Письма в ЖЭТФ, том 93, вып. 3, с. 194 – 201 © 2011 г. 10 февраля

Об уязвимости швейцарской системы когерентной квантовой криптографии по отношению к атаке с повторными измерениями

С. Н. Молотков

Институт физики твердого тела РАН, 142432 Черноголовка, Московская обл., Россия

Академия криптографии Российской Федерации, 121552 Москва, Россия

Факультет вычислительной математики и кибернетики, МГУ им. М.В. Ломоносова, 119899 Москва, Россия

Поступила в редакцию 22 декабря 2010 г.

Показано, что протокол когерентной квантовой криптографии (Coherent One Way) и, соответственно, оптоволоконные системы, использующие данный протокол квантового распределения ключей, являются уязвимыми по отношению к атаке с повторными измерениями и не гарантируют секретности передаваемых ключей в линии связи с потерями. Система когерентной квантовой криптографии используется в Швейцарии в качестве одной из линий распределения ключей в рамках европейского сетевого проекта SECOQC (SEcure COmmunications based on Quantum Cryptography). Критическая атака с повторными измерениями была пропущена при анализе криптографической стойкости данного протокола. Найдена критическая длина линии связи, при превышении которой заведомо невозможно передавать секретные ключи. Начиная с критической длины, подслушиватель знает весь передаваемый ключ, не производит ошибок на приемной стороне и остается необнаруживаемым. Для типичных значений параметров, имеющих место в реальной системе [6, 11] (среднее число фотонов $\mu = 0.5$, квантовая эффективность лавинных детекторов $\eta = 0.1$), секретность ключей нельзя гарантировать уже со сколь угодно малой длины линии связи.

Введение. Требования, предъявляемые к протоколам квантовой криптографии, сводятся, в основном, к следующему. Первое – система, использующая конкретный протокол, должна быть технологически реализуемой. Второе, и самое главное, – система должна гарантировать секретность передаваемых ключей на уровне фундаментальных законов природы, то есть быть неуязвимой для любого вида атак подслушивателя, который не ограничен никакими техническими или вычислительными возможностями.

Неидеальности аппаратуры при экспериментальной реализации оптоволоконных систем квантовой криптографии являются факторами, которые ограничивают дальность передачи ключей. Не строго однофотонный источник квантовых состояний, затухание (потери) в оптоволокне и темновые шумы лавинных детекторов приводят к тому, что невозможно гарантировать секретность передаваемых ключей, если длина линии связи (квантового канала) превышает некоторую критическую величину[1)] (см. один из последних обзоров [1]).

Потери в канале связи (даже при идеальных фотодетекторах) открывают возможность для PNS-атаки (Photon Number Splitting attack) [2]. Данная атака сводится к тому, что подслушиватель неразрушающим образом определяет число фотонов в каждой посылке, но не их состояние. Если обнаружен один фотон, то посылка блокируется. Если в канале присутствует два и более фотонов, то подслушиватель один фотон направляет на приемную сторону через свой канал с меньшими потерями (в пределе, вообще без потерь), а остальные оставляет у себя в квантовой памяти для последующих измерений. Например, для протокола BB84 после измерений на приемной стороне и раскрытия базисов легитимными пользователями подслушиватель делает измерения в уже известном базисе и достоверно определяет передаваемое квантовое состояние, соответственно, бит ключа в данной посылке. Поскольку в квантовой криптографии квантовый канал связи не контролируется, то на приемной стороне при наличии потерь в квантовом канале легитимные пользователи следят только за сохранением среднего числа посылок, достигающих приемной стороны. При заданной длине линии связи (соответственно потерях) подслушиватель может сохранить среднее число посылок, достигающих приемной стороны и не произвести ошибок. Таким образом, если потери таковы, что подслушиватель может

[1)] Напомним также, что квантовый канал связи в квантовой криптографии является не только открытым, но также доступным для любой модификации его подслушивателем. Вспомогательный классический канал также является открытым, но должен быть аутентичным.

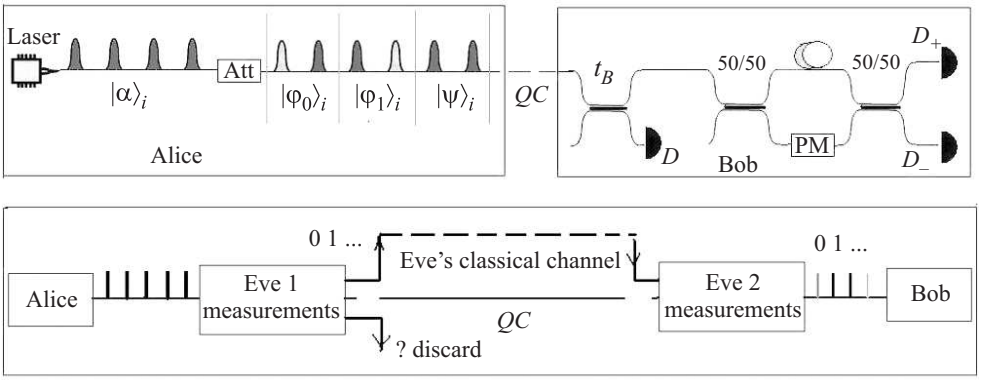

Рис.1. Верхняя половина – принципиальная схема оптоволоконной системы когерентной квантовой криптографии (Laser – лазер, работающий в режиме синхронизации мод (mode-locked), Att – управляемый аттенюатор, PM – фазовый модулятор, $D_\pm$, D – контрольные и информационные детекторы, QC – оптоволоконный квантовый канал связи). Нижняя половина – принципиальная схема атаки с повторными измерениями в квантовом канале с потерями. Как обычно, передающая сторона – Алиса, принимающая – Боб

блокировать все однофотонные посылки, то передача секретных ключей невозможна, поскольку из многофотонных посылок подслушиватель достоверно знает весь ключ и не производит ошибок на приемной стороне, то есть остается необнаруженным.

Для противодействия PNS атаке были предложены различные модификации протоколов квантовой криптографии. В протоколе с имитирующими состояниями (decoy state) [3] используются дополнительные по отношению к информационным контрольные состояния с разной интенсивностью. В протоколе SARG04 [4] состояния внутри базиса выбираются неортогональными, то есть достоверно неразличимыми даже при известном базисе. Оказалось, что протокол SARG04 теряет секретность, если затухание таково, что подслушиватель может блокировать все посылки, содержащие три и более фотонов. В протоколе с фазово-временным кодированием [5] возможна секретная передача ключей через канал с еще большими потерями, чем в протоколе SARG04, поскольку подслушиватель должен блокировать все посылки, содержащие пять фотонов и более.

Протокол когерентной квантовой криптографии (COW) [6]. Недавно была предложена новая система когерентной квантовой криптографии (Coherent One Way), рис.1, которая технологически достаточно проста и во многом близка к классическим оптоволоконным системам передачи данных. Для самодостаточности приведем краткое описание протокола, необходимое для дальнейшего. На передающей стороне используется лазер, работающий в режиме mode-locked, который выдает последовательность импульсов одинаковой интенсивности, разделенных одинаковым временным интервалом. *Все импульсы в разных посылках когерентны между собой*, то есть частотная "набивка" имеет одинаковую фазу (см. рис.1). С выхода лазера световые импульсы поступают на варьируемый аттенюатор, который либо блокирует, либо пропускает импульсы, в зависимости от того, какое состояние передается. Если передается логический 0, то первый импульс пустой (вакуумное состояние), а второй – когерентное состояние со средним числом фотонов μ. Квантовое состояние имеет вид $|\varphi_0\rangle_i = |vac\rangle \otimes |\alpha\rangle_i$, i – номер текущей посылки. Если передается логическая 1, то наоборот, первый импульс – когерентное состояние со средним числом фотонов μ, а второй – пустой, $|\varphi_1\rangle_i = |\alpha\rangle_i \otimes |\mathrm{vac}\rangle$. Вакуумное состояние и когерентное состояние $|\alpha\rangle$ неортогональны. При небольших $\mu = |\alpha|^2 < 1$ $\langle \mathrm{vac}|\alpha\rangle = e^{-\frac{\mu}{2}} \sim 1$. Неортогональность состояний гарантирует достоверную неразличимость всех трех состояний $|\varphi_0\rangle$, $|\varphi_1\rangle$ и $|\psi\rangle$. Принципиально важно для протокола, что не существует измерений, которые *с вероятностью единица* позволяют различать данные квантовые состояния.

Информационные состояния 0 и 1 посылаются в канал равновероятно, каждое с вероятностью $\frac{(1-f)}{2}$. С вероятностью f в канал посылаются контрольные состояния, представляющие пару непустых импульсов (рис.1) – $|\psi\rangle_i = |\alpha\rangle_i \otimes |\alpha\rangle_{i+1}$. Далее индекс посылки опускаем. Состояния через асимметричный светоделитель с коэффициентом деления t_B поступают либо на информационный детектор, либо на интерферометр Маха-Цандера (рис.1). На приемной стороне, кроме информационного детектора D, существуют два контрольных детектора D_+ и D_-. Из-за когерентности непустых импульсов в разных посылках при прохождении двух соседних им-

пульсов через интерферометр Маха-Цандера с разностью длин плеч, равной расстоянию между импульсами, на одном из детекторов, D_+, в соответствующем временном окне наблюдается конструктивная интерференция (отсчет в детекторе D_+), а во втором D_- – деструктивная интерференция – отсчеты отсутствуют. Вероятности отсчетов в двух детекторах соответственно равны $|\alpha_i \pm \alpha_{i+1}|^2/4$ (см. детали в [6]). Точное значение разности фаз между верхним и нижним плечами обеспечивается фазовым модулятором. Относительная разность фаз между плечами выбирается так, чтобы обеспечить конструктивную и деструктивную интерференции соседним импульсам в детекторах D_+ и D_-, соответственно. В отсутствие подслушивателя должна наблюдаться идеальная видность V интерференционной картины, $V = 100\%$.

Информационные состояния при наложении переднего и заднего импульсов не дадут идеальные конструктивную и деструктивную интерференции. Поэтому отсчеты от них будут наблюдаться в обоих детекторах.

Отсчеты в информационном детекторе в переднем или заднем временном окнах интерпретируются как 0 или 1. Отсчеты в переднем и заднем окнах могут иметь место как от информационных состояний, так и от контрольных. После передачи последовательности состояний легитимные пользователи раскрывают посылки, в которых посылались контрольные или информационные состояния (естественно, не раскрывается, какое информационное состояние 0 или 1 посылалось). Детектирование подслушивателя происходит по изменению видности интерференционной картины V и вероятности Q ошибки в информационной последовательности. У подслушивателя нет возможности *достоверно* отличить информационные состояния от контрольных. Поскольку в канале без потерь каждое посланное состояние должно достичь приемной стороны, то перепосылка состояний приведет к неизбежным ошибкам на приемной стороне.

Данная схема была реализована экспериментально и используется в Швейцарии в качестве одной из линий квантовой криптографии в рамках европейского сетевого проекта SECOQC (SEcure COmmunications based on Quantum Cryptography) [7]. Данный протокол является одним из претендентов на стандарт протокола для систем квантовой криптографии.

Общая идея атаки с повторными измерениями. Данный протокол передачи ключей является достаточно сложным для анализа. Криптографическая стойкость этого протокола исследовалась различными группами в серии работ [1, 6, 8 – 12].

Ниже будет показано, что при анализе протокола когерентной криптографии одна критическая атака на ключ была пропущена. Оказывается, что данный протокол и системы квантовой криптографии на его основе уязвимы по отношению к атаке с повторными измерениями[2)].

Идея атаки с повторными измерениями достаточно проста и может быть реализована экспериментально на сегодняшнем технологическом уровне, поскольку в отличие, например, от PNS атаки не требует квантовой памяти. Описание экспериментальной схемы измерений требует несколько большего места, поэтому имеет смысл изложить это отдельно.

Подслушиватель разрывает оптоволоконную линию связи вблизи приемной и передающей станций. Вблизи передающей станции проводит повторные измерения и сообщает их результат партнеру вблизи приемной станции по *обычному открытому классическому каналу связи*. Второй партнер, имея аппаратуру, аналогичную передающей станции, и используя сообщения от партнера, либо готовит свои квантовые состояния и посылает на приемную станцию, либо ничего не делает.

Первое преобразование-измерение позволяет различить (с некоторой вероятностью) пары состояний: $|\varphi_0\rangle$ и $|\psi\rangle$; $|\varphi_1\rangle$ и $|\psi\rangle$; $|\varphi_0\rangle$ и $|\varphi_1\rangle$. После первой стадии квантовые состояния переходят в новые.

Второе преобразование-измерение позволяет (с некоторой вероятностью) различить состояния внутри каждой пары – отличить $|\widetilde{\varphi_0}\rangle$ от $|\widetilde{\varphi_1}\rangle$, $|\widetilde{\varphi_0}\rangle$ от $|\widetilde{\psi}\rangle$, $|\widetilde{\varphi_1}\rangle$ от $|\widetilde{\psi}\rangle$. Естественно, из-за неортогональности состояний на каждом шаге возможны с некоторой вероятностью исходы измерений с неопределенным результатом (inconclusive). Данные исходы отбрасываются.

Если вероятность потерь в исходном квантовом канале связи (оптоволокне) равна или больше вероятности inconclusive исходов, то последние могут быть отброшены подслушивателем с сохранением среднего числа посылок, достигающих приемной стороны. В остальных посылках подслушиватель достоверно знает все передаваемые квантовые состояния, может их перепослать, не произвести ошибок на приемной стороне, то есть остаться недетектируемым.

Повторные преобразования-измерения. Согласно общей идеологии, любое допустимое преобразование квантовых состояний описывается квантовой

[2)] Аналогичный протокол (Differential Phase Shift Cryptography) был реализован японской группой [13, 14]. Данный протокол также уязвим по отношению к обсуждаемой атаке с повторными измерениями.

операцией (по другой терминологии – супероператором или инструментом [15, 16]) – линейным вполне положительным отображением, сохраняющим след и эрмитовость. Квантовая операция дает полное описание процесса преобразования и измерения квантового состояния [15, 16]. Квантовая операция и соответствующее ей разложение единицы на первом шаге имеют вид

$$\begin{gathered}\mathcal{E}_1(\rho) = \textstyle\sum_k M_k \rho M_k^+, \\ I = \textstyle\sum_k M_k^+ M_k, \\ k = \{\perp\varphi_0, \perp\varphi_1, \perp\psi, ?\},\end{gathered} \tag{1}$$

где индекс k нумерует "каналы" преобразования состояний, M_k – операторы Крауса [15]. После действия квантовой операции новое преобразованное квантовое состояние в k "канале" равно (с точностью до нормировки)

$$\widetilde{\rho}_k = M_k \rho M_k^+. \tag{2}$$

Если состояние после преобразования в k "канале" измеряется, то вероятность результата есть

$$\Pr(k|\rho) = \mathrm{Tr}\{M_k^+ M_k \rho\}. \tag{3}$$

Явный вид операторов в (1)–(3) на первом шаге преобразований следующий

$$\begin{aligned} M_{\perp\varphi_0} &= \frac{I - |\varphi_0\rangle\langle\varphi_0|}{\sqrt{2}}, \\ M_{\perp\varphi_1} &= \frac{I - |\varphi_1\rangle\langle\varphi_1|}{\sqrt{2}}, \\ M_{\perp\psi} &= \frac{I - |\psi\rangle\langle\psi|}{\sqrt{2}}, \end{aligned} \tag{4}$$

$$M_?^+ M_? = I - M_{\perp\varphi_0}^+ M_{\perp\varphi_0} - M_{\perp\varphi_1}^+ M_{\perp\varphi_1} - M_{\perp\psi}^+ M_{\perp\psi}. \tag{5}$$

Новые состояния в "каналах" $M_{\perp\varphi_0}$, $M_{\perp\varphi_1}$ и $M_{\perp\psi}$ подвергаются дальнейшим преобразованиям на втором шаге, а состояние в "канале" $M_?$ измеряется. Поскольку после измерений в "канале" ? состояния отбрасываются, то явный вид операторов $M_?$ нам не потребуется, так как для подсчета вероятности исхода ? достаточно знать только $M_?^+ M_?$. Операторы $M_{\perp\varphi_0}$, $M_{\perp\varphi_1}$ и $M_{\perp\psi}$ с точностью до нормировочного множителя представляют собой проекторы на направления, ортогональные, соответственно, $|\varphi_1\rangle$, $|\varphi_0\rangle$ и $|\psi\rangle$. Если бы состояния в этих каналах измерялись, то вероятности исходов первого измерения на входных состояниях $|\varphi_{0,1}\rangle$ и $|\psi\rangle$ были бы равны

$$\Pr(M_{\perp\varphi_0}||\varphi_0\rangle) = \Pr(M_{\perp\varphi_1}||\varphi_1\rangle) = \Pr(M_{\perp\psi}||\psi\rangle) \equiv 0, \tag{6}$$

$$\Pr(M_{\perp\varphi_0}||\varphi_1\rangle) = \Pr(M_{\perp\varphi_1}||\varphi_0\rangle) = \frac{1 - \langle\varphi_0|\varphi_1\rangle^2}{2}, \tag{7}$$

$$\begin{aligned} \Pr(M_?||\varphi_{0,1}\rangle) &= \frac{\langle\varphi_0|\varphi_1\rangle^2 + \langle\varphi_{0,1}|\psi\rangle^2}{2}, \\ \Pr(M_?||\psi\rangle) &= \frac{\langle\varphi_0|\psi\rangle^2 + \langle\varphi_1|\psi\rangle^2}{2}. \end{aligned} \tag{8}$$

Таким образом, из (6)–(8) следует, что в канале $M_{\perp\varphi_0}$ результат имеет место только либо от состояния $|\varphi_1\rangle$, либо от состояния $|\psi\rangle$ и никогда от состояния $|\varphi_0\rangle$. Аналогично, в канале измерений $M_{\perp\varphi_1}$ результат имеет место только от состояния $|\varphi_0\rangle$ либо от состояния $|\psi\rangle$, и никогда от состояния $|\varphi_1\rangle$. В канале $M_{\perp\psi}$ результат имеет место только либо от состояний $|\varphi_{0,1}\rangle$ и никогда от состояния $|\psi\rangle$. Исход измерений в канале $M_?$ имеет место от всех трех состояний. Данные исходы отбрасываются.

Первая стадия разделяет пары состояний. На выходе каналов $M_{\perp\varphi_{0,1}}$ и $M_{\perp\psi}$ состояния не измеряются, а подвергаются дальнейшим преобразованиям. Для наглядности удобно изобразить последовательные преобразования-измерения по разделению состояний при помощи диаграммы рис.2. После первой

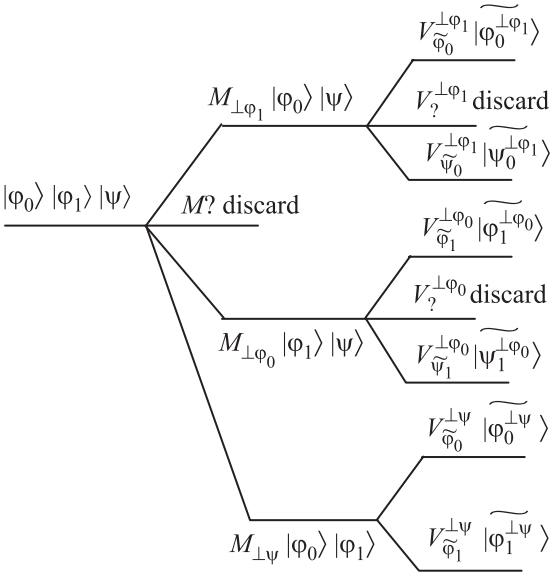

Рис.2. Схематическое представление двух последовательных преобразований-измерений

стадии в канале $M_{\perp\varphi_0}$ новые состояния (пока не нормированные), с учетом (4), имеют вид

$$\begin{aligned} |\overline{\varphi_1^{\perp\varphi_0}}\rangle &= M_{\perp\varphi_0}|\varphi_1\rangle = \frac{|\varphi_1\rangle - \langle\varphi_0|\varphi_1\rangle|\varphi_0\rangle}{\sqrt{2}}, \\ |\overline{\psi_1^{\perp\varphi_0}}\rangle &= M_{\perp\varphi_0}|\psi\rangle = \frac{|\psi\rangle - \langle\varphi_0|\psi\rangle|\varphi_0\rangle}{\sqrt{2}}, \end{aligned} \tag{9}$$

в канале $M_{\perp\varphi_1}$ имеем

$$|\overline{\varphi_0^{\perp\varphi_1}}\rangle = M_{\perp\varphi_1}|\varphi_0\rangle = \frac{|\varphi_0\rangle - \langle\varphi_0|\varphi_1\rangle|\varphi_1\rangle}{\sqrt{2}},$$
$$|\overline{\psi_0^{\perp\varphi_1}}\rangle = M_{\perp\varphi_1}|\psi\rangle = \frac{|\psi\rangle - \langle\varphi_1|\psi\rangle|\varphi_1\rangle}{\sqrt{2}}, \tag{10}$$

соответственно, в канале $M_{\perp\psi}$ имеем

$$|\overline{\varphi_0^{\perp\psi}}\rangle = M_{\perp\psi}|\varphi_0\rangle = \frac{|\varphi_0\rangle - \langle\varphi_0|\psi\rangle|\psi\rangle}{\sqrt{2}},$$
$$|\overline{\varphi_1^{\perp\psi}}\rangle = M_{\perp\psi}|\varphi_1\rangle = \frac{|\varphi_1\rangle - \langle\varphi_1|\psi\rangle|\psi\rangle}{\sqrt{2}}. \tag{11}$$

На втором шаге используются две разные квантовые операции на выходе каждого "канала" после первого преобразования-измерения. Имеем

$$\mathcal{E}_2^j(\rho_i) = \sum_k V_k^j \rho_i V_k^{j+}, \quad I = \sum_k V_k^{j+} V_k^j,$$
$$k = \{\widetilde{\varphi_{0,1}^{\perp\varphi_{1,0},\perp\psi}}, \widetilde{\psi_{0,1}^{\perp\varphi_{1,0},\perp\psi}}, ?\}; \tag{12}$$

здесь j – индекс канала первой стадии преобразования, $j = \{\perp\varphi_0, \perp\varphi_1, \perp\psi, ?\}$. Явный вид операторов следующий:

$$V_{\widetilde{\varphi_0}}^{\perp\psi} = |\widetilde{\varphi_0^{\perp\psi}}\rangle\langle\widetilde{\varphi_0^{\perp\psi}}|, \quad V_{\widetilde{\varphi_1}}^{\perp\psi} = |\widetilde{\varphi_1^{\perp\psi}}\rangle\langle\widetilde{\varphi_1^{\perp\psi}}|,$$
$$|\widetilde{\varphi_{0,1}^{\perp\psi}}\rangle = |\overline{\varphi_{0,1}^{\perp\psi}}\rangle / \sqrt{\langle\overline{\varphi_{0,1}^{\perp\psi}}|\overline{\varphi_{0,1}^{\perp\psi}}\rangle}. \tag{13}$$

Обратим внимание на то, что состояния после канала $M_{\perp\psi}$ в (11) оказываются ортогональными (поскольку $\langle\varphi_0|\psi\rangle = \langle\varphi_1|\psi\rangle$), поэтому новые состояния достоверно различимы, и исходы с неопределенным результатом (?) отсутствуют. Приведем явный вид операторов в (12)[3]:

$$V_{\widetilde{\varphi_1}}^{\perp\varphi_0} = \frac{I - |\widetilde{\psi_1^{\perp\varphi_0}}\rangle\langle\widetilde{\psi_1^{\perp\varphi_0}}|}{\sqrt{1 + \langle\widetilde{\psi_1^{\perp\varphi_0}}|\widetilde{\varphi_1^{\perp\varphi_0}}\rangle}},$$
$$V_{\widetilde{\psi_1}}^{\perp\varphi_0} = \frac{I - |\widetilde{\varphi_1^{\perp\varphi_0}}\rangle\langle\widetilde{\varphi_1^{\perp\varphi_0}}|}{\sqrt{1 + \langle\widetilde{\psi_1^{\perp\varphi_0}}|\widetilde{\varphi_1^{\perp\varphi_0}}\rangle}}, \tag{14}$$

$$V_{\widetilde{\varphi_0}}^{\perp\varphi_1} = \frac{I - |\widetilde{\psi_0^{\perp\varphi_1}}\rangle\langle\widetilde{\psi_0^{\perp\varphi_1}}|}{\sqrt{1 + \langle\widetilde{\psi_0^{\perp\varphi_1}}|\widetilde{\varphi_0^{\perp\varphi_1}}\rangle}},$$
$$V_{\widetilde{\psi_0}}^{\perp\varphi_1} = \frac{I - |\widetilde{\varphi_0^{\perp\varphi_1}}\rangle\langle\widetilde{\varphi_0^{\perp\varphi_1}}|}{\sqrt{1 + \langle\widetilde{\psi_0^{\perp\varphi_1}}|\widetilde{\varphi_0^{\perp\varphi_1}}\rangle}}, \tag{15}$$

в формулах (13)–(15) состояния

$$|\widetilde{\psi_1^{\perp\varphi_0}}\rangle = \frac{|\overline{\psi_1^{\perp\varphi_0}}\rangle}{\sqrt{\langle\overline{\psi_1^{\perp\varphi_0}}|\overline{\psi_1^{\perp\varphi_0}}\rangle}},$$
$$|\widetilde{\varphi_1^{\perp\varphi_0}}\rangle = \frac{|\overline{\varphi_1^{\perp\varphi_0}}\rangle}{\sqrt{\langle\overline{\varphi_1^{\perp\varphi_0}}|\overline{\varphi_1^{\perp\varphi_0}}\rangle}}, \tag{16}$$

$$|\widetilde{\psi_0^{\perp\varphi_0}}\rangle = \frac{|\overline{\psi_1^{\perp\varphi_0}}\rangle}{\sqrt{\langle\overline{\psi_0^{\perp\varphi_0}}|\overline{\psi_0^{\perp\varphi_0}}\rangle}},$$
$$|\widetilde{\varphi_0^{\perp\varphi_0}}\rangle = \frac{|\overline{\varphi_1^{\perp\varphi_0}}\rangle}{\sqrt{\langle\overline{\varphi_0^{\perp\varphi_0}}|\overline{\varphi_0^{\perp\varphi_0}}\rangle}}, \tag{17}$$

и

$$V_?^{+\perp\varphi_0} V_?^{\perp\varphi_0} = I - V_{\widetilde{\varphi_1}}^{+\perp\varphi_0} V_{\widetilde{\varphi_1}}^{\perp\varphi_0} - V_{\widetilde{\psi_1}}^{+\perp\varphi_0} V_{\widetilde{\psi_1}}^{\perp\varphi_0}, \tag{18}$$

$$V_?^{+\perp\varphi_1} V_?^{\perp\varphi_1} = I - V_{\widetilde{\varphi_0}}^{+\perp\varphi_1} V_{\widetilde{\varphi_0}}^{\perp\varphi_1} - V_{\widetilde{\psi_0}}^{+\perp\varphi_1} V_{\widetilde{\psi_0}}^{\perp\varphi_1}. \tag{19}$$

Для вычисления критической длины линии связи, до которой можно передавать секретные ключи, необходимо знать суммарную вероятность исходов с неопределенным результатом. Информационные состояния, отвечающие 0 и 1, посылаются в канал с вероятностями $(1-f)/2$, контрольные состояния – с вероятностью f. Матрица плотности квантового ансамбля равна

$$\rho = \frac{(1-f)}{2}(|\varphi_0\rangle\langle\varphi_0|+)|\varphi_1\rangle\langle\varphi_1|) + f|\psi\rangle\langle\psi|. \tag{20}$$

Вероятность неопределенного исхода на первой стадии, с учетом (14)–(19), равна

$$\Pr(M_?|\rho) = \mathrm{Tr}\{M_?^+ M_? \rho\} = \frac{(1-f)}{2} \times$$
$$\times \left(\frac{\langle\varphi_0|\varphi_1\rangle^2 + \langle\varphi_0|\psi\rangle^2 + \langle\varphi_0|\varphi_1\rangle^2 + \langle\varphi_1|\psi\rangle^2}{2}\right) +$$
$$+ f\left(\frac{\langle\varphi_0|\psi\rangle^2 + \langle\varphi_1|\psi\rangle^2}{2}\right) =$$
$$= \frac{(1-f)}{2}(e^{-\mu} + e^{-2\mu}) + fe^{-\mu}. \tag{21}$$

[3] Заметим, что первый и второй шаги преобразования-измерения аналогичны измерениям с тремя исходами (двумя достоверными и одним с неопределенным исходом), используемыми ранее при различении пары неортогональных состояний (см. [17]). Здесь же отметим, что протокол B92 не обеспечивает секретности в канале с потерями, если его длина превышает критическую величину. Данная длина определяется из условия равенства вероятности потерь в канале связи и вероятности inconclusive исходов.

Вероятности неопределенных исходов после второй стадии, с учетом (14–19), имеют вид

$$\begin{aligned}\Pr(V_?^{\perp\varphi_0}M^{\perp\varphi_0}|\rho) = \\ = \mathrm{Tr}\{V_?^{\perp\varphi_0}M^{\perp\varphi_0}\rho M^{+\perp\varphi_0}V_?^{+\perp\varphi_0}\} = \\ = \frac{(1-f)}{2}\langle\overline{\varphi_0^{\perp\varphi_0}}|\overline{\varphi_0^{\perp\varphi_0}}\rangle\langle\widetilde{\varphi_0^{\perp\varphi_0}}|\widetilde{\psi_0^{\perp\varphi_0}}\rangle + \\ + f\langle\overline{\psi_0^{\perp\varphi_0}}|\overline{\psi_0^{\perp\varphi_0}}\rangle\langle\widetilde{\varphi_0^{\perp\varphi_0}}|\widetilde{\psi_0^{\perp\varphi_0}}\rangle,\end{aligned} \tag{22}$$

$$\begin{aligned}\Pr(V_?^{\perp\varphi_1}M^{\perp\varphi_1}|\rho) = \\ = \mathrm{Tr}\{V_?^{\perp\varphi_1}M^{\perp\varphi_1}\rho M^{+\perp\varphi_1}V_?^{+\perp\varphi_1} = \\ = \frac{(1-f)}{2}\langle\overline{\varphi_1^{\perp\varphi_1}}|\overline{\varphi_1^{\perp\varphi_1}}\rangle\langle\widetilde{\varphi_1^{\perp\varphi_1}}|\widetilde{\psi_1^{\perp\varphi_1}}\rangle + \\ + f\langle\overline{\psi_1^{\perp\varphi_1}}|\overline{\psi_1^{\perp\varphi_1}}\rangle\langle\widetilde{\varphi_1^{\perp\varphi_1}}|\widetilde{\psi_1^{\perp\varphi_1}}\rangle.\end{aligned} \tag{23}$$

Суммарная вероятность неопределенных исходов после второго шага преобразований равна

$$\Pr(V_?^{\perp\varphi_0}M^{\perp\varphi_0}|\rho) + \Pr(V_?^{\perp\varphi_1}M^{\perp\varphi_1}|\rho) = \tag{24}$$

$$= \frac{(1-f)}{2}e^{-\frac{\mu}{2}}\sqrt{1-e^{-2\mu}}\sqrt{1-e^{-\mu}} + fe^{-\frac{\mu}{2}}\frac{1-e^{-\mu}}{\sqrt{1+e^{-\mu}}}.$$

Таким образом, полная вероятность inconclusive исходов от информационных состояний, нормированная на долю $(1-f)$ таких состояний, есть

$$\Pr(?|\mathrm{info}) = \frac{e^{-\mu}+e^{-2\mu}}{2} + e^{-\frac{\mu}{2}}\sqrt{1-e^{-2\mu}}\sqrt{1-e^{-\mu}}, \tag{25}$$

соответственно, полная вероятность inconclusive исходов от контрольных состояний, нормированная на долю f таких состояний, равна

$$\Pr(?|\mathrm{control}) = e^{-\mu} + e^{-\frac{\mu}{2}}\frac{1-e^{-\mu}}{\sqrt{1+e^{-\mu}}}. \tag{26}$$

Критическая длина линии связи. Если было послано N посылок, то при прохождении через канал с потерями будет зарегистрировано не более

$$N_{\mathrm{loss}}(L) = N\cdot\Pr(\mathrm{loss}|L) \tag{27}$$

посылок. Здесь $\Pr(\mathrm{loss}|L)$ – вероятность регистрации когерентного состояния со средним числом фотонов $\mu = |\alpha|^2$ при прохождении через канал длиной L с потерями δ (см. детали в [6], для одномодового оптоволокна $\delta = 0.2$ db/km),

$$\Pr(\mathrm{loss}|L) = 1 - e^{-\mu\cdot\eta\cdot T(L)}, \quad T(L) = 10^{-\frac{\delta L}{10}}, \tag{28}$$

где η – квантовая эффективность детектора (типичное значение для лавинных детекторов на основе InGaAs:P на длине волны 1.5 мкм составляет $\eta = 0.1 \div 0.25$ при уровне темновых шумов $P_{\mathrm{dark}} \approx \approx 10^{-5}$ counts/gate). Формула (28) отражает тот факт, что детектор не реагирует на вакуумную компоненту когерентного состояния и дает максимум вероятности того, что детектор зарегистрирует вообще что-либо.

Число достоверно известных подслушивателю информационных и контрольных посылок равно

$$\begin{aligned}N_{\mathrm{info}} &= N(1-f)(1-\Pr(?|\mathrm{info})), \\ N_{\mathrm{control}} &= Nf(1-\Pr(?|\mathrm{control})).\end{aligned} \tag{29}$$

Когда число посылок, которые должны быть зарегистрированы на приемной стороне при прохождении через канал с потерями, становится равным числу посылок, которые известны Еве достоверно, то передача секретных ключей становится невозможной.

Подслушиватель разрывает линию связи вблизи передающей и приемной стороны, как это было описано во Введении, проводит "на ходу" повторные измерения, отбрасывает исходы с неопределенным результатом, в остальных посылках подслушиватель знает достоверно все передаваемые состояния. Результаты измерений "на ходу" *по классическому* каналу связи сообщаются партнеру вблизи приемной станции. По этим сообщениям вблизи приемной станции приготавливаются квантовые состояния, которые направляются по исходной линии связи на приемную сторону.

Подслушиватель вблизи приемной стороны может приготовить когерентные состояния с правильной структурой и с таким $\mu^* \gg 1$, чтобы каждая перепосланная им посылка была зарегистрирована. Для этого нужно выбрать такую интенсивность, соответственно, среднее число фотонов в импульсе, чтобы было $\mu^*\cdot\eta \gg 1$. При типичных значениях квантовой эффективности $\eta \approx 0.1$ достаточно иметь среднее число фотонов в импульсе $\mu^* \approx 100$, при этом вероятность регистрации таких состояний легитимным пользователем на приемной стороне будет $1 - e^{-\mu^*\cdot\eta} = 1 - e^{-10} \approx 1$. Ева для достоверно известных посылок сохраняет правильную пропорцию между информационными и контрольными состояниями.

Таким образом, критическая длина линии связи, начиная с которой подслушиватель знает все информационные и контрольные состояния, определяется, с учетом (27)–(29), из равенств

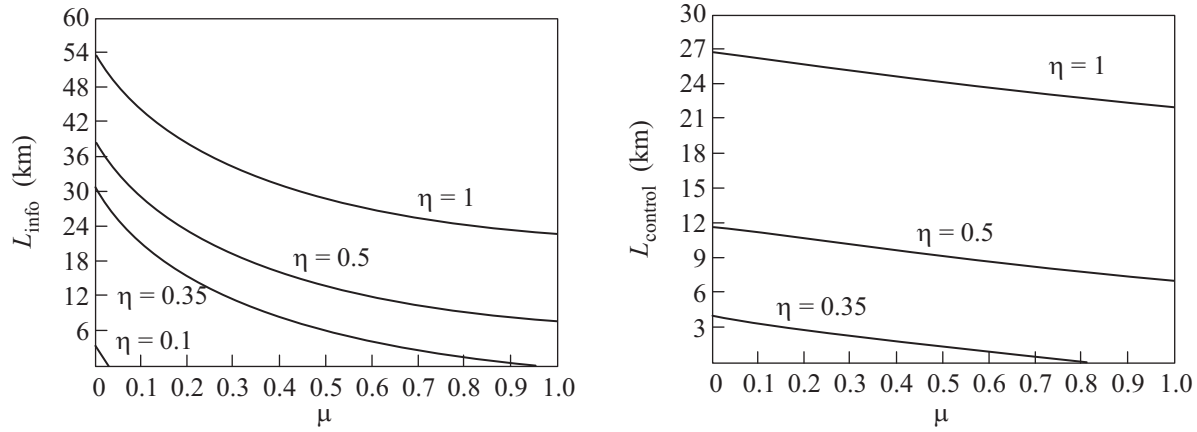

Рис.3. Зависимость критической длины канала связи как функция среднего числа фотонов при различных значениях квантовой эффективности фотодетекторов

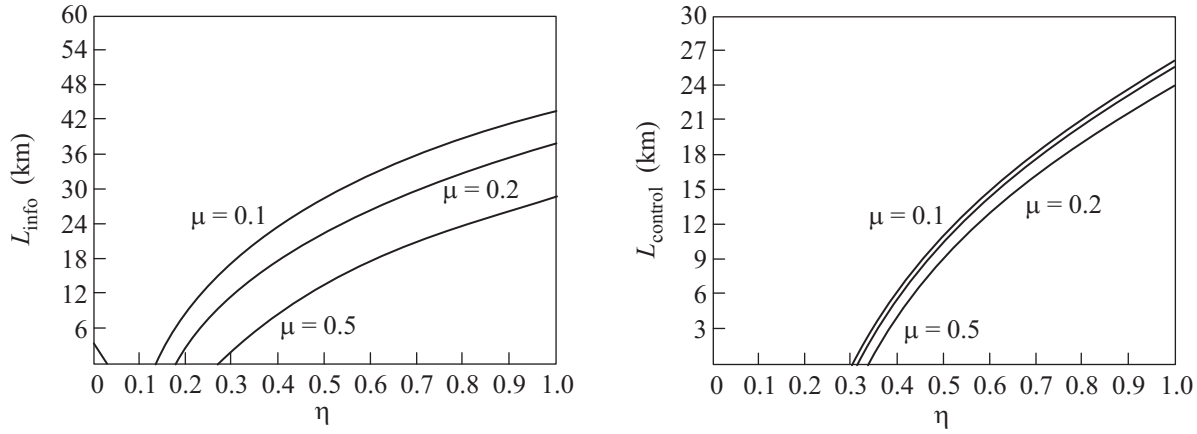

Рис.4. Зависимость критической длины канала связи как функция квантовой эффективности фотодетекторов при различных значениях среднего числа фотонов

$$L_{\text{info}} = -\frac{10}{\delta}\log\left(-\frac{1}{\mu\cdot\eta}\ln\left(\Pr(?|\text{info})\right)\right),$$
$$L_{\text{control}} = -\frac{10}{\delta}\log\left(-\frac{1}{\mu\cdot\eta}\ln\left(\Pr(?|\text{control})\right)\right). \tag{30}$$

Критическая длина линии связи, до которой можно передавать ключи и гарантировать их секретность, определяется наибольшей из длин L_{info} и L_{control}. При больших длинах подслушиватель достоверно знает все передаваемые состояния и не производит ошибок, сохраняет среднее число посылок и идеальную видность интерференции на приемной стороне, то есть остается недетектируемым.

При реальных значениях параметров, используемых в системе [6, 11] ($\mu = 0.5$ и $\eta = 10\%$), протокол оказывается несекретным уже при сколь угодно малой длине линии связи (см. левую часть рис.3, 4). Длина волоконно-оптической линии связи между Женевой и Нашатель (Geneva, Neuchatel) составляет ≈ 110 км. Длина оптоволокна при этом 150 км.

В заключение отметим, что в отличие от PNS атаки, для которой требуется пока не созданная квантовая память, данная атака технически реализуема даже на сегодняшнем уровне технологий. Как всегда отмечалось (см. [6, 8–12]), отличительной особенностью данного протокола является когерентность состояний в различных посылках. Именно на это свойство возлагались надежны на устойчивость данного протокола относительно PNS атаки при больших длинах линии связи. Для атаки с повторными измерениями факт когерентности состояний в различных посылках не играет никакой роли.

Выше не учитывались темновые отсчеты лавинных детекторов на приемной стороне. Учет темновых шумов еще больше ухудшит ситуацию для легитимных пользователей.

Выражаю благодарность коллегам по Академии криптографии Российской Федерации за постоянную поддержку. Работа частично поддержана проектом Российского фонда фундаментальных исследований # 11-02-00455.

1. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf et al., Rev. Mod. Phys. **81**, 1301 (2009).
2. G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
3. W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
4. V. Scarani, A. Acэin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **95**, 057901-1 (2004); A. Acin, N. Gisin, and V. Scarani, arXiv:quant-ph/0302037.
5. Д. А. Кронберг, С. Н. Молотков, ЖЭТФ, **136**, 650 (2009).
6. N. Gisin, G. Ribordy, H. Zbinden et al., arXiv:quant-ph/0411022.
7. SECOQC, arXiv:quant-ph/0701168.
8. D. Stucki, N. Brunner, N. Gisin et al, arXiv:quant-ph/0506097.
9. C. Branciard, N. Gisin, N. Lütkenhaus, and V.Scarani, arXiv:quant-ph/0609090.
10. C. Branciard, N. Gisin, and V. Scarani, arXiv:quant-ph/0710.4884.v2.
11. D. Stucki, C. Barreiro, S. Fasel et al., arXiv:quant-ph/08095264.
12. M. Curty, L.-L. Zhang, H.-K. Lo, and N. Lütkenhaus, arXiv:quant-ph/0609094.
13. K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002); K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. A **68**, 022317 (2003).
14. H. Takesue, S. W. Nam, Q. Zhang et al., Nature Photonics **1**, 343 (2007).
15. K. Kraus, *States, Effects and Operations*, Springer-Verlag, Berlin, 1983.
16. M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2001. М. Нильсен, И. Чанг, *Квантовые вычисления и квантовая информация*, М.: Мир, 2006.
17. A. Peres, *Quantum Theory: Concepts and Methods*, Kluwer Academic Publishers, The Netherlands, 1995.