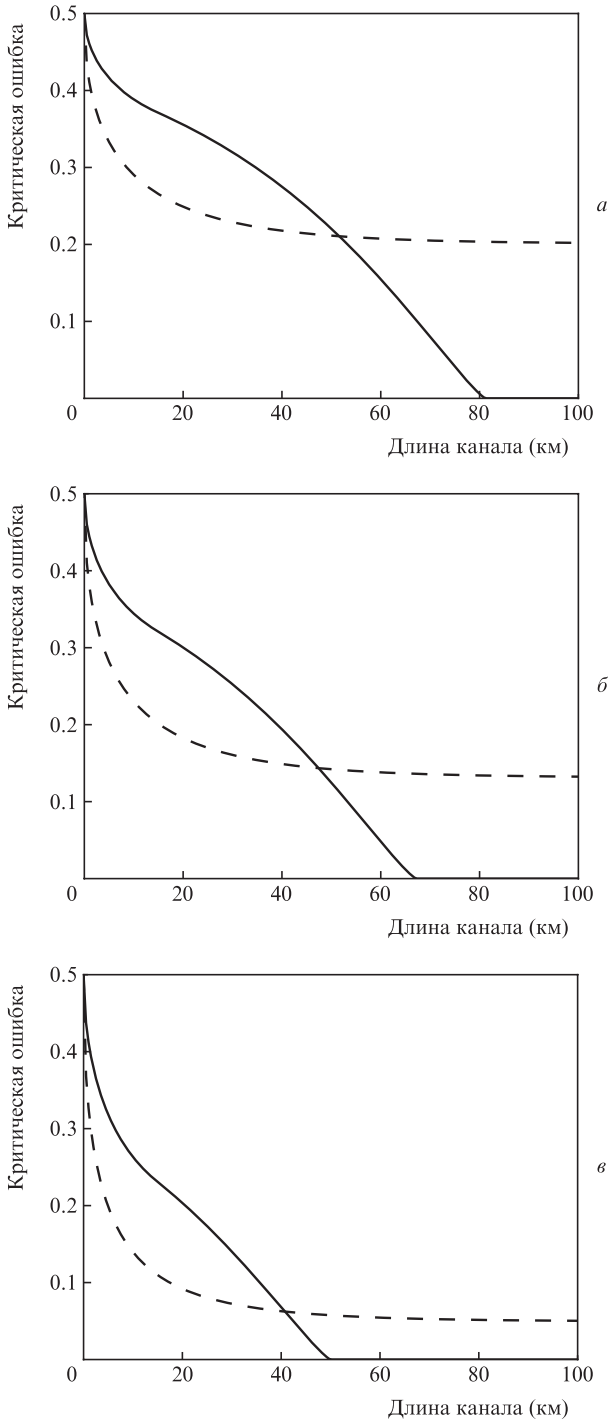

Рис.1. Сравнение критической ошибки атаки со светоделителем (штриховая линия) и рассматриваемой атаки с активным светоделителем (сплошная линия) для интенсивности $\mu = 0.1$ (*а*), 0.2 (*б*) и 0.5 (*в*).

сти несовместного исхода $\exp(-\mu_B)$, вторая может быть вычислена с использованием формулы (13), а затем также умножается на вероятность совместного исхода Боба. Оптимальным значением интенсивности для данной длины канала, таким образом, является та, при которой разность

$$I_{AB} - I_{AE} = 1 - \exp(-\mu_B) - (1 - \exp(-\mu_B))\,\frac{p_{\text{conc}}^{\text{inf}}}{1-b} \qquad (18)$$

максимальна. На рис.2 показаны оптимальная интенсивность для разных длин канала, а также критическая величина ошибки при оптимальном выборе интенсивности, если Ева решила ее внести. Для сравнения добавлена критическая ошибка атаки со светоделителем при данной длине и данном выборе интенсивности, однако заметим, что исходная интенсивность оптимизировалась в предположении, что перехватчик будет использовать именно атаку с активным светоделителем.

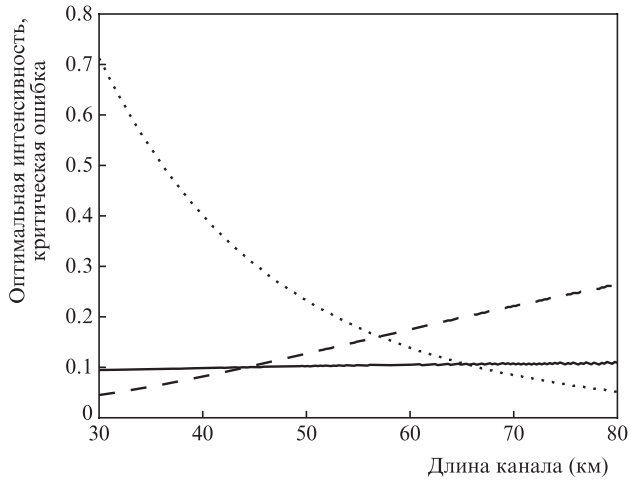

Рис.2. Оптимальная интенсивность для разных длин канала (пунктирная линия), а также критическая величина ошибки при оптимальном выборе интенсивности Евой (сплошная линия) и критическая ошибка атаки со светоделителем при данной длине и данном выборе интенсивности (штриховая линия).

Недостатком такой атаки является то, что Ева не имеет возможности усилить передаваемый Бобу сигнал для тех посылок, где она получила совместный исход. Другая слабая сторона в том, что Ева должна проводить измерения сразу же, что исключает возможность достижения ею супераддитивной информации. С другой стороны, в отличие от обычной атаки со светоделителем, такая атака, начиная с критической длины линии связи, возможна без внесения ошибки. Тем не менее, атака с измерением с определенным исходом [26] оказывается эффективнее, т.к. есть возможность усиливать интенсивность посылок, из которых была извлечена вся информация. К преимуществам рассматриваемой атаки также можно отнести относительно несложную техническую реализацию.

Таким образом, рассмотренная атака с активным светоделителем интересна, в первую очередь, тем, что она потенциально реализуема при нынешнем технологическом уровне, а не тем, что она оптимальна с точки зрения перехватчика, ограниченного только законами физики. Развитие идеи неизменной пересылки состояний представляется актуальным в контексте других протоколов квантовой криптографии, построенных на основе использования когерентных состояний [13].

Отметим также, что хотя рассмотренная атака не приводит к изменению типа состояния (контрольное состояние не может превратиться в сигнальное, и наоборот), она приводит к искажению статистики получения контрольных состояний. Данное явление связано как с изменением интенсивности пересылаемых Бобу импульсов (от μ_B к μ'_B), так и с тем, что вероятность блокировки состояний определяется вероятностью Евы получить совместный исход. В свою очередь, в случае контрольного состояния данная вероятность оказывается выше, чем в случае сигнального, и общая вероятность получения контрольного состояния Бобом увеличивается. В результате

рассматриваемая атака может быть потенциально зарегистрирована с помощью учета статистики регистрации контрольных состояний при классической постобработке ключа. Однако обычно в протоколе рассматривается лишь требование отсутствия изменения типа состояния, и для такого учета статистики будет необходимо существенное изменение протокола в части оценки информации перехватчика.

Интересным и актуальным является вопрос о модификации протокола COW для учета предлагаемой атаки. Однако данный вопрос требует дополнительного анализа и выходит за рамки данной работы.

6. Заключение

Рассмотрен новый тип атаки на когерентный протокол квантового распределения ключа COW с использованием активного светоделителя. Рассчитаны оптимальные значения параметров атаки для произвольной длины канала связи, а также проведено сравнение со стандартной атакой со светоделителем.

К преимуществам рассматриваемой атаки можно отнести относительно несложную техническую реализацию. Необходимо отметить, что предлагаемая атака фактически актуальна для каналов любой длины. Однако особую актуальность она имеет для квантово-криптографических систем, работающих в городских условиях и использующих короткие (30–50 км) городские оптоволоконные линии связи с достаточно большими потерями. В недавно проведенных экспериментах по квантовому распределению ключа в городских условиях величина потерь в канале длиной 30 км составляла ~11 дБ со скоростью генерации ключа после обработки [28] на уровне 0.5 кбит/с.

Авторы благодарят А.С.Трушечкина и О.В.Лычковского за полезные обсуждения, а также рецензентов за ряд ценных замечаний.

Работа выполнена при поддержке Минобрнауки РФ в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014–2020 годы» (соглашение №14.579.21.0105, идентификатор RFMEFI57915X0105).

1. Feynman R.P. *Intern. J. Theor. Phys.*, **21** (6), 467 (1982).
2. Feynman R.P. *Opt. News*, **11** (2), 11 (1985).
3. Deutsch D. *Proc. R. Soc. London, Ser. A*, **400**, 97 (1985).
4. Bennett C.H., Brassard G. *IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India)* (New York: IEEE, 1984, p. 175).
5. Grover L.K. *Proc. 28th Ann. ACM Symp. on the Theory of Computing* (New York: ACM Press, 1996, p. 212).
6. Shor P.W. *SIAM J. Comput.*, **26**, 1484 (1997).
7. Diffie W., Hellman M.E. *IEEE Trans. Inf. Theory*, **22** (28), 644 (1976).
8. Rivest R.L., Shamir A., Adleman L. *Commun. ACM*, **21** (2), 120 (1978).
9. Bernstein D.J. *Introduction to post-quantum cryptography* (Berlin: Springer-Verlag, 2009).
10. Shannon C. *Bell System Techn. J.*, **4** (28), 656 (1949).
11. Vernam G.S. *J. Am. Inst. Electr. Eng.*, **45**, 109 (1958).
12. Gisin N., Ribordy G., Tittel W., Zbinden H. *Rev. Mod. Phys.*, **74**, 145 (2002).
13. Scarani V., Bechmann-Pasquinucci H., Cerf N.J., Dusek M., Lutkenhaus N., Peev M. *Rev. Mod. Phys.*, **81** (3), 1301 (2009).
14. Wootters W.K., Zurek W.H. *Nature*, **299**, 802 (1982).
15. Lydersen L., Wiechers C., Wittmann C., Elser D., Skaar J., Makarov V. *Nat. Photonics*, **4**, 686 (2010).
16. Gerhardt I., Liu Q., Lamas-Linares A., Skaar J., Kurtsiefer C., Makarov V. *Nat. Commun.*, **2**, 349 (2011).
17. Jain N., Anisimova E., Khan I., Makarov V., Marquardt Ch., Leuchs G. *New J. Phys.*, **16**, 123030 (2014).
18. Stucki D., Brunner N., Gisin N., Scarani V., Zbinden H. *Appl. Phys. Lett.*, **87**, 194108 (2005).
19. Stucki D., Barreiro C., Fasel S., Gautier J.-D., Gay O., Gisin N., Thew R., Thoma Y., Trinkler P., Vannel F., Zbinden H. *Opt. Express*, **17**, 13326 (2009).
20. Stucki D., Walenta N., Vannel F., Thew R.T., Gisin N., Zbinden H., Gray S., Towery C.R., Ten S. *New J. Phys.*, **11**, 075003 (2009).
21. Alléaume R., Branciard C., Bouda J., Debuisschert T., Dianati M., Gisin N., Godfrey M., Grangier P., Langer T., Lutkenhaus N., Monyk C., Painchault P., Peev M., Poppe A., Pornin Y., Rarity J., Renner R., Ribordy G., Riguidel M., Salvail L., Shields A., Weinfurter H., Zeilinger A. *Theor. Comput. Sci.*, **560**, 62 (2014).
22. Branciard C., Gisin N., Lutkenhaus N., Scarani V. *Quantum Inf. Comput.*, **7**, 639 (2007).
23. Branciard C., Gisin N., Scarani V. *New J. Phys.*, **10**, 013031 (2008).
24. Curty M., Zhang L.L., Lo H.-K., Lutkenhaus N. *Quantum Inf. Comput.*, **7**, 665 (2007).
25. Кронберг Д.А., Молотков С.Н. *ЖЭТФ*, **145**, 5 (2014).
26. Молотков С.Н. *Письма в ЖЭТФ*, **93**, 194 (2011).
27. Холево А.С. *Квантовые системы, каналы, информация* (М.: МЦНМО, 2010).
28. Kiktenko E.O., Trushechkin A.S., Kurochkin Y.V., Fedorov A.K. *J. Phys.: Conf. Ser.*, **741**, 012081 (2016).