Письма в ЖЭТФ, том 93, вып. 12, с. 830 – 836 © 2011 г. 25 июня

О решении проблемы обеспечения стойкости квантовой криптографии для канала связи со сколь угодно большой длиной

С. Н. Молотков

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

Академия криптографии Российской Федерации

Факультет вычислительной математики и кибернетики, МГУ им. М.В. Ломоносова, 119992 Москва, Россия

Поступила в редакцию 29 апреля 2011 г.

В квантовой криптографии имеется принципиальный вопрос о существовании стойких протоколов квантового распределения ключей при любой длине (любых потерях) в линии связи. Принципиальной особенностью и новизной нашего протокола является то, что имеет место двойной контроль: 1) перед сравнением (измерением) когерентных состояний из разных временных окон производится контроль интенсивности реперного (интенсивного) квантового состояния *классическим образом*; 2) нарушение когерентности состояния детектируется интерференционными измерениями информационного квантового состояния и проверенного на сохранение интенсивности реперного квантового состояния. Таким образом, данный протокол на сегодняшний день является единственным протоколом, устойчивым относительно любых потерь в линии связи. Единственным фактором, ограничивающим дальность, являются темновые шумы детекторов.

Введение. Безусловная секретность[1)] ключей в квантовой криптографии основана на фундаментальных запретах квантовой механики [1, 2]: 1) запрете копирования (клонирования) неизвестного квантового состояния; 2) невозможности достоверного различения неортогональных квантовых состояний [2]. Фактически данные запреты являются следствием простого математического факта – некоммутирующие эрмитовы операторы (наблюдаемые) не могут иметь общей системы собственных векторов[2)].

Для квантовой криптографии важно следующее: получение информации о квантовых состояниях из неортогонального набора неизбежно приводит к их возмущению [2]. Важно отметить, что нет никаких формальных ограничений на структуру квантовых состояний. Например, квантовые состояния не обязаны быть строго однофотонными.

Если квантовые состояния, отвечающие битам ключа, передаются через квантовый канал связи без потерь, *то каждое состояние, посланное с передающей стороны, должно достигать приемной станции независимо от того, было или не было данное состояние возмущено подслушивателем.* При этом измерения на приемной стороне должны быть устроены таким образом, чтобы они могли регистрировать *любые* изменения квантовых состояний. Иначе говоря, любое получение информации подслушивателем о ключе неизбежно ведет к ошибкам на приемной стороне, по которым обнаруживается подслушиватель.

Ситуация радикально меняется, когда из-за потерь в канале связи часть посылок не достигает приемной стороны. Это открывает возможность для новых атак подслушивателя, при которых подслушиватель знает весь ключ, не производит ошибок на приемной стороне и остается недетектируемым. Таким образом, начиная с некоторой величины потерь (длины линии связи), невозможно гарантировать секретность ключей.

Отметим, что в канале с потерями структура квантового состояния (строгая однофотонность или не однофотонность) оказывается принципиально важной для секретности протокола.

Критическими атаками являются PNS-атака (Photon Number Splitting) [3] и атака с измерениями с определенным исходом (Unambigious Measurements) [4–9]. Для противодействия PNS-атаке в протоколах с несколькими базисами [10] достаточно использовать неортогональные состояния внутри базиса [11–13]. Однако при этом все равно остается возможность для UM-атаки. Она фактически и ограничивает длину линии, на которую можно

[1)] Секретность, основанную на фундаментальных законах природы, принято называть безусловной (*unconditional*), в отличие от секретности, основанной либо на недоказанной вычислительной сложности, либо на каких-то других предположениях о технических и вычислительных ограничениях подслушивателя.

[2)] Соотношения неопределенностей Гайзенберга также являются следствием этого факта.

передавать ключи и гарантировать их секретность [11–13].

Было предложено множество различных протоколов квантового распределения ключей для увеличения дальности передачи через канал с потерями [11–25]. Однако на сегодняшний день дальность передачи ключей во всех известных протоколах квантовой криптографии и системах на их основе ограничена некоторой критической длиной. При этом критическая длина принципиально конечна[3)].

Имеется фундаментальный для квантовой криптографии вопрос. *Существуют ли в принципе протоколы квантового распределения ключей в канале с потерями, которые гарантируют секретность ключей при любой длине (любых потерях) линии связи? Иначе говоря, достаточно ли фундаментальных запретов квантовой механики на различимость неортогональных квантовых состояний (см. выше) для существования упомянутых протоколов, или данных запретов принципиально недостаточно*, т.е. ограничения по дальности передачи ключей являются принципиальными или, они связаны лишь с ограничениями современного технологического уровня? Кроме того, хотелось бы иметь протоколы квантового распределения ключей на любые расстояния, реализуемых на сегодняшнем технологическом уровне, в случае не строго однофотонных источников, детекторов, которые не различают число фотонов и не реагируют на вакуумную компоненту в квантовом состоянии.

Измерения с определенным исходом. Вкратце UM-атака сводится к следующему. Пусть имеется набор неортогональных состояний $\{|\varphi_i\rangle\}$. Тогда существуют (unambigious) измерения [4–9], которые описываются разложением единицы:

$$I = \sum_i \mathcal{M}_i + \mathcal{M}_?, \tag{1}$$

где $\mathcal{M}_i$ и $\mathcal{M}_?$ – операторнозначные меры. Вероятности исходов на входном состоянии $|\varphi_i\rangle$ равны

$$\begin{aligned} \Pr(i|j) &= \mathrm{Tr}\{\mathcal{M}_j|\varphi_i\rangle\langle\varphi_i|\} \propto \delta_{i,j}, \\ \Pr(?|i) &= \mathrm{Tr}\{\mathcal{M}_\perp|\varphi_i\rangle\langle\varphi_i|\} \neq 0. \end{aligned} \tag{2}$$

Если входным состоянием было $|\varphi_i\rangle$, то исход измерений может быть либо в канале измерения i (определенный исход, в этом случае состояние идентифицируется однозначно), либо в канале измерения ? (неопределенный исход). Исход в данном канале измерений может иметь место от любого входного состояния. При таком исходе состояние неизвестно.

UM-атака. Для проведения такой атаки подслушивателю (Еве) достаточно разорвать канал связи[4)] вблизи передающей (Алиса) и приемной (Боб) станций. Подслушиватель производит UM-измерения вблизи передающей станции. Их исход он сообщает своему партнеру, находящемуся вблизи приемной стороны, по своему классическому каналу связи. Для исходов с определенным результатом вблизи приемной стороны готовится состояние, которое посылала Алиса. Если Евой получен исход с неопределенным результатом, то Бобу ничего не посылается: посылка блокируется. При $L > L_c$, когда вероятность исходов с неопределенным результатом равна вероятности потерь в квантовом канале связи, подслушиватель может блокировать посылки, в которых получен неопределенный исход. В остальных посылках Ева знает состояния достоверно и может переслать их Бобу.

Несмотря на то что часть посылок при такой атаке блокируется, при превышении длиной канала связи критической длины L_c Ева сохраняет число посылок, которые должны достичь приемной стороны в ее отсутствие, знает весь переданный ключ и не производит ошибок на приемной стороне.

При $L > L_c$ UM-атака всегда возможна. Поэтому на первый взгляд ответ на поставленный выше вопрос должен быть отрицательным: задача не имеет решения. Тем не менее ответ оказывается положительным.

Основная идея схемы квантовой криптографии. Ниже предлагается система квантовой криптографии, которая гарантирует секретность передачи ключей при любом затухании в канале связи.

Принципиально новая идея протокола состоит в использовании комбинации интенсивного и квазиоднофотонного когерентных состояний. Сначала интенсивное когерентное состояние используется частично для контроля блокировки посылок Евой, а затем для интерференционных измерений в комбинации с квазиоднофотонным состоянием.

Причина потери секретности, как было показано выше, связана с тем, что Ева может игнорировать (блокировать) часть посылок, в которых был получен неопределенный исход. Точнее, тот факт, что Ева блокирует посылку и ничего не посылает, означает, что Ева посылает вакуумное состояние. *Для того чтобы протокол был устойчив при любых потерях, необходимо запретить Еве "ничего" не посы-*

[3)] Даже при условии, что используются идеальные фотодетекторы, не имеющие темновых шумов.

[4)] Напомним, что в квантовой криптографии квантовый канал связи (волоконный кабель) не контролируется легитимными пользователями. Поэтому подслушиватель может производить любые манипуляции с ним.

лать в том случае, когда она получила неопределенный исход, т.е. запретить посылать вакуумное состояние. Другими словами, протокол должен быть устроен так, чтобы перепосылка Евой вакуумного состояния приводила к ошибкам на приемной стороне. Однако отчасти проблема состоит в том, что обычные детекторы, работающие в счете фотонов, не реагируют на вакуумную компоненту состояния.

Сначала приведем измерения, которые не позволят подслушивателю делать измерения с определенным исходом и при этом не производить ошибок на приемной стороне. Затем опишем оптоволоконную реализацию, которая отвечает таким измерениям.

В протоколе используется пара когерентных состояний, отвечающих 0 и 1.

$$\begin{aligned} 0 &- |e^{i\varphi_0}\sqrt{\mu}\rangle \quad (\varphi_0 = 0), \\ 1 &- |e^{i\varphi_1}\sqrt{\mu}\rangle \quad (\varphi_1 = \pi). \end{aligned} \tag{3}$$

Они посылаются в канал связи равновероятно, причем $|e^{i\varphi_{0,1}}\sqrt{\mu}\rangle = |\pm\alpha\rangle$ ($|\alpha|^2 = \mu$). Основная идея состоит в том, чтобы осуществлять такие измерения, которые изначально учитывали бы изменения когерентного состояния за счет потерь в линии связи, но в отсутствие подслушивателя.

После прохождения через канал связи с затуханием когерентное состояние преобразуется следующим образом (см., например, [18, 26, 27]): $|\pm\alpha\rangle \to |\pm\alpha\sqrt{T(L)}\rangle = |\pm\sqrt{\mu T(L)}\rangle$ ($T(L) = 10^{-\delta L/10}$, для одномодового оптоволокна SMF-28 величина $\delta \approx 0.2$ дб/км). Вообще говоря, при прохождении через канал когерентного состояния комплексный параметр α, кроме уменьшения амплитуды ($|\alpha| = |\alpha\sqrt{T(L)}|$), приобретает дополнительную фазу $\alpha \to e^{i\varphi_{\rm channel}}\alpha\sqrt{T(L)}$. Однако, как мы увидим ниже, данная дополнительная фаза не играет роли. Поэтому мы ее опускаем.

Два разных измерения, которые Боб выбирает случайно и равновероятно, и которые позволяют отличать состояния $|e^{i\varphi_{0,1}}\sqrt{\mu(L)}\rangle$ от любых других состояний, можно записать в виде[5)]

$$I = P(e^{i\varphi_{0,1}}\sqrt{\mu(L)}) + P_\perp(e^{i\varphi_{0,1}}\sqrt{\mu(L)}), \tag{4}$$

$$P(e^{i\varphi_{0,1}}\sqrt{\mu(L)}) = |e^{i\varphi_{0,1}}\sqrt{\mu(L)}\rangle\langle e^{i\varphi_{0,1}}\sqrt{\mu(L)}|,$$

$$P_\perp(e^{i\varphi_{0,1}}\sqrt{\mu(L)}) = I - P(e^{i\varphi_{0,1}}\sqrt{\mu(L)}).$$

[5)] Возможно использование одного измерения с тремя исходами (два исхода определенных и один неопределенный [4–9]), что эквивалентно двум измерениям в смысле различения состояний (3). Однако два разных измерения технически проще реализовать.

Выбор измерения фиксируется выбором $\varphi_{0,1}$. Каждое из двух измерений (4) имеет два исхода. При этом исход $\perp$ никогда не происходит от состояния $|e^{i\varphi_{0,1}}\sqrt{\mu(L)}\rangle$, т.к. вероятность данного исхода тождественно равна нулю:

$$\begin{aligned} &\Pr(\perp, |e^{i\varphi_{0,1}}\sqrt{\mu(L)}\rangle) = \\ &= \mathrm{Tr}\{P_\perp(e^{i\varphi_{0,1}}\sqrt{\mu(L)})|e^{i\varphi_{0,1}}\sqrt{\mu(L)}\rangle \times \\ &\times \langle e^{i\varphi_{0,1}}\sqrt{\mu(L)}|\} \equiv 0. \end{aligned} \tag{5}$$

Данные измерения обнаруживают любые изменения исходных состояний. Если Евой получен неопределенный исход, то перепосыл любого состояния, кроме правильного, в том числе и вакуумного (блокирование посылки), приведет к ошибке на приемной стороне. Например, если Алиса послала состояние $|+\alpha\rangle \to |+\alpha\sqrt{T(L)}\rangle$, а Боб выбрал измерение

$$I = P(e^{i\varphi_0}\sqrt{\mu(L)}) + P_\perp(e^{i\varphi_0}\sqrt{\mu(L)}), \tag{6}$$

то возникнет отсчет с вероятностью

$$\begin{aligned} \Pr(\perp, |\mathrm{vac}\sqrt{\mu(L)}\rangle) &= \mathrm{Tr}\{P_\perp(e^{i\varphi_0}\sqrt{\mu(L)})|\mathrm{vac}\rangle\langle\mathrm{vac}|\} = \\ &= |\langle\mathrm{vac}|e^{i\varphi_0}\sqrt{\mu(L)}\rangle|^2 = e^{-\sqrt{\mu(L)}/2} \end{aligned} \tag{7}$$

в канале измерения, где его не должно быть. Таким образом, блокирование посылки (перепосыл вакуумного состояния) неизбежно приведет к ошибке на приемной стороне Боба. Здесь $|\mathrm{vac}\rangle = |\alpha = 0\rangle$.

Нетривиальный момент состоит в реализации таких измерений. Данные измерения, по существу, сводятся к проекции когерентного состояния на такое же когерентное состояние и подпространство, ортогональные данному состоянию. Для реализации измерения необходимо, кроме исследуемого когерентного состояния, иметь еще одно когерентное состояние, синхронизированное по времени с исходным. В гайзенберговской картине параметр α когерентного состояния изменяется с оптической частотой $\sim 10^{15}$ Гц. Поэтому приготовить еще одно состояние, синхронизованное по времени и по частоте с данным состоянием, технически крайне сложно, хотя и возможно. Интерференция двух когерентных состояний, приготовленных из разных источников, была экспериментально продемонстрирована в работах [28–30]. На сегодняшний день достигнуты рекорды при синхронизации оптических частот с джиттером по времени на уровне $10^{-18}\,\mathrm{c}^{-1}$ в течение десятков секунд [31, 32]. Таким образом, сравнивать когерентные состояния, полученные из различных источников, хотя принципиально возможно (см., например, [28–30]), но технически крайне сложно.

Реализация системы и измерений. Наша идея состоит в том, чтобы использовать когерентные состояния, полученные из одного источника. Со-

стояния проходят по одному и тому же пути в канале связи. Изменение фазы у параметра α одинаково. Поэтому при измерениях общее его изменение неважно. Одно состояние с малым средним числом фотонов ($\mu = |\alpha|^2 \ll 1$) является информационным. Второе когерентное состояние имеет большое (макроскопически большое) среднее число фотонов ($\mu_c = |\alpha_c|^2 \gg 1$). Перед измерениями интенсивное когерентное состояние расщепляется светоделителем. На линейном светоделителе, как известно [26], когерентное состояние преобразуется самоподобным образом, т.е. после деления оно остается когерентным на каждом из двух выходов светоделителя. Важно также, что когерентные состояния на двух выходах светоделителя являются *незапутанными*. Это имеет место только для когерентных состояний [26].

Перед измерениями проверяется интенсивность части расщепленного когерентного состояния с большим средним числом фотонов калиброванным классическим детектором. Если обнаружено изменение интенсивности по сравнению с той, которая должна быть, то посылка выбрасывается. Если интенсивность имеет правильную величину, то вторая часть состояния (после контролируемого ослабления) используется для интерференционных измерений вместе со слабым информационным когерентным состоянием.

Оказывается, что такой процедуры достаточно, чтобы ослабленная часть когерентного состояния с большим μ_c играла роль эталонного состояния, с которым производится сравнение информационного когерентного состояния. Таким образом, данная процедура фактически реализует требуемое измерение в формулах (4)–(6).

Перейдем к описанию оптической схемы и деталям реализации. Схема приведена на рис. 1.

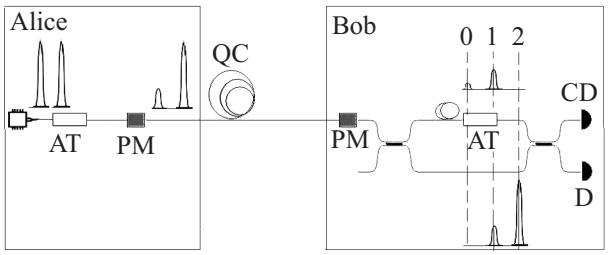

Рис. 1. Принципиальная схема оптоволоконной системы квантовой криптографии

Длина линии связи и затухание в ней известны заранее. Они являются параметрами протокола. На передающей стороне в каждой посылке, которые независимы, генерируется пара одинаковых когерентных состояний с большим средним числом фотонов ($\mu_c = |\alpha_c|^2 \gg 1$), сдвинутых по времени и имеющих общую привязку по фазе. Последнее достигается при помощи лазера, работающего в режиме синхронизации мод (mode-locked) [26]. Общая привязка фазы позволяет устроить интерференции двух данных состояний при совмещении их по времени.

При прохождении второго состояния через аттенюатор (AT на рис. 1) последний активируется и второе когерентное состояние ослабляется до квазиоднофотонного уровня ($\mu = |\alpha|^2 \ll 1$). При этом состояния остаются когерентными и сфазированными относительно друг друга. Далее Алиса случайно и равновероятно выбирает 0 или 1 и прикладывает требуемое напряжение на фазовый модулятор (PM на рис. 1) в момент прохождения квазиоднофотонного состояния $|\alpha\rangle$. После этого состояние становится равным $|\pm\alpha\rangle$. Далее пара состояний поступает в квантовый канал связи (QC на рис. 1). На приемной стороне Боб случайно и независимо от Алисы прикладывает напряжение на фазовый модулятор в момент прохождения квазиоднофотонного состояния, чтобы скомпенсировать фазу у параметра α, приобретенную на стороне Алисы.

Совмещение состояний по времени достигается при помощи интерферометра Маха–Цандера с разной длиной плеч. Разность оптического пути по верхнему и нижнему плечу интерферометра равна расстоянию между парой состояний. В верхнем плече встроен аттенюатор с фиксированным коэффициентом ослабления, таким, чтобы ослабленное когерентное состояние с большим средним числом фотонов сравнялось по интенсивности с квазиоднофотонным. Если фазы Алисы и Боба одинаковы ($\varphi_A = \varphi_B = 0$ или $\varphi_A = \varphi_B = \pi$), то конструктивная интерференция при наложении сдвинутых по времени когерентных состояний из верхнего и нижнего плеча имеет место в нижнем однофотонном детекторе (D на рис. 1).

Более формально ситуация выглядит следующим образом. На первом светоделителе входные состояния на верхнем входе равны $|\sqrt{\mu(L)}\rangle_1 \otimes |\sqrt{\mu_c(L)}\rangle_2$, а на нижнем входе это вакуумные состояния. Индексы “1” и “2” обозначают временные окна, в которых локализованы когерентные состояния.

После прохождения первого светоделителя когерентные состояния преобразуются следующим образом (см., например, [26]): в верхнем плече с учетом задержки назад во времени – $|\sqrt{\mu(L)}/\sqrt{2}\rangle_0 \otimes$ $\otimes |\sqrt{\mu_c(L)}/\sqrt{2}\rangle_1$, а в нижнем плече $|-\sqrt{\mu(L)}/\sqrt{2}\rangle_1 \otimes$ $\otimes |-\sqrt{\mu_c(L)}/\sqrt{2}\rangle_2$. Светоделители можно выбрать симметричными.

Далее в верхнем плече в момент прохождения когерентного состояния с большим средним числом фотонов активируется аттенюатор (AT на рис. 1), который изменяет среднее число фотонов в *фиксированное* число раз, а именно в $(\mu(L)/\mu_c(L))^{-1}$ раз. При этом состояния в верхнем плече становятся равными $|[\mu^2(L)/\mu_c(L)]/\sqrt{2}\rangle_0 \otimes |\sqrt{\mu(L)}/\sqrt{2}\rangle_1$. Величина ослабления при типичных $\mu \approx 0.1$ и интенсивности классического когерентного состояния в 0.1 mW составляет ≈ 170 db.

После преобразования на втором светоделителе состояния в нижнем плече имеют вид $|[\mu^2(L)/\mu_c(L)]/2\rangle_0 \otimes |\sqrt{\mu(L)}\rangle_1 \otimes |\sqrt{\mu_c(L)}/2\rangle_2$, а в верхнем плече – вид $|-[\mu^2(L)/\mu_c(L)]2\rangle_0 \otimes |\mathrm{vac}\rangle_1 \otimes \otimes |\sqrt{\mu_c(L)}/2\rangle_2$. Таким образом, в среднем временном окне 1 при совпадении фаз Алисы и Боба и в отсутствие внешнего возмущения имеет место конструктивная интерференция информационного состояния и ослабленного когерентного состояния с большим числом фотонов на выходе нижнего плеча интерферометра. По верхнему выходу во временном окне 2 классический детектор (CD на рис. 1) регистрирует интенсивность когерентного ("классического") состояния $|\sqrt{\mu_c(L)}/2\rangle_2$. Если обнаружено изменение интенсивности когерентного состояния с большим μ_c, то посылка отбрасывается.

Покажем теперь, почему данный протокол устойчив относительно UM-атаки, т.е. UM-измерения не позволяют Еве: 1) *знать весь ключ*, 2) *сохранить среднее число регистрируемых посылок на приемной стороне*; 3) *не произвести при этом ошибок на приемной стороне.*

Для этого нам потребуется два факта.

1. Отклик (фототок) классического детектора является некоторой известной (калиброванной) функцией интенсивности сигнала (среднего числа фотонов в когерентном состоянии μ_c; см., например, [26]).

2. Однофотонный детектор не реагирует на вакуумную компоненту. Вероятность регистрации детектора пропорциональна[6] $1 - e^{-\eta\mu(L)}$, где η – квантовая эффективность детектора (см., например, [18]). Типичное значение на телекоммуникационной длине волны 1.55 мкм составляет $\eta \approx 10{-}30\%$).

Если в какой-то посылке Ева получила неопределенный исход, то имеется лишь несколько вариантов ее дальнейших действий.

1. Послать наугад произвольное информационное когерентное состояние $|\pm\alpha(L)\rangle$. Очевидно, что это приведет к ошибке на приемной стороне. Будут отсчеты во временном окне 1, когда их не должно быть. Например, для Алисы $\varphi_A = 0$, для Боба $\varphi_B = 0$, а Ева выбрала $\varphi_E = \pi$ (см. (5)–(7)). Среднее число регистрируемых посылок при этом сохранится.

2. Ничего не посылать. Как было сказано выше, это отвечает перепосылке вакуумного состояния. Это также приведет к ошибкам. Например, если Алиса посылала состояние $|+\alpha(L)\rangle$ ($\varphi_A = 0$), а Боб выбрал значение фазы $\varphi_B = \pi$, то отсчета в однофотонном детекторе не должно быть, поскольку на входе детектора во временном окне 1 будет состояние $|[+\alpha(L) - \alpha(L)]/2\rangle_2 = |\mathrm{vac}\rangle_2$. Перепосыл наугад неправильного состояния $|-\alpha(L)\rangle$ приведет к тому, что на входе детектора будет состояние $|[-\alpha(L) - \alpha(L)]/2\rangle_2$. Это приведет к ошибочному отсчету в тех посылках, где его не должно было бы быть.

3. Блокировать посылку целиком (как когерентное состояние с большим μ_c, так и квазиоднофотонное когерентное состояние с малым μ). В этом случае будет зарегистрировано изменение интенсивности когерентного состояния с большим μ_c детектором CD. По этой же причине Ева не может увеличить интенсивность контрольного когерентного состояния, оставаясь при этом незамеченной.

Таким образом, поскольку интенсивность когерентного состояния с большим μ_c контролируется классическом образом, Ева не может изменить истинного информационного квантового когерентного состояния ни в одной посылке. Это неизбежно приведет к ошибкам на приемной стороне. Важно отметить, что Ева детектируется при любой длине линии связи и, соответственно, при любых потерях. Формально это связано с тем, что среднее число в когерентном состоянии убывает экспоненциально с длиной ($\mu(L) \sim 10^{-\delta L/10}$) и ни при каком L в нуль не обращается. Естественно, скорость генерации ключей при этом экспоненциально падает с длиной. Однако секретность ключей гарантируется при любом L. Единственным ограничивающим фактором для данного протокола являются темновые шумы однофотонного детектора.

Сравнение с другими системами квантовой криптографии. В последние годы были предложены новые схемы квантовой криптографии [11–23], предположительно устойчивые относительно UM-атаки. Одной из таких схем является DPS QKD [23]. Данная система разрабатывалась в рамках межотраслевого проекта в Японии [33]. Покажем причину потенциальной уязвимости схем, подобных [18]. Это позволит выявить и локализовать истинную

[6] Конкретный функциональный вид вероятности отсчета однофотонного детектора неважен. Он может быть любой функцией от доли компонент с ненулевым числом фотонов в когерентном состоянии.

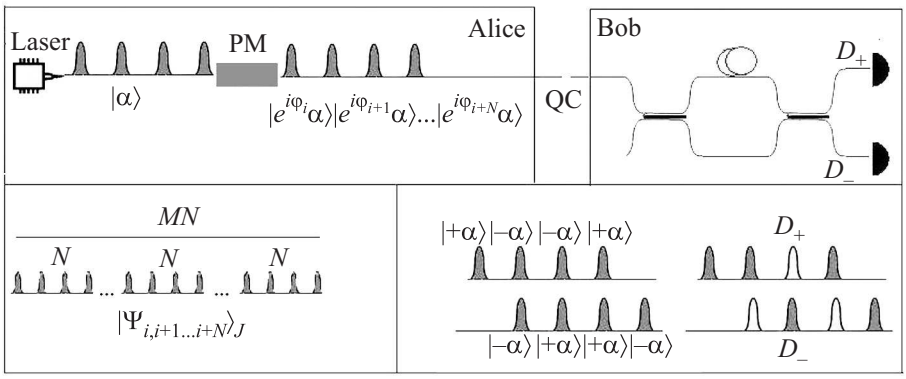

Рис. 2. Принципиальная схема оптоволоконной системы квантовой криптографии с дифференциально-фазовым кодированием (Differential Phase Shift) [23]

причину потери секретности при длине линии связи с потерями больше критической.

В протоколе [23] информация о ключе кодируется в относительную разность фаз в пакете когерентных состояний, которые имеют вид

$$|\alpha_1\rangle \otimes |\alpha_2\rangle \otimes \dots |\alpha_N\rangle, \tag{8}$$

где $\alpha_i = \pm\alpha$. Одинаковые значения фаз соседних состояний (и α_i, и $\alpha_{i\pm}$ – либо со знаком "+", либо со знаком "–") отвечают логическому 0, а разные значения соседних фаз – логической 1 (см. рис.2).

На приемной стороне последовательность состояний сдвигается на одну позицию при помощи интерферометра Маха–Цандера. На входе детектора D_+ имеет место конструктивная интерференция сдвинутых состояний: $\dots|[\alpha_i(L) + \alpha_{i+1}(L)]/2\rangle\dots$, а на входе детектора D_- – деструктивная интерференция: $\dots|[\alpha_i(L) - \alpha_{i+1}(L)]/2\rangle\dots$.

В данном протоколе для детектирования подслушивания легитимные пользователи следят только за ошибкой на приемной стороне и средним числом посылок, которые должны достичь приемной станции. Ошибкой считается отсчет во временном окне, где его не должно было быть.

Поскольку однофотонные детекторы $D_\pm$ не реагируют на вакуумную компоненту состояния, вероятность получения отсчета в непустом временном окне есть $1 - e^{-\mu\eta T(L)}$. Вероятность получения отсчета во всех N посылках из пакета равна $(1 - e^{-\mu\eta T(L)})^N$, а вероятность отсутствия отсчетов от целого пакета из N посылок – $(e^{-\mu\eta T(L)})^N$. *Важно отметить, что статистика распределения отсчетов по временным окнам в системе* DPS *никак не контролируется* [23]. *Протокол с контролем распределения отсчетов пока даже не сформулирован.*

Протокол потенциально уязвим относительно измерений с определенным исходом. Ева разрывает квантовый канал вблизи станций Алисы и Боба и делает UM-измерения в каждом отдельном временном окне (см. (1), (2), (4)) вблизи передающей стороны. Вероятность получения определенного исхода есть $p_{\text{ОК}} = 1 - e^{-\mu}$. Вероятность неопределенного исхода $p_? = e^{-\mu}$.

В реальной ситуации последовательность когерентных состояний всегда конечна ($N \sim 10$ [18, 23]). Пусть всего посылается $J = 1, 2 \dots, M$ пакетов по N посылок. Внутри пакета когерентность сохраняется, а между пакетами – нет. Это будет приводить к ошибкам у Боба даже в отсутствие Евы. Цель Евы – не произвести дополнительных ошибок внутри пакета и узнать передаваемые состояния. Ева может рассматривать пакет из N посылок как *одно составное* квантовое состояние $|\Psi_{i,i+1...i+N}\rangle_J = |\alpha_i\rangle_J \otimes |\alpha_{i+1}\rangle_J \otimes \dots |\alpha_{i+N}\rangle_J$. Она будет различать их при помощи измерений с определенным исходом (см.(1), (2)).

На приемной стороне из MN ($M \gg 1$) посланных состояний при большом MN будет зарегистрировано $M \cdot N(1 - e^{-\mu\eta T(L)})$ посылок, которые будут, естественно, случайно распределены по M пакетам.

Вероятность неопределенного исхода у Евы при различении состояний $|\Psi_{i,i+1...i+N}\rangle_J$ (целых пакетов) не хуже, чем $P(?|\Psi_J) = (e^{-\mu})^N$. Если получен неопределенный исход, то Ева блокирует пакет. Если получен определенный исход, то Ева знает весь пакет. Однако ей надо сохранить среднее число посылок. Для этого Ева вместо тех пакетов, которые ей известны, готовит пакеты с большим средним числом фотонов $\mu^* > 1$ в каждом временном окне с той же фазой, что и у исходных. При этом вероятность регистрации в каждом временном окне у Боба будет равна $1 - e^{-\mu^*\eta} \approx 1$ (при $\mu^*\eta \gg 1$ реально достаточно сделать $\mu^* \approx 100$). Это гарантирует Еве, что все перепосланные и известные ей посылки будут зарегист-

рированы Бобом. Условие сохранения среднего числа посылок определяется из равенства среднего числа потерянных из-за затухания посылок, случайно распределенных по разным пакетам, числу выброшенных целых пакетов-состояний из серии из M пакетов-состояний: $MNe^{-\mu T(L)} = MP(?|\Psi_J) = M(e^{-\mu})^N$ (пусть даже в пользу Боба, $\eta = 100\%$). *Еще раз отметим, что статистика распределения утерянных посылок не контролируется. Поэтому если произошла пропажа целых пакетов (последовательных посылок из N штук), то на приемной стороне при таком событии Ева не будет обнаружена, поскольку такая потеря в конкретной серии из M пакетов может иметь место сама по себе, без участия Евы. В протоколе [23] такие события пропускаются легитимными пользователями. Фактически Ева заменяет полное число пропавших и незарегистрированных посылок, случайно разбросанных по всей серии, на выброшенные целые пакеты с сохранением полного числа зарегистрированных посылок.* Для критической длины имеем $L > L_c = \frac{10}{\delta}\log_{10}[1/(N + \ln(N)/\mu)]$. Так как правая часть отрицательна, протокол не гарантирует секретного распределения ключей, начиная с нулевой длины линии. Таким образом, Ева знает весь ключ и не производит ошибок. Ева, конечно, при этом меняет распределение незарегистрированных посылок, но эта статистика распределения отсутствующих отсчетов не контролируется Алисой и Бобом.

Причина этого состоит в том, что: 1) в протоколе легитимные пользователи не следят за статистикой распределения отсчетов по временным окнам (следят только за ошибкой); 2) не контролируется интенсивность перепосланных состояний (это обстоятельство важно для гарантированной регистрации перепосланных пакетов).

В протоколах [18, 23], в которых возмущение когерентных состояний производится путем сравнения этих же когерентных состояний из разных временных окон, проблема не решается, поскольку все состояния проходят через канал связи и могут быть подвержены модификации подслушивателем.

Выражаю благодарность коллегам по Академии криптографии Российской Федерации за постоянную поддержку. Работа поддержана грантами РФФИ # 11-02-00455 и 10-02-90036-Бел.

1. W. K. Wooters and W. H. Zurek, Nature **299**, 802 (1982).
2. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
3. G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
4. D. Dieks, Phys. Lett. A **126**, 303, (1988).
5. I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
6. A. Peres, Phys. Lett. A **128**, 19 (1988).
7. G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995).
8. A. Chefles, Phys. Lett. A **239**, 339 (1998).
9. P. Raynal, arXiv:quant-ph/0611133.
10. C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proc.of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, p. 175.
11. V. Scarani, A. Acэin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **95**, 057901-1 (2004).
12. A. Acin, N. Gisin, and V. Scarani, arXiv:quant-ph/0302037.
13. Д. А. Кронберг, С. Н. Молотков, ЖЭТФ **136**, 650 (2009).
14. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf et al., Rev. Mod. Phys. **81**, 1301 (2009).
15. W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
16. N. Gisin, G. Ribordy, H. Zbinden et al., arXiv:quant-ph/0411022.
17. *SECOQC, White Paper on Quantum Key Distribution and Cryptography*, arXiv:quant-ph/0701168.
18. D. Stucki, N. Brunner, N. Gisin et al., arXiv:quant-ph/0506097.
19. C. Branciard, N. Gisin, N. Lütkenhaus, and V. Scarani, arXiv:quant-ph/0609090.
20. C. Branciard, N. Gisin, and V. Scarani, arXiv:quant-ph/0710.4884.v2.
21. D. Stucki, C. Barreiro, S. Fasel et al., arXiv:quant-ph/08095264.
22. M. Curty, L.-L. Zhang, H.-K. Lo, and N. Lütkenhaus, arXiv:quant-ph/0609094.
23. 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).
24. H. Takesue, S. W. Nam, Q. Zhang et al., Nature Photonics **1**, 343 (2007).
25. K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
26. Л. Мандель, Э. Вольф, *Оптическая когерентность и квантовая оптика*, М.: Физматлит, 2000; L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*, Cambridge University Press, 1995.
27. L. J. Wang, X. Y. Zou, and L. Mandel, Phys. Rev. A **44**, 4614 (1991).
28. R. Kaltenbaek, B. Blauensteiner, M. Zukowski et al., arXiv:quant-ph/0603048.
29. L. Mandel, Phys. Rev. A **28**, 929 (1983).
30. H. Paul, Rev. Mod. Phys. **58**, 209 (1986).
31. N. R. Newbury, P. A. Williams, and W. C. Swann, Optics Letters **32**, 3056 (2007).
32. S. M. Foreman, K. W. Holman, D. D. Hudson et al., Rev. Scien. Instrum. **78**, 021101 (2007).
33. *Updating Quantum Cryptography*, arXiv:quant-ph/09054325.