КВАНТОВАЯ КРИПТОГРАФИЯ

О роли флуктуаций интенсивности в квантовой криптографии на основе когерентных состояний

Д.А.Кронберг, Ю.В.Курочкин

Рассмотрен новый способ атаки в квантовой криптографии на основе когерентных состояний, требующий только возможности изменения в некоторых пределах интенсивности состояний, достигающих приемной стороны. Вычислена критическая ошибка (QBER) протокола B92 с интенсивным реперным состоянием для различных ограничений интенсивности.

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

1. Введение

Целью квантовой криптографии является распределение секретного ключа между удаленными пользователями (называемыми Алисой и Бобом) без предположений о вычислительных или технологических возможностях перехватчика (Евы). В частности, Ева может быстро решать NP-полные задачи, поэтому легитимные пользователи не вправе использовать важное предположение классической асимметричной криптографии. Основное ограничение, накладываемое квантовой механикой, состоит в том, что нельзя извлечь всю информацию из набора неортогональных квантовых состояний. В протоколах квантового распределения ключей Алиса и Боб используют неортогональные квантовые состояния для кодирования битов ключа, и эти протоколы разработаны так, чтобы Ева не могла получить всей информации о ключе без внесения ошибки в сигнальные состояния.

Протоколы квантовой криптографии на когерентных состояниях представляют большой интерес, поскольку они не требуют наличия однофотонных источников и их практическая реализация относительно проста. В таких криптографических схемах в качестве информационных состояний используются ослабленные лазерные импульсы, передаваемые по оптоволоконным линиям связи.

Затухание когерентных импульсов в оптоволоконных линиях связи дает перехватчику новые возможности, в дополнение к традиционным атакам, в ходе которых перехватчик старается извлечь информацию из ансамбля неортогональных состояний. Можно выделить два наиболее важных способа атаки на когерентные протоколы: так называемая атака светоделителем и атака измерением с определенным исходом (USD-атака).

Д.А.Кронберг. Математический институт им. В.А.Стеклова РАН, Россия, 119991 Москва, ул. Губкина, 8;
e-mail: dmitry.kronberg@gmail.com
Ю.В.Курочкин. Российский квантовый центр, Россия, 143025 Москва, Сколково, ул. Новая, 100А

Поступила в редакцию 24 мая 2018 г., после доработки – 3 июля 2018 г.

При атаке светоделителем Ева отводит часть каждого состояния в свою квантовую память, используя светоделитель, а оставшуюся часть посылает Бобу по идеальному каналу без затухания. После применения этой атаки Боб получает состояния в точности той интенсивности, которую он ожидает, поэтому атака светоделителем не детектируется на приемной стороне, но Ева получает лишь частичную информацию, ограниченную величиной Холево ее состояний [1]. После отбрасывания позиций с неопределенным результатом измерений, Боб имеет полную информацию о ключе. Цель Евы в том, чтобы иметь столько же информации о ключе, сколько и Боб, поэтому для компенсации своей неполной информации она может внести ошибку в канал между Алисой и Бобом. Чем больше информации Ева может получить из своих состояний, тем меньшую ошибку ей нужно внести. Поэтому критическая ошибка протоколов на когерентных состояниях против атаки светоделителем зависит от длины канала (она уменьшается для больших длин) и от исходной интенсивности (чем выше интенсивность, тем ниже критическая ошибка).

При USD-атаке [2] Ева проводит измерение с определенным исходом над каждым состоянием, которое иногда дает полную информацию, а иногда дает неопределенный исход (часто такой исход называют также несовместным). Если Еве повезло получить всю информацию, она посылает Бобу состояния более высокой интенсивности, а при неопределенном исходе блокирует посылку.

USD-атака не вносит ошибку, и поэтому является очень мощной, но для нее требуется возможность блокировки части посылок и усиления интенсивности другой части. Вообще говоря, после этой атаки Ева посылает не исходные состояния, а смесь состояний высокой интенсивности и вакуумных состояний. Протоколы на когерентных состояниях стремятся заблокировать эту возможность, то есть стремятся детектировать отправку вакуумных состояний. Распространенные методы включают в себя:

1. Отправку не только информационных состояний, но и состояний-ловушек другой интенсивности. Это позволяет обнаружить перехватчика по измененной статистике состояний разного типа [3].

2. Отправку контрольных состояний наряду с информационными, что делает USD-атаку более сложной и добавляет легитимным пользователям новый параметр видности для детектирования перехватчика. Известным протоколом на этой схеме является протокол Coherent One-Way (COW) [4].

3. Отправку кортежей когерентных состояний с кодированием информации через разность фаз соседних состояний, как в дифференциально-фазовом протоколе [5]. Блокирование одного состояния в этом случае также вносит ошибку.

4. Использование реперного состояния большой интенсивности, которое должно быть задетектировано Бобом. Информация кодируется в разность фаз реперного и слабого информационного импульсов. Схема была предложена при описании оригинального протокола B92 [6]. Если Ева заблокирует информационный импульс, это вызовет ошибку на приемной стороне.

В результате USD-атака может быть применена, только если интенсивность состояний, достигающих Боба, может изменяться от нуля (при отправке вакуумных состояний, т.е. при блокировании сообщения) до бесконечности, и эта атака может не вносить ошибки. Атака светоделителем не меняет интенсивность на приемной стороне и может быть применена к любому протоколу на когерентных состояниях в условиях линии связи с затуханием, но у нее сравнительно большая критическая ошибка. Встает вопрос, как Ева может использовать возможность изменять интенсивность состояний в более общем случае, когда интенсивность должна быть в некотором установленном диапазоне.

Недавно была предложена новая идея атаки на протокол COW, которая была названа «атака активным светоделителем» [7]. Она не требует измерения с определенным исходом, потому что в ней измерение применяется лишь к части исходного состояния, а остальная часть может быть отправлена Бобу без изменений. Поэтому такой способ атаки может подойти в ситуациях, когда USD-атака плохо применима, например в случае протокола COW. Наша цель в том, чтобы обобщить эту атаку для других протоколов.

В настоящей работе предлагается новый способ атаки, который в ряде случаев может рассматриваться как обобщение USD-атаки и атаки светоделителем, а также являться обобщением атаки активным светоделителем. Предложенный способ требует изменения интенсивности достигающих Боба состояний, и чем больше эта интенсивность может варьироваться, тем эффективнее атака (т.е. тем меньше критическая ошибка). Мы рассмотрим применение этой атаки к протоколу B92 с интенсивным реперным состоянием, чья стойкость была доказана в [8].

2. Протокол B92 и описание основных способов атаки

Когерентное состояние $|\alpha\rangle$ выражается через комплексное число α как

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

где $|n\rangle$ – состояние Фока. Среднее число фотонов $\mu = |\alpha|^2$ называется интенсивностью когерентного состояния. Интенсивность на выходе канала длиной l может быть записана как

$$\mu' = \mu 10^{-\frac{\delta l}{10}}, \tag{2}$$

где $\delta \approx 0.2$ дБ/км – коэффициент затухания для оптоволокна. Протокол B92 с интенсивным реперным состоянием использует два неортогональных когерентных состояния, соответствующие сигналам 0 и 1:

$$\begin{aligned} &0\colon |A\rangle \otimes |\alpha\rangle, \\ &1\colon |A\rangle \otimes |-\alpha\rangle, \end{aligned} \tag{3}$$

где $|A| \gg |\alpha|$. Это кортежи из реперного и информационного состояний, каждое из которых локализовано в соответствующем временном окне; значение бита закодировано в разности фаз. Боб использует светоделитель с коэффициентом пропускания α/A, чтобы отделить часть реперного состояния той же интенсивности, что и информационное состояние. Остальная часть реперного состояния тоже измеряется, чтобы иметь возможность детектировать блокирование всего двухмодового состояния. После этого состояние переходит в следующее:

$$\begin{aligned} &0\colon |\alpha\rangle \otimes |\alpha\rangle, \\ &1\colon |\alpha\rangle \otimes |-\alpha\rangle. \end{aligned} \tag{4}$$

Боб использует интерферометр Маха–Цендера, чтобы преобразовать состояния в

$$\begin{aligned} &0\colon |0\rangle \otimes |\sqrt{2}\,\alpha\rangle, \\ &1\colon |\sqrt{2}\,\alpha\rangle \otimes |0\rangle, \end{aligned} \tag{5}$$

где $|0\rangle$ – вакуумное состояние. Затем измерение в каждой моде описывается наблюдаемой величиной

$$M_0 = |0\rangle\langle 0|, \quad M_1 = \sum_{i=1}^{+\infty} |i\rangle\langle i|, \tag{6}$$

где исход 0 означает отсутствие клика детектора, а исход 1 означает детектирование состояния. Вероятность детектирования состояния интенсивности μ равна $1 - \mathrm{e}^{-\mu}$, и она мала для состояний малой интенсивности.

Исход 1 в первой моде означает значение бита 0, исход 1 во второй моде означает 1, если же нигде не было исхода 1, Боб фиксирует неопределенный исход измерения. Чем длиннее линия, тем меньше интенсивность состояния на выходе и тем выше вероятность неопределенного исхода. После сеанса связи Алиса и Боб используют публичный аутентичный канал для того, чтобы отбросить позиции с неопределенными результатами.

Опишем две основные атаки на этот протокол. Фаза реперного состояния может быть легко измерена, поэтому мы предполагаем, что она известна Еве. Следовательно, основная задача Евы – извлечь информацию из двух состояний $|\alpha\rangle$ и $|-\alpha\rangle$ так, чтобы ее взаимная информация с Алисой равнялась взаимной информации Алисы и Боба, внеся при этом как можно меньшую ошибку. В обеих атаках Ева будет использовать затухание в канале.

Из теоремы Стайнспринга (см., напр., [1]) следует, что любое преобразование квантовой системы (т.е. кванто-

вый канал) может быть описано как унитарное взаимодействие системы и окружения. В ситуации атаки на протоколы квантовой криптографии Ева может владеть всем окружением. Атака с однозначным различением состояний может быть описана преобразованием

$$|\alpha\rangle \to |\psi_0\rangle = \sqrt{1-\mathrm{e}^{-2\mu}}\,|\beta\rangle|e_0\rangle + \mathrm{e}^{-\mu}|0\rangle|f\rangle,$$
$$|-\alpha\rangle \to |\psi_1\rangle = \sqrt{1-\mathrm{e}^{-2\mu}}\,|-\beta\rangle|e_1\rangle + \mathrm{e}^{-\mu}|0\rangle|f\rangle, \quad (7)$$

где $|\pm\beta\rangle$ – новые когерентные состояния Боба высокой интенсивности; $|e_0\rangle$, $|e_1\rangle$ и $|f\rangle$ – взаимно ортогональные состояния Евы. Легко убедиться, что условие унитарности выполнено: $\langle\psi_0|\psi_1\rangle = \mathrm{e}^{-2\mu} = \langle\alpha|-\alpha\rangle$. Вероятность успешного различения состояний равна $1-\mathrm{e}^{-2\mu}$, и Боб получает состояния

$$\rho_0^{\mathrm{B}} = \mathrm{Tr}_{\mathrm{E}}|\psi_0\rangle\langle\psi_0| = (1-\mathrm{e}^{-2\mu})|\beta\rangle\langle\beta| + \mathrm{e}^{-2\mu}|0\rangle\langle 0|,$$
$$\rho_1^{\mathrm{B}} = \mathrm{Tr}_{\mathrm{E}}|\psi_1\rangle\langle\psi_1| = (1-\mathrm{e}^{-2\mu})|-\beta\rangle\langle-\beta| + \mathrm{e}^{-2\mu}|0\rangle\langle 0|. \quad (8)$$

Ожидаемая вероятность определенного исхода Боба при измерении состояний (5) после канала с затуханием и интерферометра Маха–Цендера

$$1-\mathrm{e}^{-2\mu'}, \quad (9)$$

где μ' находится из (2). Для больших значений $|\beta|^2$ эта вероятность меньше, чем вероятность определенного исхода при измерении состояний (8):

$$(1-\mathrm{e}^{-2\mu})(1-\mathrm{e}^{-2|\beta|^2}). \quad (10)$$

Поэтому, производя эту атаку, Ева может установить интенсивность состояний $|\pm\beta\rangle$, получаемых Бобом, такой, чтобы вероятности (9) и (10) совпадали. Но, из-за наличия интенсивного реперного состояния, эта атака невозможна для протокола B92, т. к. Боб может детектировать ее из-за потерь реперного состояния. Для других протоколов эта атака может быть потенциально обнаружена по изменению интенсивности состояний Боба: от нуля до $|\beta|^2$. Ниже мы рассмотрим стратегию Евы, когда на состояния Боба накладываются некоторые ограничения.

При атаке светоделителем Ева разделяет каждое состояние на свою часть интенсивности $|\varepsilon|^2$ и часть Боба интенсивности μ'. Если в часть Боба вносится ошибка с вероятностью q, то преобразование записывается как

$$|\alpha\rangle \to |\varphi_0\rangle = (\sqrt{1-q}\,|\sqrt{\mu'}\rangle|g_0\rangle + \sqrt{q}\,|-\sqrt{\mu'}\rangle|g_1\rangle)|\varepsilon\rangle,$$
$$|-\alpha\rangle \to |\varphi_1\rangle = (\sqrt{q}\,|\sqrt{\mu'}\rangle|g_1\rangle + \sqrt{1-q}\,|-\sqrt{\mu'}\rangle|g_0\rangle)|-\varepsilon\rangle, \quad (11)$$

где $|g_0\rangle$ и $|g_1\rangle$ – взаимно ортогональные состояния, соответствующие информации Евы о том, была ли внесена ошибка на данной позиции или нет (они не дают Еве информации о значении бита); $|\pm\sqrt{\mu'}\rangle$ – когерентные состояния, достигающие Боба и имеющие интенсивность μ', вычисляемую из (2). Легко убедиться, что условие унитарности выполняется, если интенсивность состояний Евы $|\pm\varepsilon\rangle$ равна $\mu-\mu'$, что и достигается светоделителем.

При этом частичные состояния Боба

$$\rho_0^{\mathrm{B}} = \mathrm{Tr}_{\mathrm{E}}|\varphi_0\rangle\langle\varphi_0| = (1-q)|\sqrt{\mu'}\rangle\langle\sqrt{\mu'}| + q|-\sqrt{\mu'}\rangle\langle-\sqrt{\mu'}|,$$
$$\rho_1^{\mathrm{B}} = \mathrm{Tr}_{\mathrm{E}}|\varphi_1\rangle\langle\varphi_1| = q|\sqrt{\mu'}\rangle\langle\sqrt{\mu'}| + (1-q)|-\sqrt{\mu'}\rangle\langle-\sqrt{\mu'}|, \quad (12)$$

и их интенсивность в точности равна ожидаемому значению (2). Еве нужно внести ошибку, чтобы ее информация о состояниях Алисы стала такой же, как и информация Боба. Информация Евы дается величиной Холево χ состояний $|\pm\varepsilon\rangle$, поэтому необходимую вероятность ошибки можно найти из

$$1-h_2(q) = \chi(\{|\varepsilon\rangle,|-\varepsilon\rangle\}) = h_2\left[\frac{1-\mathrm{e}^{-2(\mu-\mu')}}{2}\right], \quad (13)$$

где $h_2(q) = -q\log q - (1-q)\log(1-q)$ – бинарная энтропия Шеннона. При длине канала, стремящейся к бесконечности (и, следовательно, высоком затухании), предельное значение критической ошибки задается как

$$1-h_2(q) = \chi(\{|\alpha\rangle,|-\alpha\rangle\}) = h_2\left(\frac{1-\mathrm{e}^{-2\mu}}{2}\right). \quad (14)$$

Следует отметить, что рассмотренная стратегия атаки светоделителем не оптимальна, т. к. Ева может провести более эффективное внесение ошибки при попытке получения дополнительной информации из ансамбля неортогональных состояний $|\pm\alpha\rangle$. Тем не менее, в случае большого затухания этот более сложный сценарий атаки не дает существенной выгоды. В настоящей работе рассматривается идея атаки с более простым внесением ошибки – добавлением шума.

Сравнивая эти два основных способа атаки, можно увидеть, что USD-атака может быть применена только если протокол позволяет изменять интенсивность от нуля до бесконечности, в то время как атака светоделителем может быть применена к любому протоколу на когерентных состояниях в условиях линии связи с потерями, однако ее критическая ошибка всегда больше нуля (и, более того, она превышает предельное значение, задаваемое (14)). USD-атака извлекает выгоду из возможности принимать решение, зависящее от успеха измерения.

3. Атака с флуктуациями интенсивности

Теперь предположим, что Боб может проверить интенсивность полученных состояний. Для протокола B92 с интенсивным реперным состоянием это может, например, означать, что Боб измеряет интенсивность реперного состояния и проверяет, лежит ли она внутри определенного диапазона. Поскольку интенсивности реперного и информационного состояний должны быть связаны между собой, Ева не может изменить одну из них, не внося дополнительной ошибки. Поэтому, измеряя интенсивность реперного состояния, Алиса и Боб могут также проверить интенсивность информационного состояния. Основной вопрос работы таков: если интенсивность информационного состояния может меняться от $\mu_{\min} < \mu'$ до $\mu_{\max} > \mu'$, как Ева может использовать это?

Перед описанием основной атаки рассмотрим операцию мягкой фильтрации, введенную в [9, 10]. Она в довольно общем виде извлекает информацию из неортого-

нальных состояний, и измерение с определенным исходом является ее частным случаем. Мягкая фильтрация действует на набор из двух когерентных состояний $|\pm\alpha\rangle$ как

$$|\alpha\rangle \to |\psi_0\rangle = \sqrt{p}\,|\beta\rangle|e\rangle + \sqrt{1-p}\,|0\rangle|f\rangle,$$
$$|-\alpha\rangle \to |\psi_1\rangle = \sqrt{p}\,|-\beta\rangle|e\rangle + \sqrt{1-p}\,|0\rangle|f\rangle. \quad (15)$$

В отличие от измерения с определенным исходом (7), состояния на выходе $|\pm\beta\rangle$ могут не быть ортогональными, а состояния Евы, отвечающие удачному исходу, совпадают: $|e_0\rangle = |e_1\rangle = |e\rangle$. Обозначим их интенсивность как $\mu_{\text{в}}$, тогда условие унитарности $\langle\alpha|-\alpha\rangle = \langle\psi_0|\psi_1\rangle$ записывается как

$$\mathrm{e}^{-2\mu} = p\mathrm{e}^{-2\mu_{\text{в}}} + 1 - p, \quad (16)$$

поэтому вероятность успеха

$$p = \frac{1-\mathrm{e}^{-2\mu}}{1-\mathrm{e}^{-2\mu_{\text{в}}}}. \quad (17)$$

Если выходные состояния ортогональны, вероятность успеха в точности такая же, как для измерения с определенным исходом (9). В этом случае состояния $|e_0\rangle$ и $|e_1\rangle$ также можно сделать ортогональными, так как это не влияет на условие унитарности. Но если состояния на выходе не ортогональны, вероятность успеха увеличивается, и она достигает единицы, если интенсивность на выходе такая же, как и на входе.

Мягкая фильтрация (будем в дальнейшем для краткости называть ее фильтрацией) делает состояния более различимыми с некоторой вероятностью p или выдает неопределенный исход с вероятностью $1-p$. Если фильтрация прошла успешно, можно извлечь больше информации из «более информативных» состояний $|\pm\beta\rangle$. Поэтому фильтрация является довольно общим случаем извлечения информации.

Теперь опишем основную атаку. Ее схема выглядит так:

1. Ева отводит себе часть каждого состояния на светоделителе.

2. Ева проводит мягкую фильтрацию над своей частью состояния.

3. В зависимости от успеха фильтрации Ева либо (в случае удачи) отправляет состояние высокой интенсивности с малой величиной ошибки Бобу, либо (в случае неудачной фильтрации) посылает состояние малой интенсивности с высокой вероятностью ошибки.

Эта атака применяется к протоколу на состояниях (4) интенсивности μ и использует два параметра: часть t состояния, к которой применяется фильтрация, и коэффициент усиления a. Сначала Ева отводит светоделителем часть состояния интенсивности $t\mu$ для извлечения информации; остальная часть интенсивности $(1-t)\mu$ на этом шаге остается неизменной. Выходная интенсивность для фильтрации равна $at\mu$, поэтому вероятность успеха

$$p = \frac{1-\mathrm{e}^{-2t\mu}}{1-\mathrm{e}^{-2at\mu}}.$$

В случае успеха Ева может извлечь много информации о значении бита, и для нее желательно послать Бобу состояние высокой интенсивности μ_1, чтобы он имел хорошие шансы получить определенный исход. Поскольку максимальная интенсивность состояний Боба ограничена $\mu_{\max}$, значение μ_1 не должно превышать $\min\{\mu_{\max}, (1-t)\mu\}$ (ниже будет рассмотрена модификация атаки, где также возможны состояния интенсивности выше $(1-t)\mu$). В этом случае Ева также забирает оставшуюся часть состояния и получает состояния интенсивности $at\mu + (1-t)\mu - \mu_1$, поэтому ее информация о ключе

$$I_{\text{AE}}^{\text{succ}} = h_2\left(\frac{1-\mathrm{e}^{-2[at\mu+(1-t)\mu-\mu_1]}}{2}\right).$$

В случае неудачной фильтрации Ева может получить мало информации о значении бита и использует светоделитель еще раз, чтобы отвести часть оставшегося состояния интенсивности $(1-t)\mu$. Тогда она посылает Бобу состояние малой интенсивности $\mu_2 \geqslant \mu_{\min}$. В этом случае информация Евы

$$I_{\text{AE}}^{\text{fail}} = h_2\left(\frac{1-\mathrm{e}^{-2[(1-t)\mu-\mu_2]}}{2}\right).$$

Интенсивности μ_1 и μ_2 также должны удовлетворять тому условию, что ожидаемое количество определенных исходов остается неизменным. Это в итоге дает три соотношения:

$$\mu_1 \leqslant \min\{\mu_{\max}, (1-t)\mu\},\ \ \mu_2 \geqslant \mu_{\min},$$
$$p(1-\mathrm{e}^{-2\mu_1}) + (1-p)(1-\mathrm{e}^{-2\mu_2}) = 1-\mathrm{e}^{-2\mu'}. \quad (18)$$

В зависимости от результата фильтрации Ева вносит ошибку в состояния Боба: величины q_1 и q_2 для успешной и неудачной фильтрации соответственно. Как и в атаке светоделителем, цель этой ошибки в том, чтобы сделать информацию Боба о ключе равной информации Евы. Вероятности ошибки задаются как

$$I_{\text{AE}}^{\text{succ}} = 1 - h_2(q_1),$$
$$I_{\text{AE}}^{\text{fail}} = 1 - h_2(q_2). \quad (19)$$

Состояния Боба после этой атаки

$$\rho_0^{\text{B}} = p[(1-q_1)\,|\sqrt{\mu_1}\rangle\langle\sqrt{\mu_1}\,| + q_1|-\sqrt{\mu_1}\rangle\langle-\sqrt{\mu_1}\,|]$$
$$+ (1-p)[(1-q_2)\,|\sqrt{\mu_2}\rangle\langle\sqrt{\mu_2}\,| + q_2|-\sqrt{\mu_2}\rangle\langle-\sqrt{\mu_2}\,|],$$
$$\rho_1^{\text{B}} = p[q_1\,|\sqrt{\mu_1}\rangle\langle\sqrt{\mu_1}\,| + (1-q_1)|-\sqrt{\mu_1}\rangle\langle-\sqrt{\mu_1}\,|]$$
$$+ (1-p)(q_2\,|\sqrt{\mu_2}\rangle\langle\sqrt{\mu_2}\,| + (1-q_2)|-\sqrt{\mu_2}\rangle\langle-\sqrt{\mu_2}\,|), \quad (20)$$

и ожидаемая им в среднем ошибка записывается как

$$q = q_1 p(1-\mathrm{e}^{-2\mu_1}) + q_2(1-p)(1-\mathrm{e}^{-2\mu_2}). \quad (21)$$

Задача Евы в подборе оптимальных параметров атаки t и a, чтобы ее информация сравнялась с информацией Боба при как можно меньшей средней ошибке (21); это обычная вычислительная задача.

4. Результаты для разных ограничений

Теперь посмотрим, как критическая ошибка изменяется для разных типов ограничений. Мы увидим, что чем жестче ограничения (т.е. чем ближе интенсивность Боба должна быть к ожидаемому значению), тем выше критическая ошибка и тем ближе она к критической ошибке при атаке светоделителем, которая подходит для ситуаций, когда флуктуации интенсивности невозможны вовсе.

Мы рассмотрим протокол с исходной интенсивностью состояний Алисы $\mu_A = 0.2$ фотона на импульс; интенсивность реперного состояния не играет роли. Также для простоты введем параметр s и рассмотрим следующие значения μ_{min} и μ_{max} (где μ' снова задается (2)):

$$\mu_{min} = (1-s)\mu', \qquad \mu_{max} = \frac{\mu'}{1-s}.$$

Случай $s = 0$ соответствует жестким ограничениям, когда возможна только атака светоделителем. В случае $s = 1$ интенсивность может принимать значения от нуля до бесконечности, и возможна атака измерением с определенным исходом.

Можно выделить три основных типа ограничений:

1. Обе интенсивности ограничены, т.е. интенсивность Боба μ_B должна быть между μ_{min} и μ_{max}.

2. Ограничение снизу, т.е. интенсивность Боба μ_B должна быть не меньше μ_{min}.

3. Ограничение сверху, т.е интенсивность Боба μ_B должна не превышать μ_{max}.

Критическая ошибка для двух значений параметра s при этих трех основных типах ограничений показана на рис.1 в зависимости от длины канала с параметром затухания $\delta = 0.2$ дБ/км. Эти значения ошибки сравниваются с ошибкой при атаке светоделителем, которая соответствует случаю $s = 0$.

Можно видеть, что если накладывается только верхнее ограничение $\mu_B \leqslant \mu'/(1-s)$, то для некоторых значений параметра s при атаке Ева может получить всю информацию, не внося ошибку, если длина канала достаточно велика. В этом случае Ева проводит измерение с определенным исходом над каждым состоянием интенсивности $\mu_A - \mu'/(1-s)$, блокирует состояние в случае неудачи, иначе же отправляет Бобу состояние наибольшей возможной интенсивности $\mu'/(1-s)$. Условие отсутствия ошибки при атаке записывается как

$$\left\{1 - \exp\left[-2\left(\mu_A - \frac{\mu'}{1-s}\right)\right]\right\} \times \left[1 - \exp\left(-2\frac{\mu'}{1-s}\right)\right] = 1 - e^{-2\mu'},$$

и можно видеть, что, если длина канала стремится к бесконечности, это условие принимает простой вид

$$s > e^{-2\mu_A}. \tag{22}$$

Важно отметить, что если это условие не выполнено или есть ограничение снизу $\mu_B \geqslant \mu_{min}$ для любого $\mu_{min} > 0$, то атака не может быть атакой с нулевой ошибкой. В самом деле, в этом случае Ева уже не может блокировать состояния, и для любого сообщения должна послать состояние Бобу, которое может быть задетектировано с ненулевой вероятностью. Максимальная информация, которую

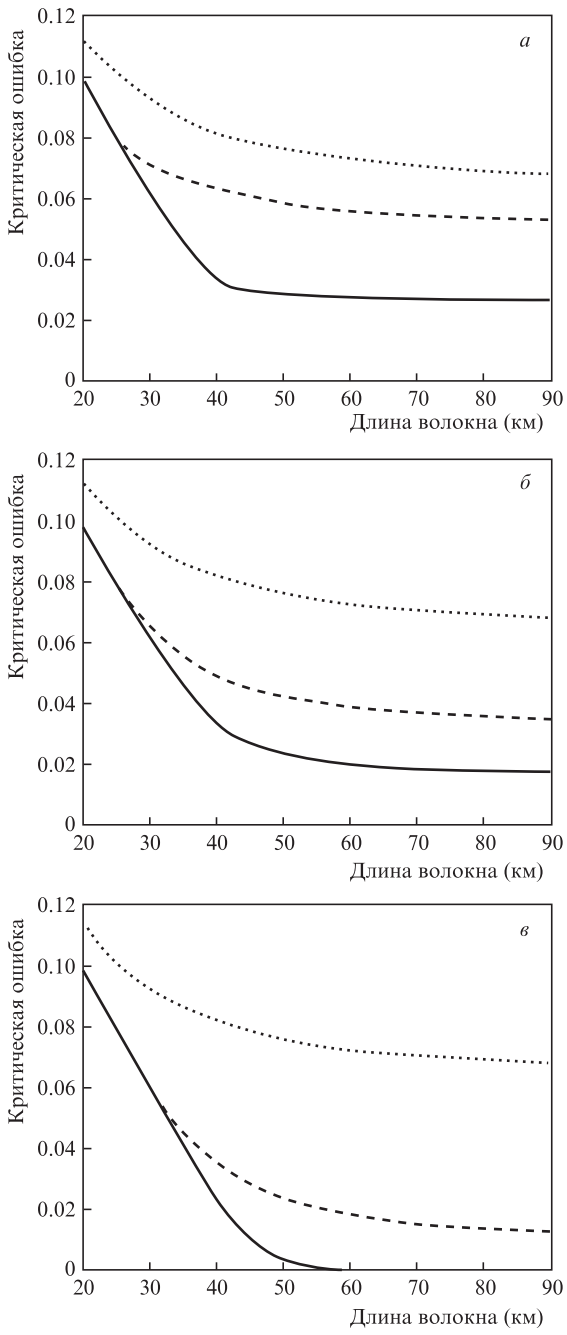

Рис.1. Зависимость критической ошибки от длины волокна в случае, когда интенсивность Боба должна удовлетворять условиям $(1-s)\mu' \leqslant \mu_B \leqslant \mu'/(1-s)$ (*а*), $\mu_B \geqslant (1-s)\mu'$ (*б*) и $\mu_B \leqslant \mu'/(1-s)$ (*в*) при $s = 0.5$ (штриховая линия) и 0.75 (сплошная линия). Пунктирной линией показан случай $s = 0$.

Ева может извлечь из состояний, ограничена величиной Холево, и наименьшая ошибка, которую Ева может внести в состояния малой интенсивности, дается (14). Поскольку Боб получает совместный исход с ненулевой вероятностью, он также получает ненулевую ошибку.

5. Выводы и обсуждение результатов

Атака светоделителем возможна для любой схемы квантового распределения ключей на когерентных состояниях в условиях затухания, т.к. действия Евы моделируют затухание идеальным образом. Мы рассмотрели атаку, которая возможна, если Ева может также слегка изме-

нять интенсивность состояний Боба. Вообще говоря, при такой атаке Ева получает выгоду от возможности принимать решения: Ева производит попытку извлечения информации и принимает решение о том, стоит ей посылать состояние высокой или низкой интенсивности.

Атака может быть улучшена использованием других методов внесения ошибок, особенно для случая небольшого затухания в канале. Мы рассмотрели простое внесение шума, но если Ева будет измерять некоторые состояния, она получит больше информации.

Другой возможной модификацией атаки в отсутствие ограничения сверху может быть использование состояний с интенсивностью, которая выше изначально используемой Алисой. Это возможно в случае успешной фильтрации. С этой точки зрения построенная атака является обобщением обеих атак: измерением с определенным исходом и атаки светоделителем.

Описанные выше улучшения и приложения этой атаки к другим известным протоколам являются темой для будущих исследований.

Этот способ атаки показывает необходимость контроля интенсивности со стороны Боба для противодействия подслушиванию. Если Алиса и Боб могут проверить, что интенсивность ограничена снизу (т.е. что Ева не блокирует состояния) или что наибольшее значение интенсивности меньше значения, даваемого (22), то такая атака не может дать Еве всю информацию без внесения ошибки. Более того, мы можем предположить, что условия подобного рода могут быть достаточными для секретности протоколов на когерентных состояниях против любой атаки в предположении, что Боб получает когерентные состояния и может проверить их интенсивность. Поэтому разработка протоколов, способных обеспечить контроль интенсивности на приемной стороне, является важной задачей.

Работа поддержана грантом Российского научного фонда (проект №17-11-01388) в Математическом институте им. В.А.Стеклова РАН.

1. Холево А.С. *Квантовые системы, каналы, информация* (М.: МЦНМО, 2010).
2. Dusek M., Jahma M., Lutkenhaus N. *Phys. Rev. A*, **62**, 022306 (1999).
3. Lo H.-K., Ma X., Chen K. *Phys. Rev. Lett*., **94**, 230504 (2005).
4. Stucki D., Brunner N., Gisin N., Scarani V., Zbinden H. *Appl. Phys. Lett*., **87**, 194108 (2005).
5. Inoue K., Waks E., Yamamoto Y. *Phys. Rev. Lett*., **89**, 037902 (2002).
6. Bennett C.H. *Phys. Rev. Lett*., **68**, 3121 (1992).
7. Кронберг Д.А., Киктенко Е.О., Федоров А.К., Курочкин Ю.В. *Квантовая электроника*, **47** (2), 163 (2017) [*Quantum Electron*., **47** (2), 163 (2017)].
8. Tamaki K., Lutkenhaus N., Koashi M., Batuwantudawe J. *Phys. Rev. A*, **80**, 032302 (2009).
9. Кронберг Д.А., Молотков С.Н. *Письма в ЖЭТФ*, **100**, 305 (2014) [*JETF Lett*., **100**, 279 (2014)].
10. Kronberg D.A. *Laser Phys.*, **24**, 025202 (2014).