ЖЭТФ, 2008, том 134, вып. 1 (7), стр. 39–64

О СТОЙКОСТИ ПРАКТИЧЕСКОЙ КВАНТОВОЙ КРИПТОГРАФИИ: ПРОТОКОЛ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ BB84

С. Н. Молотков*

Институт физики твердого тела Российской академии наук
142432, Черноголовка, Московская обл., Россия

Академия криптографии Российской Федерации,
Факультет вычислительной математики и кибернетики,
Московский государственный университет им. М. В. Ломоносова
119899, Москва, Россия

Поступила в редакцию 8 февраля 2008 г.

В реальных оптоволоконных системах квантовой криптографии неидеальность лавинных фотодетекторов, неоднофотонность источника квантовых состояний и затухание в канале связи могут приводить при определенном наборе параметров к невозможности передачи ключей. Простыми средствами показано, что в случае, когда действия подслушивателя не лимитируются никакими техническими ресурсами и ограничены лишь фундаментальными запретами квантовой механики на различимость квантовых состояний, а легитимные участники протокола используют устройства, реализуемые на нынешнем технологическом уровне, система квантовой криптографии позволяет передавать ключи и гарантировать их секретность. Получены соотношения между параметрами реальных оптоволоконных систем квантовой криптографии и длиной канала связи, до которой гарантируется секретная передача ключей. Определены предельные значения для скорости генерации финального ключа в реальном времени, на которую можно рассчитывать при нынешнем технологическом уровне. Получена также критическая длина линии для строго однофотонного источника и неидеальных фотодетекторов, которая при достигнутых на сегодняшний день значениях квантовой эффективности ($\eta \approx 20\,\%$) и вероятности темновых отсчетов ($p_{dark} \sim 10^{-7}$) для лавинных фотодетекторов, может достигать 300 км.

PACS: 03.67.Hk

1. ВВЕДЕНИЕ

Квантовая криптография, другими словами, распределение криптографических ключей либо по оптоволоконным каналам связи, либо через открытое пространство гарантирует не только детектирование любых попыток подслушивания, но и конфиденциальность (секретность) передаваемых ключей, если ошибка в первичных ключах на приемной стороне не превышает некоторой критической величины. Величина критической ошибки зависит от используемого протокола распределения ключей и определяется лишь фундаментальными законами квантовой механики.

В квантовой криптографии принципиально невозможно отличить ошибки в первичных ключах, возникающие от действий подслушивателя, от ошибок, возникающих из-за неидеальностей самой системы. Поэтому все ошибки приходится списывать на действия подслушивателя.

Первым, основным и наиболее исследованным протоколом квантового распределения ключей является протокол BB84 (Bennett, Brassard) [1]. В результате длительных исследований для данного протокола для идеального случая (строго однофотонный источник состояний, идеальные детекторы, канал связи без потерь) различными способами было доказано [2–5], что секретное распределение ключей возможно, если критическая величина ошибки в первичных ключах не превышает $Q_c \approx 11\,\%$. Данная

*E-mail: molotkov@issp.ac.ru

величина ошибки является теоретическим пределом в том смысле, что она дает верхнюю границу ошибок $Q < Q_c$, до которой возможно распределение ключей и гарантируется их секретность, если подслушиватель действует оптимальным образом. Оптимальность в данном контексте понимается в следующем смысле. Подслушиватель использует такую стратегию, которая при данной наблюдаемой ошибке Q на приемной стороне, позволяет ему извлечь максимум возможной информации о передаваемом ключе. Такая стратегия была впервые явно построена в работе [6]. При этом действия подслушивателя не ограничены никакими ресурсами и техническими возможностями, а ограничены лишь фундаментальными законами природы (квантовой механики). Поэтому часто секретность ключей, которую гарантирует квантовая криптография, называют безусловной (unconditional), в отличие от секретности, основанной, например, на вычислительной сложности или технических ограничениях.

Критическая ошибка для протокола BB84 определяется как корень трансцендентного уравнения

$$1 - 2H(Q) = 0, \tag{1}$$

где

$$H(Q) = -Q \log Q - (1 - Q) \log(1 - Q)$$

— бинарная энтропийная шенноновская функция.

Отметим, что в знаменитой работе [2] величина критической ошибки равна корню уравнения

$$1 - H(2Q) - H(Q) = 0, \quad Q_c \approx 7.5\,\%,$$

что меньше, чем корень уравнения (1). В дальнейшем данный результат был улучшен в работе [5] с использованием случайного усиления секретности (privacy amplification).

Максимальная длина секретного ключа, который может быть получен при наблюдаемой ошибке $Q < Q_c$, есть

$$n_{key} = n(1 - 2H(Q)), \tag{2}$$

n — число бит на приемной стороне, оставшихся после согласования базисов и оценки вероятности ошибки. Случайная последовательность 0 и 1 длиной n_{key} является общим секретным ключом для двух пространственно-удаленных легитимных пользователей (называемых обычно Алисой и Бобом), о котором подслушиватель не имеет никакой информации[1)].

[1)] Точнее, имеет сколь угодно экспоненциально малую информацию по параметру секретности, который легитимными пользователями может быть выбран любым при достаточно длинной последовательности.

Для оптимальной стратегии подслушивателю (называемому обычно Евой) требуется квантовая память и возможность выполнять коллективные измерения над длинной последовательностью квантовых состояний для извлечения максимума классической информации о ключе.

Величина критической ошибки для данного протокола является в определенном смысле «мировой» постоянной, поскольку определяется лишь через фундаментальную энтропийную функцию классической и квантовой теории информации и не содержит никаких параметров самой системы, а определяется только протоколом.

При выводе уравнения (1) считается, что сама по себе система квантовой криптографии является идеальной. Точнее говоря, предполагается, что используется строго однофотонный источник квантовых состояний, фотодетекторы также являются идеальными — имеют единичную ($\eta = 100\,\%$) квантовую эффективность и не имеют собственных шумов (вероятность темновых отсчетов $p_{dark} = 0$). Считается также, что квантовый канал связи является каналом без потерь — квантовые состояния могут искажаться (например, состояние поляризации может изменяться при распространении), но не поглощаться в канале связи.

Несмотря на большой прогресс в понимании природы секретности ключей в квантовой криптографии для идеальных условий, необходимо иметь ответы на вопросы, возникающие для реальных практических систем квантовой криптографии, которые далеки от идеальных.

Основными источниками неидеальностей реальных оптоволоконных систем квантовой криптографии являются следующие.

1) Источник информационных квантовых состояний не является строго однофотонным. В реальных условиях используется сильно ослабленное лазерное излучение. Поскольку лазерное излучение представляет собой когерентное квантовое состояние, распределение числа фотонов в нем является пуассоновским. Это означает, что кроме вакуумной и однофотонной компонент в импульсе присутствуют, хотя и с малой вероятностью, компоненты с двумя и более фотонами. Обычно излучение ослабляется до уровня $\mu = 0.1$–0.5, μ — среднее число фотонов в импульсе.

2) Лавинные фотодетекторы имеют не единичную квантовую эффективность $\eta < 100\,\%$. Кроме того, для оптоволоконных реализаций протокола BB84 используется пара фотодетекторов, которые имеют разные квантовые эффективности η_1 и η_2. Типич-

ные значения квантовой эффективности лавинных фотодетекторов на длине волны 1.3–1.55 мкм составляют $\eta = 0.1$–0.4.

3) Лавинные фотодетекторы имеют собственные шумы, приводящие к темновым отсчетам. Все используемые фотодетекторы для регистрации фотонов на телекоммуникационной длине волны 1.3–1.55 мкм работают в стробируемом режиме для уменьшения темновых отсчетов. Вероятность темновых отсчетов определяется как вероятность получения темнового отсчета во временном окне строба и составляет $p_{dark} = 10^{-4}$–10^{-6} отсч./строб. Типичные длительности стробирующих импульсов составляют 1–2.5 нс. Для уменьшения темновых шумов всегда используется охлаждение лавинных детекторов. При этом типичная температура охлаждения фотодетекторов составляет $-40\,^{\circ}$C–$80\,^{\circ}$C. При охлаждении до температур жидкого азота достижима вероятность темновых отсчетов $p_{dark} = 10^{-7}$, что является рекордным значением, однако охлаждение жидким азотом является неудобным и, поэтому, нежелательным. Кроме того, такое глубокое охлаждение приводит к увеличению времени рассасывания лавины (эффект afterpulsing).

4) Оптоволоконный канал связи также является неидеальным. Наиболее критическим параметром для секретности ключей при не строго однофотонном источнике является затухание в оптоволокне (исчезновение фотонов при передаче). Минимум затухания, как известно, достигается на длине волны 1.55 мкм в стандартном одномодовом волокне SMF-28, типичное значение составляет $\alpha \approx 0.2$ дБ/км.

Неидеальность системы и канала связи (особенно потери в нем) открывают возможности для новых атак подслушивателя на передаваемый ключ, которые были невозможны в условиях идеальной системы [7–9].

Основной вопрос, на который необходимо иметь ответ, состоит в следующем. Пусть заданы реальные параметры системы — квантовые эффективности фотодетекторов η_1, η_2, вероятности p_1, p_2 темновых отсчетов, среднее число μ фотонов в импульсе, коэффициент α затухания в канале связи, длина L оптоволоконного канала связи. Пусть на приемной стороне длина битовой последовательности первичного ключа, оставшейся после согласования базисов и оценки вероятности ошибок, есть n. Пусть далее $\tilde{Q}$ — наблюдаемая вероятность ошибок в первичных ключах.

Какой длины секретный ключ может быть получен в данных условиях?[2)]

В криптографии, в том числе и квантовой, всегда исходят из консервативных оценок возможностей легитимных пользователей (Алисы и Боба) и подслушивателя (Евы).

Считается, что возможности легитимных пользователей ограничены уровнем современных технологий. Применительно к задачам квантовой криптографии это означает следующее.

1) Алиса и Боб не имеют квантовой памяти, не могут сохранять квантовые состояния и вынуждены производить их детектирование «на ходу».

2) Алиса и Боб не могут делать неразрушающие измерения по определению числа фотонов в импульсе[3)].

3) Фотодетектор Боба не различает число фотонов при регистрации. Это отвечает реальной ситуации для лавинных фотодетекторов.

4) Фотодетекторы Боба не идеальные, имеют квантовую эффективность $\eta < 1$ и ненулевые собственные шумы (темновые отсчеты с вероятностью $p_{dark} \neq 0$ во временном окне строба).

5) Источник квантовых состояний Алисы не является строго однофотонным, а представляет собой сильно ослабленное лазерное излучение (когерентное состояние с малым средним числом фотонов $\mu \approx 0.1$–0.5).

6) Алиса и Боб не могут использовать квантовый канал связи без затухания[4)].

Консервативно считается, что Ева, напротив, не ограничена никакими техническими возможностями, а ограничена лишь фундаментальными запретами квантовой механики. Фактически детектирование попыток подслушивания и секретность квантовой криптографии держатся на двух запретах квантовой механики. Во-первых, это невозможность копирования неизвестного квантового состояния, что является следствием линейности квантовой теории. Имеется в виду невозможность копирования с правильным исходом с вероятностью еди-

[2)] Если ключ не может быть получен, то его длина формально считается равной нулю.

[3)] Иначе Алиса перед посылкой состояний в канал связи могла бы проверять число фотонов. Если после приготовления состояния обнаружено более одного фотона, то состояние не посылается.

[4)] Роль канала связи выполняет одно и то же оптоволокно. Если по нему передается сильно ослабленное излучение (квантовые состояния), то канал работает как квантовый. Если передается классическая информация обычными телекоммуникационными средствами, то канал работает как классический.

ница. Во-вторых, это невозможность извлечения информации из неортогональных квантовых состояний без их возмущения, что является фактически следствием того, что некоммутирующая пара операторов (наблюдаемых) не может иметь общей системы собственных векторов.

Технические возможности Евы, не противоречащие законам природы, могут быть любыми. Поэтому считается, что Ева имеет:

1) долговременную квантовую память;

2) возможность проводить любые квантовомеханические измерения, включая коллективные (измерения над произвольным числом квантовых состояний) при помощи идеальных регистрирующих устройств (без собственных шумов и с единичной эффективностью);

3) возможность делать неразрушающие измерения для определения числа фотонов в канале связи (только числа фотонов, но не их состояния, последнее противоречит законам квантовой механики);

4) возможность заменить квантовый канал связи с затуханием между Алисой и Бобом на идеальный без затухания[5)].

Сами по себе темновые отсчеты и не единичная квантовая эффективность фотодетекторов у Боба при строго однофотонном источнике и затухании в канале связи не приводят к новым видам атак Евы на передаваемый ключ. Однако при этом возникает ограничение на длину канала связи, до которой возможна передача секретного ключа.

Неоднофотонность источника состояний вместе с затуханием в канале связи даже при идеальных фотодетекторах у Боба приводит к новому классу атак Евы на ключ. Такая атака называется PNS-атакой (Photon Number Splitting Attack) (см. [7–9]).

В реальной ситуации в качестве квазиоднофотонного источника используется сильно ослабленное лазерное излучение, которое представляет собой когерентное состояние $|\mu\rangle$, в котором фиксировано лишь среднее число фотонов μ. Поскольку относительная фаза состояний $|\mu\rangle$ в разных посылках не синхронизирована, в канале связи подслушиватель реально «видит» статистическую смесь с разным числом фотонов,

$$\rho = e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}|n\rangle\langle n|, \tag{3}$$

где $|n\rangle$ — фоковское состояние с числом фотонов n.

Вероятности обнаружить в канале $k = 0, 1, 2\ldots$ и т. д. фотонов, соответственно, равны

$$p_k = e^{-\mu}\frac{\mu^k}{k!}. \tag{4}$$

При малых $\mu = 0.1$–0.3 основную долю составляет вакуумная компонента — отсутствие фотонов в канале. Вероятность присутствия одного фотона в канале есть

$$p_1 = \mu e^{-\mu}, \tag{5}$$

соответственно, вероятность обнаружить в канале два и более фотона равна

$$p_{>1} = 1 - e^{-\mu} - \mu e^{-\mu}. \tag{6}$$

Например, при $\mu = 0.1$ вероятность однофотонной компоненты составляет $p_1 = 0.09$, а вероятность многофотонной компоненты $p_{>1} \approx 0.005$. Основную долю составляет вакуумная компонента $p_{vac} \approx 0.905$. Это означает, что приблизительно в 90 % посылок в канал вообще ничего не поступает.

Квантовая механика допускает неразрушающие и невозмущающие (nondemolition) измерения. Как известно, любое измерение в квантовой механике описывается разложением единицы:

$$I = \sum_{n=0}^{\infty}\mathcal{P}_n, \quad \mathcal{P}_n = |n\rangle\langle n|, \tag{7}$$

где $\mathcal{P}_n$ — измеряющий оператор (в данном случае проектор) на фоковское подпространство с числом фотонов n. После измерения компоненты с k фотонами система остается в том же состоянии:

$$|k\rangle\langle k| = \frac{\mathcal{P}_k\left(|k\rangle\langle k|\right)\mathcal{P}_k}{\mathrm{Tr}\{\mathcal{P}_k\left(|k\rangle\langle k|\right)\mathcal{P}_k\}}. \tag{8}$$

Таким образом, Ева может определить число фотонов в канале связи, не возмущая само квантовое состояние. При этом, например, состояние поляризации, которое отвечает за передаваемый бит, если используется поляризационное кодирование, Ева не узнает, она лишь определяет невозмущающим образом число фотонов.

PNS-атака (атака с расщеплением числа фотонов) сводится к следующему. Ева определяет число фотонов в канале связи в каждой посылке. Если число фотонов равно 1, то Ева блокирует канал

[5)] Напомним, что в квантовой криптографии канал связи между Алисой и Бобом считается открытым. Поэтому Алиса и Боб никак не контролируют канал связи, и считается, что Ева имеет полный доступ к нему и имеет возможность проводить с каналом связи любые технические манипуляции, вплоть до его замены другим каналом связи.

связи. В том случае, если обнаружено более 1 фотона, один фотон Ева оставляет себе в квантовой памяти[6], остальные посылает через свой идеальный квантовый канал связи (или канал с меньшим затуханием, чем исходный) Бобу.

Общее число фотонов, дошедших от Алисы к Бобу в присутствии Евы, остается прежним, поскольку Ева использует канал с меньшим затуханием. Ева начинает делать измерения над своими состояниями в квантовой памяти после раскрытия базисов Бобом. После раскрытия базисов Ева проводит измерения в известном базисе, в случае протокола BB84 после измерений Ева достоверно узнает состояния в каждой посылке при известном базисе, поскольку внутри базиса состояния ортогональны, а значит достоверно различимы.

Начиная с некоторой критической длины канала связи, соответственно, затухания в нем, Ева может блокировать все посылки с однофотонной компонентой. Это возможно, если доля поглощаемых фотонов в канале равна доле однофотонной компоненты. При этом Ева будет иметь полную информацию о передаваемом ключе, не создавая ошибок на приемной стороне и оставаясь незамеченной.

Из приведенных рассуждений видно, что квантовая криптография при квазиоднофотонном источнике и потерях в канале связи может обеспечить секретность ключей лишь до определенной длины линии связи. При длине, большей критической, подслушиватель знает весь передаваемый ключ и остается незамеченным.

Здесь пока не учитывалась неидеальность фотодетекторов на приемной стороне. Ясно, что неидеальность фотодетекторов может лишь уменьшить критическую длину.

2. PNS-АТАКА (АТАКА С РАСЩЕПЛЕНИЕМ ЧИСЛА ФОТОНОВ) НА ПЕРЕДАВАЕМЫЙ КЛЮЧ

2.1. Качественные соображения

Прежде, чем описать протокол и вычисления по определению критической ошибки и длины ключа, изложим саму идею.

Пусть заданы длина L квантового канала связи, потери α в канале, среднее число μ фотонов в лазерном импульсе, эффективности $\eta_{1,2}$ фотодетекторов и собственные темновые шумы в них $p_{1,2}$. Далее, пусть вероятность однофотонной компоненты в импульсе есть

$$n_1 = \mu e^{-\mu}, \tag{9}$$

соответственно, вероятность многофотонной компоненты с числом фотонов более одного есть

$$n_{>1} = 1 - e^{-\mu} - \mu e^{-\mu}, \tag{10}$$

где $e^{-\mu}$ — вероятность вакуумной компоненты.

Доля фотонов, которые достигнут приемной стороны, равна[7]

$$(n_1 + n_{>1})10^{-\alpha L/10}, \tag{11}$$

где коэффициент поглощения для стандартных одномодовых оптических волокон составляет $\alpha = 0.18$–0.2 дБ/км. Вероятность долета фотонов (11) является константой протокола, которая подсчитывается легитимными пользователями заранее перед передачей ключей. Вероятность поглощения в канале связи составляет

$$(n_1 + n_{>1})(1 - 10^{-\alpha L/10}). \tag{12}$$

Этой долей фотонов подслушиватель может манипулировать по своему усмотрению.

Стратегия подслушивателя сводится к следующему. Не изменяя общей вероятности прилета фотонов на приемную сторону (иначе протокол будет прерван легитимными пользователями), подслушиватель может блокировать часть посылок, где в канале присутствует один фотон, а часть однофотонных посылок подслушивателю придется оставить, чтобы не изменить общей вероятности достижения приемной стороны.

Доля однофотонных посылок, которые Ева вынуждена оставить, составляет

$$n_Q = n_1 - (n_1 + n_{>1})(1 - 10^{-\alpha L/10}) = \\ = \mu e^{-\mu} - (1 - e^{-\mu})(1 - 10^{-\alpha L/10}). \tag{13}$$

[6] Строго говоря, из-за бозевского характера частиц и их неразличимости Ева не может с вероятностью единица направить один фотон из многофотонной компоненты себе, остальные Бобу. Например, отведение одного фотона из двухфотонного состояния при помощи симметричного светоделителя возможно лишь с вероятностью 1/2. Ниже для упрощения и консервативно в пользу Евы считаем, что она может оставить в квантовой памяти один фотон из многофотонной компоненты с вероятностью единица.

[7] Пакеты с разным числом фотонов, вообще говоря, имеют разные вероятности поглощения. Вероятность достичь приемной стороны хотя бы одному фотону из k-фотонного пакета равна $1 - p_{loss}^k$ (в режиме линейного поглощения), что больше, чем $1 - p_{loss}$ (p_{loss} — вероятность поглощения одного фотона в линии). Поэтому наша оценка является консервативной в пользу Евы, поскольку число долетевших фотонов меньше, чем в реальной ситуации, и позволяет Еве блокировать бóльшее число однофотонных посылок.

Доля однофотонных посылок, которые Ева блокирует, есть $n_1 - n_Q$. Соответственно, Ева оставляет все многофотонные посылки. Доля таких посылок с учетом (12), (13) равна

$$n_{>1} = 1 - e^{-\mu} - \mu e^{-\mu}. \tag{14}$$

Критическая длина L_c квантового канала связи, при которой доля однофотонной компоненты отлична от нуля и которую Ева вынуждена оставить, определяется из условия

$$L_c = -\frac{10}{\alpha} \log_{10} \left(1 - \frac{\mu e^{-\mu}}{1 - e^{-\mu}} \right). \tag{15}$$

При длине канала, большей критической, Ева может блокировать все однофотонные посылки, а из многофотонных посылок, оставляя одно состояние у себя в квантовой памяти до стадии раскрытия базисов легитимными пользователями, а затем измеряя уже в правильном базисе, может извлечь всю информацию о ключе, не создавая ошибок на приемной стороне. Зависимости критической длины от среднего числа фотонов в импульсе приведены на рис. 1[8)].

Если длина квантового канала связи меньше критической величины, то Ева не может блокировать все однофотонные посылки и вынуждена извлекать информацию о ключе из однофотонных состояний. Ева неизбежно будет производить ошибку на приемной стороне у Боба только за счет измерения и возмущения состояний в однофотонных посылках.

Ранее была построена явная атака для протокола BB84 для идеального строго однофотонного источника [6], достигающая теоретического предела по ошибке. Данная стратегия является оптимальной в том смысле, что подслушиватель извлекает максимум информации о ключе, производя при этом минимально возможную ошибку на приемной стороне.

Все состояния, как однофотонные, так и многофотонные, после своих манипуляций Ева направляет на приемную станцию через свой идеальный (без потерь) канал связи.

Таким образом, ошибка на приемной стороне от действий Евы возникает только для однофотонных посылок, для которых Ева не имеет полной информации о ключе. Для многофотонных состояний каждый передаваемый бит после раскрытия базисов между Алисой и Бобом ей известен.

[8)] Отметим, что критическая длина — не длина секретности для протокола, до которой можно обеспечить передачу секретных ключей. Это длина, при превышении которой уже заведомо нельзя обеспечить секретную передачу ключей при данном среднем числе фотонов μ в импульсе (см. рис. 1).

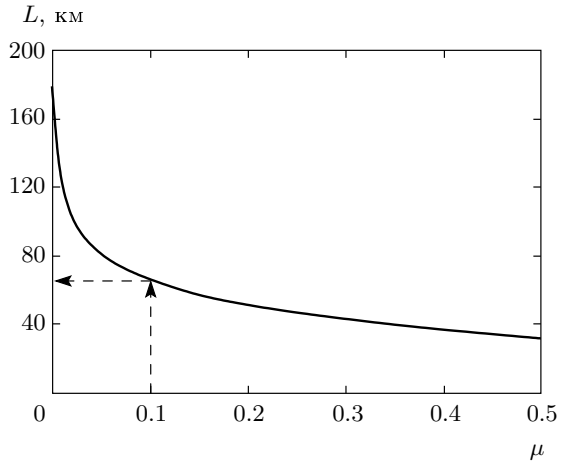

Рис. 1. Критическая длина канала связи в зависимости от среднего числа фотонов в импульсе. Как следует из графика, при ослаблении лазерного излучения до уровня в среднем $\mu = 0.1$ фотонов в импульсе секретная передача ключей через канал связи с затуханием на расстояние, большее 60 км, в принципе невозможна, даже при идеальных фотодетекторах

Наблюдаемая ошибка на приемной стороне, кроме ошибок, производимых Евой, включает в себя также ошибки от темновых отсчетов фотодетекторов.

Дальнейшей нашей задачей является вычисление зависимости между наблюдаемой на приемной стороне и длиной секретного ключа, который может быть получен при остальных фиксированных параметрах системы.

2.2. Действия легитимных пользователей

Приведем сначала протокол действий Алисы и Боба.

1. Алиса случайно и равновероятно выбирает один из двух сопряженных базисов $b = +$ или $b = \times$.

2. В каждом из базисов случайно и равновероятно приготавливается одно из состояний, отвечающих классическим битам 0 или 1 ($i = 0$ или $i = 1$), $|\phi_\mu(b, i)\rangle$ (см. п. 2.4), которое направляется в оптоволоконный канал связи. Данные состояния отвечают ослабленному лазерному излучению со средним числом фотонов μ.

3. Проводится посылка достаточно длинной серии квантовых состояний.

4. На приемной стороне Боб случайно и независимо от Алисы в каждой посылке выбирает базис для измерений (см. п. 2.7).

5. Факт регистрации состояний в каждой посылке сообщается Алисе через открытый классический канал связи, обеспечивающий целостность и аутентичность данных (см., например, подробности о требованиях к классическому каналу связи [10]).

6. После длинной серии измерений Алиса и Боб через открытый классический канал связи сообщают базисы (но не состояния в каждом базисе). Посылки, где базисы не совпадали, отбрасываются.

7. Далее Боб сообщает те посылки, где было зарегистрировано срабатывание двух фотодетекторов сразу (см. п. 2.8). Такие посылки отбрасываются.

8. Далее подсчитывается число фотоотсчетов, которое должно было бы наблюдаться при заданных параметрах системы и длине квантового канала связи и которое затем сравнивается с реальным наблюдаемым числом фотоотсчетов. Если наблюдаемое число отсчетов не выходит за статистическое отклонение с ожидаемым числом фотоотсчетов, то протокол продолжается. В противном случае протокол прерывается. При этом Алиса и Боб имеют по битовой строке — «сырой» (sifted) ключ, — причем битовая строка Боба содержит ошибки.

9. Боб случайно выбирает примерно половину оставшихся фотоотсчетов и раскрывает результаты измерений через открытый классический канал связи. Алиса также раскрывает посланные в этих посылках биты. Алиса и Боб оценивают наблюдаемую вероятность ошибки. Раскрытые позиции отбрасываются (см. п. 2.9).

10. Если вероятность наблюдаемой ошибки меньше критической величины для данных параметров системы и длины квантового канала связи, то Алиса и Боб для оставшихся битовых последовательностей проводят коррекцию ошибок через открытый классический канал связи (см. пп. 2.10, 2.12). После этой стадии Алиса и Боб имеют одинаковые битовые строки — «очищенный» ключ, но еще не секретный ключ.

11. После коррекции ошибок Алиса и Боб проводят усиление секретности [11] (сжатие) «очищенного» ключа при помощи универсальных хэш-функций второго рода [12]. Степень сжатия определяется наблюдаемой вероятностью ошибки и другими параметрами системы (см. п. 2.13). В результате возникают две одинаковые битовые строки у Алисы и Боба, которые являются общим секретным ключом.

2.3. Действия подслушивателя

Поскольку атака Евы на передаваемый ключ строится конструктивно и явно, для удобства дальнейшего изложения приведем также протокол действий подслушивателя.

1. Ева разрывает квантовый канал связи, поскольку вне приемной и передающей станций Алиса и Боб не контролируют оптоволоконную линию.

2. В каждой посылке Ева проводит неразрушающие измерения по определению числа фотонов в линии (см. п. 2.5).

3. Зная, сколько фотонов должно поступить на приемную станцию к Бобу, Ева блокирует часть однофотонных посылок. Для остальной части Ева использует измерения со своим вспомогательным состоянием, которые сводятся к следующему.

3.1. Для тех однофотонных посылок, которые Ева не может блокировать, она готовит свое вспомогательное квантовое состояние, которое приводится во взаимодействие с передаваемым однофотонным состоянием. После взаимодействия передаваемое состояние и состояние Евы оказываются в совместном запутанном состоянии. Свое состояние, модифицированное после взаимодействия, Ева сохраняет в квантовой памяти, а возмущенное состояние Алисы направляет к Бобу через свой идеальный (без потерь) канал связи.

3.2. После раскрытия базисов легитимными пользователями и отбрасывания части посылок Ева также отбрасывает состояния из квантовой памяти для этих посылок. Для оставшихся у нее состояний, которые возникли от взаимодействия с однофотонными состояниями Алисы, Ева проводит коллективные измерения на стадии коррекции ошибок легитимными пользователями, когда Алиса сообщает набор кодовых слов. Данные коллективные измерения строятся с учетом таблицы кодовых слов Алисы и позволяют извлечь максимально возможное количество классической информации из ансамбля квантовых состояний у Евы (см. п. 2.6).

4. Для посылок, в которых обнаружено более одного фотона, Ева оставляет один в квантовой памяти, а остальные направляет через идеальный канал связи к Бобу (см. п. 2.11).

5. После раскрытия базисов Алисой и Бобом Ева проводит индивидуальные измерения над сохраненными у себя в квантовой памяти состояниями в уже известном базисе, что позволяет ей знать каждый бит информации, переданный Алисой для многофотонной доли состояний.

2.4. Приготовление информационных состояний

В протоколе в качестве информационных состояний используются четыре состояния по два состояния в каждом из двух сопряженных базисов, которые будем обозначать как +, ×. Состояния имеют вид в базисе +

$$|\phi(+0)\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle),$$
$$|\phi(+1)\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), \tag{16}$$

в базисе ×

$$|\phi(\times 0)\rangle = \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle),$$
$$|\phi(\times 1)\rangle = \frac{1}{\sqrt{2}}(|1\rangle - i|2\rangle). \tag{17}$$

Это однофотонные состояния, представляющие собой суперпозицию двух локализованных во временных слотах 1 и 2 состояний $|1\rangle$ и $|2\rangle$. Как правило, в оптоволоконной реализации протокола BB84 используется фазовое кодирование (рис. 2), в котором классическим битам 0 или 1 сопоставляется различная относительная фаза двух состояний, локализованных в разных временных окнах.

В канал связи после прохождения передающего интерферометра Маха–Цандера, фазового модулятора и ослабителя (см. рис. 2) поступают состояния вида

$$\rho_\mu(b,i) = \sum_{n=0}^{\infty} \rho^{(n)} = \\ = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |\phi^n(b,i)\rangle\langle\phi^n(b,i)|, \tag{18}$$

где

$$|\phi^n(b,i)\rangle = \mathrm{Sym}\{|\phi(b,i)\rangle^{\otimes n}\}$$

— симметризованное тензорное произведение для n-фотонного состояния. Поскольку относительная фаза когерентных состояний в каждой посылке никак не фиксирована, подслушиватель воспринимает состояние в канале связи как статистический ансамбль, который описывается матрицей плотности (18). Последнее означает, что с вероятностью $e^{-\mu}\mu^n/n!$ в канале присутствуют n идентичных фотонов, каждый из которых находится в квантовом состоянии $|\phi(b,i)\rangle$.

2.5. Неразрушающие измерения подслушивателя для определения числа фотонов в канале связи

Для определения числа фотонов в канале связи подслушиватель использует неразрушающие измерения. Как известно, любое измерение в квантовой механике может быть описано некоторым разложением единицы. Каждому исходу измерения сопоставляется положительный эрмитов оператор, причем их сумма по всем исходам дает единичный оператор. Такое разложение единицы является формализованным описанием измерения и в нашем случае имеет вид

$$I = \sum_{n=0}^{\infty} I_n,$$
$$I_n = \mathcal{P}_n = (|1\rangle\langle 1|)^{\otimes n} + (|2\rangle\langle 2|)^{\otimes n}, \tag{19}$$

где $|1\rangle$ и $|2\rangle$ — базисные состояния (см. (16), (17)), $\mathcal{P}_n$ — проектор на подпространство с числом фотонов n.

Результат измерения над любым состоянием $\rho_\mu^{(n)}$, лежащим только в подпространстве с числом фотонов n, имеет вероятность исхода, равную единице:

$$\mathrm{Tr}\{\mathcal{P}_n \rho_\mu^{(n)} \mathcal{P}_n\} = \mathrm{Tr}\{\rho_\mu^{(n)} \mathcal{P}_n^2\} = \\ = \mathrm{Tr}\{\rho_\mu^{(n)} I_n\} = \mathrm{Tr}\{\rho_\mu^{(n)}\} = 1. \tag{20}$$

Состояние системы после измерения есть

$$\tilde{\rho}_\mu^{(n)} = \frac{\mathcal{P}_n \rho_\mu^{(n)} \mathcal{P}_n}{\mathrm{Tr}\{\mathcal{P}_n \rho_\mu^{(n)} \mathcal{P}_n\}} = \rho_\mu^{(n)}, \tag{21}$$

поскольку $\mathcal{P}_n^2 = \mathcal{P}_n = I_n$ — единичный оператор в подпространстве с числом фотонов n.

Таким образом, подслушиватель может определить число фотонов (но не их состояние) в канале связи.

2.6. Атака подслушивателя на однофотонные состояния

После определения числа фотонов в канале связи Ева блокирует часть однофотонных посылок (см. (13)). Оптимальная атака на однофотонные состояния для протокола BB84 может быть построена явно [6]. Для оставшихся однофотонных посылок Ева использует свою вспомогательную квантовую систему $|A\rangle$ (ancilla), которая некоторое время взаимодействует с передаваемым однофотонным состоянием.

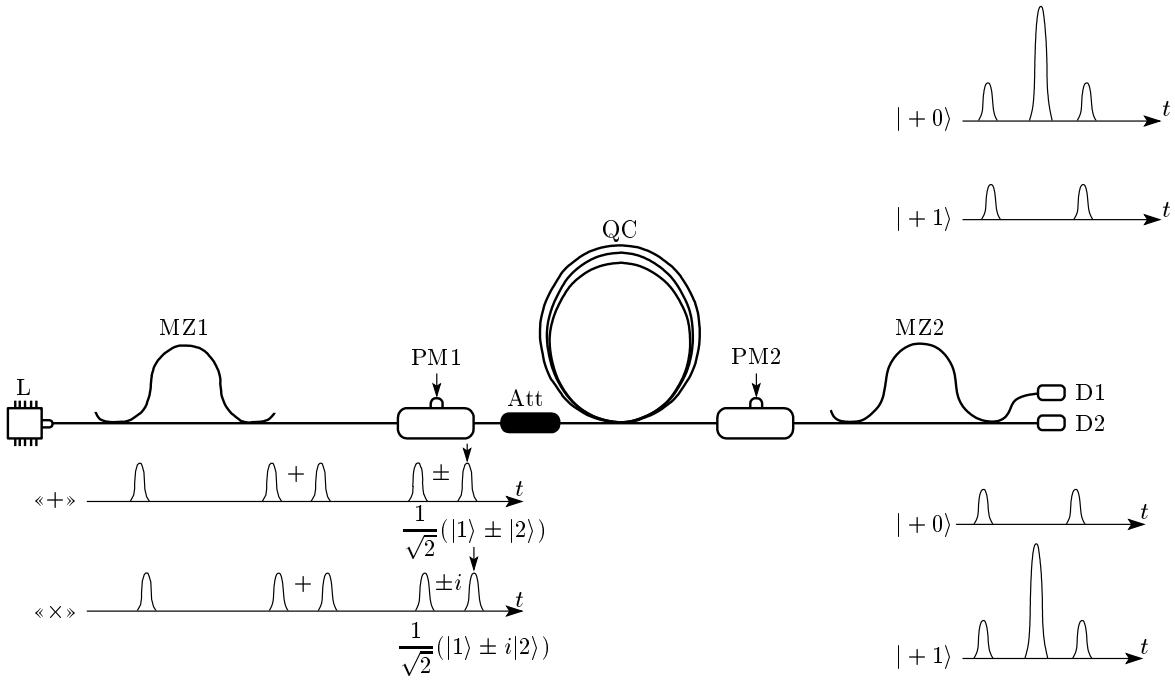

Рис. 2. Схема оптоволоконной системы квантовой криптографии. Обозначения: L — лазер, MZ1, MZ2 — разбалансированные оптоволоконные интерферометры Маха – Цандера на передающей и приемной сторонах, PM1, PM2 — фазовые модуляторы, Att — аттенюатор, QC — оптоволоконный квантовый канал связи, D1, D2 — лавинные фотодетекторы. На выходе интерферометра Маха – Цандера (MZ1) возникает состояние, являющееся суперпозицией двух локализованных по времени состояний («половинок»). Выбор базиса и состояний на приемной стороне осуществляется приложением напряжения на фазовый модулятор (PM1) в момент прохождения задней «половинки». На выходе MZ1 формируется одно из четырех информационных состояний $|\phi(b,i)\rangle$. После прохождения аттенюатора (Att) состояние ослабляется до квазиоднофотонного уровня. На приемной стороне выбор базиса проводится также посредством приложения напряжения в момент прохождения задней «половинки» квантового состояния. Окончательное преобразование состояния осуществляется при помощи интерферометра Маха – Цандера (MZ2). Например, максимум интерференционной картины от состояния $|\phi(+0)\rangle$ возникает в центральном временном слоте на входе фотодетектора D1, а на входе фотодетектора D2 отсчетов вообще не возникает. Для состояния $|\phi(+1)\rangle$ ситуация обратная, максимум — на входе фотодетектора D2, минимум — на входе D1. Для состояний в базисе $\times$ интерференционная картина противоположная. Максимум интерференционной картины от состояния $|\phi(\times 0)\rangle$ имеет место на выходе D2, для состояния $|\phi(\times 1)\rangle$ — на фотодетекторе D1

Взаимодействие вспомогательной системы и передаваемого состояния описывается унитарным оператором U_{EB}, который Ева задает по своему усмотрению. После взаимодействия состояние Алисы и ancilla оказываются, вообще говоря, в запутанном (не факторизованном) состоянии. Возмущенное состояние Алисы направляется к Бобу, а ancilla остается у Евы.

Для полного описания унитарного оператора U_{EB} достаточно выяснить его действие на базисные состояния $|1\rangle$, $|2\rangle$. Имеем

$$U_{EB}(|1\rangle \otimes |A\rangle) = |\Psi_1\rangle = |\phi_1\rangle \otimes |1\rangle + |\theta_1\rangle \otimes |2\rangle, \quad (22)$$

$$U_{EB}(|2\rangle \otimes |A\rangle) = |\Psi_2\rangle = |\varphi_2\rangle \otimes |1\rangle + |\phi_2\rangle \otimes |2\rangle. \quad (23)$$

Унитарность требует сохранения нормировки для каждого состояния и углов между ними:

$$\langle \Psi_i | \Psi_j \rangle = \delta_{ij}, \quad i,j = 1,2,3. \quad (24)$$

Информационные состояния преобразуются следующим образом. В базисе + имеем

$$U_{EB}(|\phi(+0)\rangle \otimes |A\rangle) = |\Psi_{EB}(+0)\rangle = \\ = |\phi(+0)\rangle \otimes \frac{|\Phi_+^+\rangle + |\Theta_+^+\rangle}{2} + \\ + |\phi(+1)\rangle \otimes \frac{|\Phi_+^-\rangle - |\Theta_+^-\rangle}{2}, \quad (25)$$

$$U_{EB}(|\phi(+1)\rangle\otimes|A\rangle)=|\Psi_{EB}(+1)\rangle=$$
$$=|\phi(+1)\rangle\otimes\frac{|\Phi_+^+\rangle-|\Theta_+^+\rangle}{2}+$$
$$+|\phi(+0)\rangle\otimes\frac{|\Phi_+^-\rangle+|\Theta_+^-\rangle}{2}. \quad (26)$$

Для базиса $\times$ получаем

$$U_{EB}(|\phi(\times0)\rangle\otimes|A\rangle)=|\Psi_{EB}(\times0)\rangle=$$
$$=|\phi(\times0)\rangle\otimes\frac{|\Phi_\times^+\rangle+|\Theta_\times^+\rangle}{2}+$$
$$+|\phi(\times1)\rangle\otimes\frac{|\Phi_\times^-\rangle-|\Theta_\times^-\rangle}{2}, \quad (27)$$

$$U_{EB}(|\phi(\times1)\rangle\otimes|A\rangle)=|\Psi_{EB}(\times1)\rangle=$$
$$=|\phi(\times1)\rangle\otimes\frac{|\Phi_\times^+\rangle-|\Theta_\times^+\rangle}{2}+$$
$$+|\phi(\times0)\rangle\otimes\frac{|\Phi_\times^-\rangle+|\Theta_\times^-\rangle}{2}. \quad (28)$$

Квантовые состояния, введенные в формулах (25)–(28), связаны с исходными (22)–(23) следующими соотношениями:

$$|\Phi_+^\pm\rangle=|\phi_1\rangle\pm|\phi_2\rangle,\quad |\Theta_+^\pm\rangle=|\theta_1\rangle\pm|\varphi_2\rangle, \quad (29)$$

$$|\Phi_\times^\pm\rangle=|\phi_1\rangle\pm i|\phi_2\rangle,\quad |\Theta_\times^\pm\rangle=|\theta_1\rangle\pm i|\varphi_2\rangle. \quad (30)$$

Для дальнейшего анализа важную роль играют соображения симметрии. Всегда можно выбрать размерность пространства состояний для $|A\rangle$ так, чтобы состояния $|\phi_i\rangle$, $|\theta_i\rangle$ и $|\varphi\rangle$ лежали во взаимно ортогональных подпространствах.

После вторжения Евы в канал связи состояния, которые доступны для измерений Боба на приемной стороне, описываются матрицами плотности, которые получаются взятием частичного следа по пространству состояний Евы. Имеем в базисе $\times$

$$\rho_B(+0)=\mathrm{Tr}\{|\Psi_{EB}(+0)\rangle\langle\Psi_{EB}(+0)|\}=$$
$$=|\phi(+0)\rangle\langle\phi(+0)|\frac{\langle\Phi_+^+|\Phi_+^+\rangle+\langle\Theta_+^+|\Theta_+^+\rangle}{4}+$$
$$+|\phi(+1)\rangle\langle\phi(+1)|\frac{\langle\Phi_+^-|\Phi_+^-\rangle+\langle\Theta_+^-|\Theta_+^-\rangle}{4}, \quad (31)$$

$$\rho_B(+1)=\mathrm{Tr}\{|\Psi_{EB}(+1)\rangle\langle\Psi_{EB}(+1)|\}=$$
$$=|\phi(+1)\rangle\langle\phi(+1)|\frac{\langle\Phi_+^+|\Phi_+^+\rangle+\langle\Theta_+^+|\Theta_+^+\rangle}{4}+$$
$$+|\phi(+0)\rangle\langle\phi(+0)|\frac{\langle\Phi_+^-|\Phi_+^-\rangle+\langle\Theta_+^-|\Theta_+^-\rangle}{4}. \quad (32)$$

Аналогично для состояний в базисе $\times$ получаем

$$\rho_B(\times0)=\mathrm{Tr}\{|\Psi_{EB}(\times0)\rangle\langle\Psi_{EB}(\times0)|\}=$$
$$=|\phi(\times0)\rangle\langle\phi(\times0)|\frac{\langle\Phi_\times^+|\Phi_\times^+\rangle+\langle\Theta_\times^+|\Theta_\times^+\rangle}{4}+$$
$$+|\phi(\times1)\rangle\langle\phi(\times1)|\frac{\langle\Phi_\times^-|\Phi_\times^-\rangle+\langle\Theta_\times^-|\Theta_\times^-\rangle}{4}, \quad (33)$$

$$\rho_B(\times1)=\mathrm{Tr}\{|\Psi_{EB}(\times1)\rangle\langle\Psi_{EB}(\times1)|\}=$$
$$=|\phi(\times1)\rangle\langle\phi(\times1)|\frac{\langle\Phi_\times^+|\Phi_\times^+\rangle+\langle\Theta_\times^+|\Theta_\times^+\rangle}{4}+$$
$$+|\phi(\times0)\rangle\langle\phi(\times0)|\frac{\langle\Phi_\times^-|\Phi_\times^-\rangle+\langle\Theta_\times^-|\Theta_\times^-\rangle}{4}. \quad (34)$$

Поскольку базисы $+$ и $\times$ выбираются случайно и равновероятно, требование симметрии диктует, что ошибка, производимая Евой на приемной стороне, не должна зависеть от выбора базиса, т. е. должна быть одинаковой в разных базисах. Кроме того, условие унитарности U_{EB} фактически сводится к сохранению нормировки и углов между $|\phi(+0)\rangle$, $|\phi(\times0)\rangle$, $|\phi(+1)\rangle$ и $|\phi(\times1)\rangle$, что приводит к условиям: в базисе $+$

$$\begin{aligned}&\langle\Phi_+^+|\Phi_+^-\rangle+\langle\Theta_+^+|\Theta_+^-\rangle=0,\\ &\langle\Phi_+^+|\Phi_+^-\rangle-\langle\Theta_+^+|\Theta_+^-\rangle=0\end{aligned} \quad (35)$$

и в базисе $\times$

$$\begin{aligned}&\langle\Phi_\times^+|\Phi_\times^-\rangle+\langle\Theta_\times^+|\Theta_\times^-\rangle=0,\\ &\langle\Phi_\times^+|\Phi_\times^-\rangle-\langle\Theta_\times^+|\Theta_\times^-\rangle=0.\end{aligned} \quad (36)$$

Вероятность ошибки Q на приемной стороне у Боба дается коэффициентом при $|1_+\rangle$, когда Алисой было послано состояние $|0_+\rangle$ в базисе $+$. Аналогично для единицы в базисе $\times$. Равенство ошибок в разных базисах с учетом соотношений (31)–(36) дает

$$Q=\frac{\langle\Phi_+^-|\Phi_+^-\rangle+\langle\Theta_+^-|\Theta_+^-\rangle}{4}=$$
$$=\frac{\langle\Phi_\times^-|\Phi_\times^-\rangle+\langle\Theta_\times^-|\Theta_\times^-\rangle}{4}. \quad (37)$$

Соответственно, вероятность правильного отсчета у Боба равна

$$1-Q=\frac{\langle\Phi_+^+|\Phi_+^+\rangle+\langle\Theta_+^+|\Theta_+^+\rangle}{4}=$$
$$=\frac{\langle\Phi_\times^+|\Phi_\times^+\rangle+\langle\Theta_\times^+|\Theta_\times^+\rangle}{4}. \quad (38)$$

Упомянутые выше условия удовлетворяются, если модифицированные состояния Евы после взаимодействия $|A\rangle$ с состоянием Алисы выбрать в виде (см. также [13])

$$|\phi_1\rangle = \sqrt{1-Q}|x\rangle \otimes |x\rangle,$$
$$|\phi_2\rangle = \sqrt{1-Q}(\cos\alpha|x\rangle \otimes |x\rangle + \sin\alpha|y\rangle \otimes |x\rangle), \quad (39)$$

$$|\theta_1\rangle = \sqrt{Q}|x\rangle \otimes |y\rangle,$$
$$|\varphi_2\rangle = \sqrt{Q}(\cos\alpha|x\rangle \otimes |y\rangle + \sin\alpha|y\rangle \otimes |y\rangle). \quad (40)$$

Здесь $|i\rangle \otimes |j\rangle$ $(i,j = x,y)$ — ортогональные нормированные базисные состояния в пространстве состояний ancilla у Евы. С учетом требований симметрии унитарный оператор, задаваемый Евой, однозначно параметризуется двумя параметрами Q, α. Угол α Ева должна выбрать так, чтобы максимизировать свою информацию о ключе при условии, что на приемной стороне у Боба будет наблюдаемый процент ошибок Q.

С учетом соотношений (31)–(40) матрица плотности на приемной стороне у Боба принимает вид (в базисе +)

$$\rho_B(+0) = (1-Q)|\phi(+0)\rangle\langle\phi(+0)| + Q|\phi(+1)\rangle\langle\phi(+1)|, \quad (41)$$

$$\rho_B(+1) = (1-Q)|\phi(+1)\rangle\langle\phi(+1)| + Q|\phi(+0)\rangle\langle\phi(+0)|, \quad (42)$$

аналогично для 0 и 1 в базисе $\times$ получаем

$$\rho_B(\times 0) = (1-Q)|\phi(\times 0)\rangle\langle\phi(\times 0)| + Q|\phi(\times 1)\rangle\langle\phi(\times 1)|, \quad (43)$$

$$\rho_B(\times 1) = (1-Q)|\phi(\times 1)\rangle\langle\phi(\times 1)| + Q|\phi(\times 0)\rangle\langle\phi(\times 0)|. \quad (44)$$

Связь между наблюдаемой у Боба вероятностью ошибки Q и параметром α дается соотношением[9)]

$$Q = \frac{1-\cos\alpha}{2}. \quad (45)$$

До раскрытия базисов Ева не проводит никаких измерений и сохраняет свои состояния в квантовой памяти.

[9)] Далее будет видно, что величина Q играет роль ошибки на приемной стороне только в случае идеальных фотодетекторов. Для не идеальных фотодетекторов наблюдаемая ошибка отличается от Q.

Состояния Евы находятся взятием частичного следа по пространству состояний Боба. Если в базисе + Алисой был послан 0, то состояние Евы при этом будет

$$\rho_E(+0) = \frac{(|\Phi_+^+\rangle + |\Theta_+^+\rangle)(\langle\Phi_+^+| + \langle\Theta_+^+|)}{4} + \frac{(|\Phi_+^-\rangle - |\Theta_+^-\rangle)(\langle\Phi_+^-| - \langle\Theta_+^-|)}{4}, \quad (46)$$

аналогично для случая, когда Алисой была послана 1 в базисе +, имеем

$$\rho_E(+1) = \frac{(|\Phi_+^+\rangle - |\Theta_+^+\rangle)(\langle\Phi_+^+| - \langle\Theta_+^+|)}{4} + \frac{(|\Phi_+^-\rangle + |\Theta_+^-\rangle)(\langle\Phi_+^-| + \langle\Theta_+^-|)}{4}. \quad (47)$$

Для посылок в базисе $\times$ находим

$$\rho_E(\times 0) = \frac{(|\Phi_\times^+\rangle + |\Theta_\times^+\rangle)(\langle\Phi_\times^+| + \langle\Theta_\times^+|)}{4} + \frac{(|\Phi_\times^+\rangle - |\Theta_\times^+\rangle)(\langle\Phi_\times^+| - \langle\Theta_\times^+|)}{4}, \quad (48)$$

аналогично для случая, когда Алисой была послана 1 в базисе $\times$, имеем

$$\rho_E(\times 1) = \frac{(|\Phi_\times^+\rangle - |\Theta_\times^+\rangle)(\langle\Phi_\times^+| - \langle\Theta_\times^+|)}{4} + \frac{(|\Phi_\times^+\rangle + |\Theta_\times^+\rangle)(\langle\Phi_\times^+| + \langle\Theta_\times^+|)}{4}. \quad (49)$$

2.7. Измерения на приемной стороне

Обсудим измерения на приемной стороне. В реальной ситуации в качестве фотодетекторов используют, как правило, лавинные фотодиоды, которые работают в стробируемом режиме. Регистрируемый фотон рождает электрон-дырочную пару, которая затем рождает лавину носителей, импульс тока от которой регистрируется электронной схемой. Для нас будет существенно то, что лавинные фотодетекторы не различают число фотонов в импульсе. Из общих соображений можно думать, что вероятность регистрации пакетов, состоящих из разного числа одинаковых фотонов тем больше, чем больше число фотонов. По крайней мере, вероятность является растущей функцией числа фотонов в пакете. Использование того факта, что вероятность регистрации зависит от числа фотонов в пакете, наделяет фотодетекторы свойством различать (пусть даже частично) число фотонов в пакете. Для того чтобы

не привлекать какие-то модельные соображения, которые играют в пользу легитимного пользователя на приемной стороне, будем консервативно считать, что вероятность регистрации пакетов с разным числом фотонов в одинаковом состоянии не зависит от числа фотонов в пакете.

Другими словами, будем считать, что вероятности регистрации однофотонной и многофотонной компонент лазерного излучения (когерентного состояния) одинаковы и определяются лишь вероятностью самого присутствия однофотонной или многофотонной компоненты в квантовом состоянии. С точки зрения криптографии, такая модель является консервативной в пользу подслушивателя в том смысле, что не улучшает технические возможности легитимных пользователей по сравнению с существующим технологическим уровнем.

Боб на приемной стороне использует измерение в двух сопряженных базисах, которые он выбирает случайно и независимо от Алисы в каждой посылке. Технически выбор базисов осуществляется подачей соответствующего напряжения на фазовый модулятор на приемной станции (см. рис. 2).

Формальное описание любого квантовомеханического измерения (в нашем случае идеальных фотодетекторов с квантовой эффективностью единица и нулевыми темновыми отсчетами) задается разложением единицы.

Измерение в базисе + описывается разложением единицы

$$I=\sum_{n=0}^{\infty}\left(|\phi^n(+0)\rangle\langle\phi^n(+0)|+\right.$$

$$\left.+\,|\phi^n(+1)\rangle\langle\phi^n(+1)|\right), \quad (50)$$

а в базисе × разложением

$$I=\sum_{n=0}^{\infty}\left(|\phi^n(\times 0)\rangle\langle\phi^n(\times 0)|+\right.$$

$$\left.+\,|\phi^n(\times 1)\rangle\langle\phi^n(\times 1)|\right). \quad (51)$$

После передачи всей последовательности происходит согласование базисов между Алисой и Бобом через открытый классический канал связи. Посылки, в которых базисы не совпадали, отбрасываются. Вероятность получения результатов в совпадающих базисах для однофотонной компоненты в случае идеальных фотодетекторов есть

$$\begin{aligned}\Pr(0|0)&=\mathrm{Tr}\{\rho_B(+0)|\phi(+0)\rangle\langle\phi(+0)|\}=\\&=\mathrm{Tr}\{\rho_B(\times 0)|\phi(\times 0)\rangle\langle\phi(\times 0)|\}=\\&=\Pr(1|1)=\mathrm{Tr}\{\rho_B(+1)|\phi(+1)\rangle\langle\phi(+1)|\}=\\&=\mathrm{Tr}\{\rho_B(\times 1)|\phi(\times 1)\rangle\langle\phi(\times 1)|\}=1-Q, \quad (52)\end{aligned}$$

$$\begin{aligned}\Pr(0|1)&=\mathrm{Tr}\{\rho_B(+0)|\phi(+1)\rangle\langle\phi(+1)|\}=\\&=\mathrm{Tr}\{\rho_B(\times 0)|\phi(\times 1)\rangle\langle\phi(\times 1)|\}=\\&=\Pr(1|0)=\mathrm{Tr}\{\rho_B(+1)|\phi(+0)\rangle\langle\phi(+0)|\}=\\&=\mathrm{Tr}\{\rho_B(\times 1)|\phi(\times 0)\rangle\langle\phi(\times 0)|\}=Q. \quad (53)\end{aligned}$$

Здесь $\Pr(i|j)$ — условная вероятность того, что Алисой был послан бит i, а Боб интерпретировал результат как бит j; как видно, в случае идеальных фотодетекторов параметр Q представляет собой вероятность ошибки у Боба при регистрации однофотонных состояний после их возмущения подслушивателем.

2.8. Подсчет наблюдаемого числа фотоотсчетов на приемной стороне

Учтем теперь неидеальность фотодетекторов. Для упрощения дальнейших вычислений будет удобно считать, что фотодетекторы являются идеальными и измерения описываются разложениями единицы (50), (51), а неидеальности детекторов удобно учесть прямо в матрице плотности, которая описывает состояние, приходящее на идеальные детекторы. Такой прием является формальным и не изменяет условные вероятности, поэтому такое описание эквивалентно описанию с исходной матрицей плотности и неидеальными детекторами.

Рассмотрим модификацию матрицы плотности, поступающую на фотодетекторы. Пусть базисы Алисы и Боба согласованы. Пусть Алиса посылает состояние +0 (см. (16)) и Боб проводит измерения в базисе +. Технически всегда к моменту прихода состояния независимо от выбора базиса стробируются (активируются) оба фотодетектора 1 и 2 (см. рис. 2).

Пусть квантовые эффективности фотодетекторов равны η_1, η_2 и вероятности темновых отсчетов во временном окне стробирования — соответственно p_1, p_2.

Множества различных событий фотоотсчетов удобно представить в виде диаграмм (рис. 3). Имеются следующие множества различных событий при регистрации возмущенного Евой состояния +0 в детекторах 1 и 2 в одном временном окне стробирования:

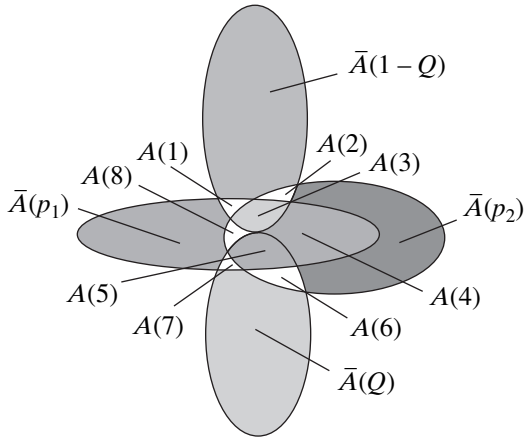

Рис. 3. Различные множества событий фотоотсчетов для состояния $+0$

$A(1-Q)$ — отсчет в детекторе 1 от состояния (41), правильный отсчет $0 \to 0$;
$\overline{A}(1-Q)$ — отсчет только в детекторе 1 (см. рис. 3);
$A(Q)$ — отсчет в детекторе 2 от состояния (41), ошибочный отсчет $0 \to 1$;
$\overline{A}(Q)$ — отсчет только в детекторе 2 (см. рис. 3);
$A(p_1)$ — темновые отсчеты в детекторе 1, имеют место независимо от прихода состояния;
$\overline{A}(p_1)$ — темновые отсчеты только в детекторе 1 (см. рис. 3);
$A(p_2)$ — темновые отсчеты в детекторе 2, имеют место независимо от прихода состояния;
$\overline{A}(p_2)$ — темновые отсчеты только в детекторе 2 (см. рис. 3);
$A(1)$ — одновременные отсчеты в одном и том же временном окне стробирования в детекторе 1 от прихода состояния и темнового отсчета (воспринимается как один отсчет, так как фотодетектор не различает число фотонов);
$A(2)$ — одновременные отсчеты в одном и том же временном окне стробирования в детекторе 1 от прихода состояния, и детекторе 2 от темнового отсчета (воспринимаются как два отсчета в разных детекторах);
$A(3)$ — одновременные отсчеты в одном и том же временном окне стробирования в детекторе 1 от прихода состояния и темнового отсчета, и в детекторе 2 от темнового отсчета (воспринимаются как два отсчета в фотодетекторах 1 и 2);
$A(4)$ и $A(8)$ — одновременные отсчеты в одном и том же временном окне стробирования в детекторе 1, и в детекторе 2 от темновых отсчетов (воспринимаются как два отсчета в фотодетекторах 1 и 2);
$A(5)$ — одновременные отсчеты в одном и том же временном окне стробирования в детекторе 2 от прихода состояния и темнового отсчета, и в детекторе 1 от темнового отсчета (воспринимаются как два отсчета в фотодетекторах 1 и 2);
$A(6)$ — одновременные отсчеты в одном и том же временном окне стробирования в детекторе 2 прихода состояния и темнового отсчета (воспринимается как один отсчет, так как фотодетектор не различает число фотонов);
$A(7)$ — одновременные отсчеты в одном и том же временном окне стробирования в детекторе 2 от прихода состояния и темнового отсчета (воспринимается как один отсчет, так как фотодетектор не различает число фотонов);
$A(8)$ — одновременные темновые отсчеты в одном и том же временном окне стробирования в детекторах 1 и 2 (воспринимаются как два отсчета).

Отметим, что два множества событий $A(1-Q) \cap \cap A(Q) = \emptyset$ не перекрываются (не может быть одновременных отсчетов от однофотонного состояния в двух детекторах).

Согласно протоколу (п. 2.2), посылки, где наблюдаются отсчеты одновременно в детекторах 1 и 2, отбрасываются.

Множество отсчетов в детекторе 1 от возмущенного Евой однофотонного состояния $+0$ и темновых отсчетов есть объединения следующих множеств событий (см. рис. 3):

$$\overline{A}(1-Q) \cup \overline{A}(p_1) \cup A(1), \tag{54}$$

аналогично для множества отсчетов в детекторе 2 имеем

$$\overline{A}(Q) \cup \overline{A}(p_2) \cup A(6). \tag{55}$$

Введем более компактные обозначения. Вероятности событий (54) и (55) соответственно равны

$$\begin{aligned}\mathcal{F}(+0) &= \Pr\{\overline{A}(1-Q) \cup \overline{A}(p_1) \cup A(1)\} = \\ &= (1-Q)\eta_1(n_Q)(1-p_2) + p_1(1-p_2) - \\ &-(1-Q)\eta_1(n_Q)p_1(1-p_2) - Q\eta_2(n_Q)p_1(1-p_2),\end{aligned} \tag{56}$$

$$\begin{aligned}\mathcal{D}(+0) &= \Pr\{\overline{A}(Q) \cup \overline{A}(p_2) \cup A(6)\} = \\ &= Q\eta_2(n_Q)(1-p_1) + p_2(1-p_1) - Q\eta_2(n_Q)p_2(1-p_1) - \\ &- (1-Q)\eta_1(n_Q)p_2(1-p_1).\end{aligned} \tag{57}$$

Подсчет вероятностей детектирования для остальных состояний проводится аналогично предыдущему. При этом нужно учесть, что состояние $+1$ ($|\phi(+1)\rangle$) в отличие от состояния $+0$ ($|\phi(+0)\rangle$), изображенного на рис. 2, дает максимум интерференционной картины на фотодетекторе D2.

Интерференционная картина от состояний в базисе $\times$ является обратной по отношению к интерференционной картине для состояний в базисе $+$. Максимум от состояния $\times 1$ ($|\phi(\times 1)\rangle$) наблюдается на фотодетекторе D1, а максимум от состояния $\times 0$ ($|\phi(\times 0)\rangle$) — на фотодетекторе D2.

Поэтому достаточно провести вычисления для состояний $+0$, для остальных состояний выражения получаются соответствующей заменой индексов. Симметрия протокола и техническая реализация приводят к тому, что имеют место соотношения

$$\mathcal{F}(+0) = \mathcal{F}(\times 1), \tag{58}$$

$$\mathcal{F}(\times 0) = \mathcal{F}(+1) = (1-Q)\eta_2(n_Q)(1-p_1) + p_2(1-p_1) - (1-Q)\eta_2(n_Q)p_2(1-p_1) - Q\eta_1(n_Q)p_2(1-p_1), \tag{59}$$

$$\mathcal{D}(+0) = \mathcal{D}(\times 1), \tag{60}$$

$$\mathcal{D}(+1) = \mathcal{D}(\times 0) = Q\eta_2(n_Q)(1-p_1) + p_2(1-p_1) - Q\eta_2(n_Q)p_2(1-p_1) - (1-Q)\eta_1(n_Q)p_2(1-p_1). \tag{61}$$

Здесь введены обозначения $\eta_{1,2}(n_Q) = \eta_{1,2}n_Q$.

Запишем теперь матрицу плотности (пока не нормированную) состояния, искаженного подслушивателем и темновыми отсчетами, поступающего на идеальные фотодетекторы:

$$\rho_B(+0) = \mathcal{F}(+0)|\phi(+0)\rangle\langle\phi+0| + \mathcal{D}(+0)|\phi(+1)\rangle\langle\phi+1|, \tag{62}$$

$$\rho_B(+1) = \mathcal{F}(+1)|\phi(+1)\rangle\langle\phi+1| + \mathcal{D}(+1)|\phi(+0)\rangle\langle\phi+0|, \tag{63}$$

$$\rho_B(\times 0) = \mathcal{F}(\times 0)|\phi(\times 0)\rangle\langle\phi\times 0| + \mathcal{D}(\times 0)|\phi(\times 1)\rangle\langle\phi\times 1|, \tag{64}$$

$$\rho_B(\times 1) = \mathcal{F}(\times 1)|\phi(\times 1)\rangle\langle\phi\times 1| + \mathcal{D}(\times 0)|\phi(\times 0)\rangle\langle\phi\times 0|. \tag{65}$$

Таким образом, вероятность правильной регистрации однофотонной компоненты есть

$$1 - Q_1(Q) = \frac{\sum_{b=+,\times;i=0,1}\mathcal{F}(bi)}{\sum_{b=+,\times;i=0,1}(\mathcal{F}(bi)+\mathcal{D}(bi))} = \frac{(1-Q)\eta(n_Q) - (1-Q)(\eta_1(n_Q)p_1 + \eta_2(n_Q)p_2) + \eta(n_Q)p_1p_2 - (\eta_1(n_Q)p_2 + \eta_2(n_Q)p_1) + p_{dark} - 2p_1p_2}{\eta(n_Q) - (\eta_1(n_Q)p_1 + \eta_2(n_Q)p_2) - 2(\eta_1(n_Q)p_2 + \eta_2(n_Q)p_1) + 2p_{dark} + 2\eta(n_Q)p_1p_2 - 4p_1p_2}, \tag{66}$$

соответственно, вероятность неправильной регистрации однофотонной компоненты есть

$$Q_B(Q) = \frac{\sum_{b=+,\times;i=0,1}\mathcal{D}(bi)}{\sum_{b=+,\times;i=0,1}(\mathcal{F}(bi)+\mathcal{D}(bi))} = \frac{Q\eta(n_Q) - Q(\eta_1(n_Q)p_1 + \eta_2(n_Q)p_2) + \eta(n_Q)p_1p_2 - (\eta_1(n_Q)p_2 + \eta_2(n_Q)p_1) + p_{dark} - 2p_1p_2}{\eta(n_Q) - (\eta_1(n_Q)p_1 + \eta_2(n_Q)p_2) - 2(\eta_1(n_Q)p_2 + \eta_2(n_Q)p_1) + 2p_{dark} + 2\eta(n_Q)p_1p_2 - 4p_1p_2}, \tag{67}$$

где $\eta(n_Q) = (\eta_1 + \eta_2)n_Q$, $p_{dark} = p_1 + p_2$.

2.9. Наблюдаемая ошибка на приемной стороне

Подсчитаем теперь наблюдаемую ошибку на приемной стороне.

Ошибка от возмущения подслушивателем однофотонных состояний приводит к ошибке (62). Состояния, происходящие из многофотонной компоненты, поступают на приемную сторону без возмущений. Такие невозмущенные состояния на приемной стороне выглядят как состояния (67), но с $Q = 0$. Результирующая наблюдаемая ошибка $\tilde{Q}(Q)$ на приемной стороне с учетом вероятностей однофотонной (13) и многофотонной (14) компонент равна

$$\tilde{Q}(Q) = Q_Q(Q) + Q_{>1}(Q=0) + Q_{dark}(Q), \tag{68}$$

$$Q_Q(Q) = \frac{1}{\Sigma} \times \times \{Q\eta(n_Q) - Q(\eta_1(n_Q)p_1 + \eta_2(n_Q)p_2)\}, \tag{69}$$

$$Q_{>1}(Q) = \frac{1}{\Sigma} \times \\ \times \{Q\eta(n_1) - Q(\eta_1(n_1)p_1 + \eta_2(n_1)p_2)\}, \quad (70)$$

$$Q_{dark}(Q) = \frac{1}{\Sigma}\{p_{dark} - 2p_1p_2 + \eta(n_{1,Q})p_1p_2 - \\ - Q(\eta_1(n_Q)p_1 + \eta_2(n_Q)p_2) - \\ - (\eta_1(n_{1,Q})p_2 + \eta_2(n_{1,Q})p_1)\}. \quad (71)$$

Здесь

$$\Sigma = \eta(n_{1,Q}) - (\eta_1(n_{1,Q})p_1 + \eta_2(n_{1,Q})p_2) - \\ - 2(\eta_1(n_{1,Q})p_2 + \eta_2(n_{1,Q})p_1) + 2p_{dark} + \\ + 2\eta(n_{1,Q})p_1p_2 - 4p_1p_2, \quad (72)$$

$$\eta(n_{1,Q}) = \eta(n_Q + n_{>1}), \quad \eta_{1,2}(n_Q) = \eta_{1,2}n_Q,$$

$$\eta_{1,2}(n_1) = \eta_{1,2}n_{>1}, \quad \eta_{1,2}(n_{1,Q}) = \eta_{1,2}(n_Q + n_{>1}).$$

В формулах (68)–(71) учтено также, что два множества событий — отсчеты от однофотонной компоненты и отсчеты от многофотонной компоненты — не пересекаются.

Ошибка на приемной стороне принимает простое выражение в отсутствие темновых отсчетов:

$$\tilde{Q}(Q) = Q\frac{n_Q}{n_Q + n_{>1}} + 0\frac{n_{>1}}{n_Q + n_{>1}}. \quad (73)$$

Первое слагаемое отвечает за ошибки при детектировании возмущенных подслушивателем однофотонных состояний, второе — за ошибки от невозмущенных состояний. Для этих состояний ошибка при детектировании возникает только за счет неидеальности фотодетекторов.

Переменная Q теперь становится внутренним параметром задачи, который подслушиватель может задавать по своему выбору. Данный параметр фактически определяется выбором унитарного оператора Евы (22), (23). Поскольку Ева не может контролировать фотодетекторы на приемной стороне (изменять их эффективность и темновые шумы), цель Евы сводится к тому, чтобы извлечь максимум информации, который допускается законами квантовой механики, из ансамбля своих вспомогательных квантовых состояний (46)–(49) при данной наблюдаемой ошибке $\tilde{Q}(Q)$ на приемной стороне. Классическая информация из квантовых состояний извлекается при помощи измерений. Цель подслушивателя состоит в оптимальном различении квантовых состояний (46)–(49), хранящихся в квантовой памяти.

После измерений на приемной станции, согласования базисов, оценки вероятности наблюдаемой ошибки и отбрасывания раскрытых позиций, Алиса и Боб имеют битовые строки длины n. Причем строка Боба — «сырой» ключ — содержит ошибки.

Подслушиватель имеет регистр квантовой памяти с состояниями (46)–(49),

$$\rho_E(b_1i_1) \otimes \rho_E(b_2i_2) \otimes \ldots \otimes \rho_E(b_ni_n). \quad (74)$$

В каждой позиции Ева знает, к какому базису относится состояние (индекс b_k), хотя само состояние ей не известно. Поэтому Еве требуется только различить состояния (46) и (47) или состояния (48) и (49). Поскольку матрицы плотности состояний Евы, даже относящиеся к одному базису, не коммутируют, Ева не может достоверно различить эти состояния и, соответственно, достоверно узнать, что было послано, 0 или 1. Ева может делать индивидуальные измерения над каждым состоянием в регистре отдельно, выбрав при этом такое измерение, которое минимизирует ошибку различения отдельных пар состояний. Однако этот способ не самый лучший. Квантовая механика не запрещает делать коллективные измерения сразу над всем регистром состояний. Оказывается, что при таком способе подслушиватель может извлечь больше классической информации (грубо говоря, узнать большее число бит). Такие измерения Ева должна делать в самом конце протокола, после того, как Алиса и Боб исправят ошибки, обмениваясь вспомогательной классической информацией через открытый канал связи. При построении своих измерений Ева использует информацию, выданную через открытый канал при коррекции ошибок.

2.10. Коррекция ошибок легитимными пользователями в «сыром» ключе

На этой стадии Алиса и Боб находятся в ситуации классического бинарного симметричного канала связи с вероятностью ошибки $\tilde{Q}(Q)$. Наиболее эффективная процедура исправления ошибок сводится к использованию случайных кодов [14]. На словах данная процедура сводится к следующему. Алиса генерирует $2^{n(C_{clas}(\tilde{Q}(Q))-\delta)}$ ($\delta \to 0$ при $n \to \infty$) случайных кодовых слов. Здесь

$$C_{clas}(\tilde{Q}(Q)) = 1 - H(\tilde{Q}(Q)), \\ H(x) = -x\log x - (1-x)\log(1-x), \quad (75)$$

соответственно пропускная способность классического бинарного симметричного канала связи и бинарная энтропийная функция Шеннона. Свою посланную битовую последовательность Алиса также включает в этот список. Далее эта таблица кодовых

слов через открытый канал связи сообщается Бобу. Ева также знает эту таблицу.

Согласно теореме кодирования для канала с шумом, при таком числе кодовых слов Боб с вероятностью единица выберет правильную строку бит, посланную Алисой. Выбор осуществляется просмотром всех кодовых слов и сравнением их с битовой строкой Боба. Боб выбирает то кодовое слово, которое ближе всего в метрике Хэмминга к его последовательности. После этого Боб исправляет свои ошибочные биты.

Исправление ошибок случайными шенноновскими кодами является наиболее эффективным в том смысле, что случайные коды обладают минимальной избыточностью при максимальном кодовом расстоянии.

«Скорость» C_{clas} случайных кодов — число бит в пересчете на одну позицию, которое может быть передано с нулевой вероятностью ошибки в асимптотическом пределе длинной последовательности через канал связи с шумом $\tilde{Q}(Q)$ — определяется формулой (75). Поскольку битовых последовательностей длины n ($n \to \infty$) существует всего 2^n, оглашение таблицы кодовых слов размером $2^{nC_{clas}(\tilde{Q}(Q))}$ означает, что битовая последовательность на приемной стороне произошла из одной из битовых последовательностей из таблицы кодовых слов. Поэтому остальные $2^{n(1-C_{clas}(\tilde{Q}(Q)))}$ последовательностей могут не рассматриваться при коррекции ошибок. Двоичный логарифм от размерности данного множества, равный $n(1-C_{clas}(\tilde{Q}(Q)))$, фактически представляет собой избыточность случайного кода — количество бит информации, передаваемой через открытый канал связи при коррекции ошибок.

При коррекции ошибок конструктивно декодируемыми кодами, избыточность которых выше, через открытый канал раскрывается большее количество бит информации (фактически это количество отвечает количеству контрольных бит проверок на четности).

В этом смысле, при коррекции ошибок случайными кодами через открытый канал связи легитимными пользователями раскрывается минимально возможное теоретически количество бит информации, которое доступно подслушивателю. Хотя процедура коррекции ошибок случайными кодами является конструктивной (описывается явно), она не является эффективно реализуемой, поскольку требует перебора и сравнения битовой последовательности с ошибками на приемной стороне с экспоненциально большой по длине последовательности таблицей кодовых слов.

На практике коррекция ошибок происходит итерационными методами посредством двусторонних обменов классической информацией через открытый канал связи. При этом так же, как при коррекции кодами (случайными или регулярными) раскрывается некоторое количество бит информации, которое затем должно быть изъято из «очищенного» ключа. Такое «изъятие» происходит на стадии усиления секретности (хэширования — сжатия «очищенного» ключа, см. ниже).

После стадии коррекции ошибок Алиса и Боб имеют одинаковые битовые последовательности — «очищенный», но еще не секретный ключ. Общий секретный ключ Алисы и Боба получается путем усиления секретности [11] «очищенного» ключа.

2.11. Измерения подслушивателя над многофотонными и однофотонными состояниями

После раскрытия базисов Ева измеряет хранящиеся в квантовой памяти состояния, происходящие из многофотонной компоненты, в правильном базисе идеальными детекторами. После этого ей становится известен каждый бит для позиций, происходящих из многофотонной компоненты.

Рассмотрим теперь позиции в квантовой памяти у Евы, происходящие из однофотонных состояний. После раскрытия базисов Алиса и Ева находятся в ситуации неидеального квантового канала связи. Состояния (16), (17) Алисы на входе квантового канала связи преобразуются в состояния (46)–(49) на выходе у Евы:

$$\rho_A(bi) = |\phi(bi)\rangle\langle\phi(bi)| \to \rho_E(bi) = \mathcal{T}[\rho_A(bi)], \quad (76)$$

где $\mathcal{T}[\dots]$ — отображение (часто называемое супероператором), переводящее матрицы плотности в матрицы плотности. Такое отображение является линейным, сохраняет эрмитовость, след и является вполне положительным (completely positive) [15].

Если классический канал без памяти задается переходными (условными) вероятностями между входом и выходом, то квантовый канал связи задается упомянутым выше отображением.

Цель Евы — извлечь из последовательности квантовых состояний посредством измерений максимально возможное количество классической информации, которое допускается квантовой механикой. Такой канал называют квантово-классическим [16].

Максимально допустимое количество классической информации ограничено фундаментальной ве-

личиной Холево [16], которая применительно к нашему случаю имеет вид

$$\overline{C}(Q) = S\left(\frac{1}{4}\sum_{bi=1}^{4}\mathcal{T}[\rho_A(bi)]\right) - \\ - \frac{1}{4}\sum_{bi=1}^{4} S(\mathcal{T}[\rho_A(bi)]), \quad (77)$$

где $S(\rho) = -\operatorname{Tr}(\rho\log\rho)$ — энтропия фон Неймана[10]. На входе канала Алиса выбирает состояния из алфавита квантовых состояний (16), (17) равновероятно с априорными вероятностями $1/4$. Здесь индекс bi принимает 4 значения (базисы и состояния).

Оказывается, что данная верхняя граница (77) достижима [16, 17]. Неформально она достигается следующим образом. На входе канала связи Алиса генерирует в соответствии с априорными вероятностями не более $2^{n(\overline{C}(Q)-\delta)}$ кодовых слов (последовательностей квантовых состояний длины n). Данная кодовая таблица открыто публикуется.

Поскольку базисы раскрыты, набор из M битовых кодовых слов $w^{(1)}, w^{(2)}, \ldots, w^{(M)}$ ($w^{(k)} = (i_1^k, i_2^k, \ldots, i_n^k)$, $i_j^k = 0, 1$, $k = 1, \ldots, M$) однозначно связан с квантовыми состояниями (16), (17), из которых данные битовые строки могли произойти,

$$\rho_A^{(k)}(b_1 i_1) \otimes \rho_A^{(k)}(b_2 i_2) \otimes \ldots \otimes \rho_A^{(k)}(b_n i_n).$$

Здесь, например, состояние $\rho_A^{(k)}(b_1 i_1)$, если первый бит в k-м кодовом слове Алисы $i_1^k = 0$ и раскрытый базис в первой посылке был b_1.

Таким образом, после оглашения Алисой таблицы классических битовых кодовых слов Ева знает всю таблицу из кодовых слов квантовых состояний, но не знает, какая конкретная последовательность была послана.

Другими словами, из-за однозначной связи классических и квантовых слов можно считать, что Алиса и Ева соединены неидеальным квантовым каналом связи. Формально можно считать, что Алиса кодирует классические последовательности $w^{(k)}$ в тензорное произведение матриц плотности Евы

$$\rho_{w^{(k)}} = \rho_E(b^{k_1} i^{k_1}) \otimes \rho_E(b^{k_2} i^{k_2}) \otimes \ldots \otimes \rho_E(b^{k_n} i^{k_n}).$$

Число таких квантовых кодовых слов равно числу классических кодовых слов, которое выбирается Алисой в зависимости от наблюдаемой ошибки у Боба.

[10] Переменная Q в (45) однозначно определяет квантовые состояния у Евы через связь с углом α в формуле (45), описывающей унитарное преобразование.

Далее в квантовый канал связи посылается поштучно одна из кодовых квантовых последовательностей и никакая другая. На выходе квантового канала связи используются измерения, которые описываются разложением единицы (см. детали в работе [16]):

$$I = \sum_{k=1}^{M} X_{w^{(k)}}, \quad X_{w^{(k)}} = \left(\sum_{l=1}^{M} P P_{w^{(l)}} P\right)^{-1/2} \times \\ \times P P_{w^{(k)}} P \left(\sum_{l=1}^{M} P P_{w^{(l)}} P\right)^{-1/2}, \quad (78)$$

где $P_{w^{(k)}}$ — проектор на типичное подпространство для оператора $\rho_{w^{(k)}}$, т. е. спектральный проектор оператора $\rho_{w^{(k)}}$, отвечающий собственным числам $\lambda_J = \lambda_{j_1}\lambda_{j_2}\ldots\lambda_{j_n}$ в интервале

$$2^{-n\left(\frac{1}{4}\sum_{bi=1}^{4} S(\mathcal{T}[\rho_A(bi)])+\delta\right)} < \lambda_J < \\ < 2^{-n\left(\frac{1}{4}\sum_{bi=1}^{4} S(\mathcal{T}[\rho_A(bi)])-\delta\right)}.$$

Напомним, что $\rho_E(bi) = \mathcal{T}[\rho_A(bi)]$ (см. (76)). Далее P — проектор на типичное подпространство для оператора $\left(\sum_{bi=1}^{4}\frac{1}{4}\rho_E(bi)\right)^{\otimes n}$, где

$$P = \sum_{J\in Typ} |\lambda_J\rangle\langle\lambda_J|. \quad (79)$$

Здесь

$$|\lambda_J\rangle = |\lambda_{j_1}\rangle \otimes |\lambda_{j_2}\rangle \otimes \ldots \otimes |\lambda_{j_n}\rangle,$$

$|\lambda_{j_m}\rangle$ — собственные векторы оператора, типичное пространство — это подпространство всех последовательностей, для которых

$$Typ = \{J : 2^{-n\left(S\left(\frac{1}{4}\sum_{bi=1}^{4}\mathcal{T}[\rho_A(bi)]\right)+\delta\right)} < \lambda_J < \\ < 2^{-n\left(S\left(\frac{1}{4}\sum_{bi=1}^{4}\mathcal{T}[\rho_A(bi)]\right)-\delta\right)}\}.$$

Для вычисления $\overline{C}(Q)$ потребуются собственные числа λ_{1-4} матрицы плотности

$$\sum_{bi=1}^{4}\frac{1}{4}\rho_E(bi) = \frac{1}{2}\times \\ \times \begin{pmatrix} 1-Q & (1-Q)\varepsilon(Q) & 0 & 0 \\ (1-Q)\varepsilon(Q) & 1-Q & 0 & 0 \\ 0 & 0 & Q & Q\varepsilon(Q) \\ 0 & 0 & Q\varepsilon(Q) & Q \end{pmatrix}, \quad (80)$$

$$\lambda_{1,2} = \frac{1-Q}{2}\,\frac{1\pm\varepsilon(Q)}{2}, \quad \lambda_{3,4} = \frac{Q}{2}\,\frac{1\pm\varepsilon(Q)}{2},$$

$$\varepsilon(Q) = 1 - 2Q.$$

Собственные числа частичных матриц плотности $\rho_E(bi)$ равны $1-Q$ и Q. Находим

$$\overline{C}(Q) = -Q\log Q - (1-Q)\log(1-Q). \qquad (81)$$

2.12. Критическая ошибка, до которой возможно распределение ключей

Взаимная информация между битовой строкой Алисы и Боба и Алисы и Евы в пересчете на одну позицию, соответственно, равны

$$I(A;E) = \overline{C}(Q)\frac{n_Q}{n_Q+n_{>1}} + \frac{n_{>1}}{n_Q+n_{>1}}, \qquad (82)$$

$$I(A;B) = C_{clas}(\tilde{Q}(Q)). \qquad (83)$$

Согласно работе [18], распределение секретного ключа возможно, если $I(A;B) > I(A;E)$. Критическая ошибка, до которой возможно распределение секретных ключей, определяется из уравнения

$$1 - H(\tilde{Q}(Q)) - H(Q)\frac{n_Q}{n_Q+n_{>1}} - \\ - \frac{n_{>1}}{n_Q+n_{>1}} = 0. \qquad (84)$$

Простой вид формула (84) приобретает при $\eta_1 = \eta_2 = \eta$ и $p_1 = p_2 = 0$:

$$1 - \frac{1}{1+\zeta}H\left(Q\frac{1}{1+\zeta}\right) - H(Q) = 0, \quad \zeta = \frac{n_{>1}}{n_Q}, \qquad (85)$$

где ζ — отношение многофотонной и однофотонной компонент, точнее, той доли однофотонной компоненты, которая не может быть блокирована Евой.

2.13. Усиление секретности «очищенного» ключа

Вообще говоря, того факта, что средняя ошибка Евы стремится к единице, еще не достаточно для гарантии секретности ключа, поскольку информация Евы о ключе согласно соотношениям (82), (83) не является экспоненциально малой.

Неформально усиление секретности ключа означает получение из ключа исходной длины, о котором подслушиватель имеет конечную информацию, ключа меньшей длины путем сжатия, о котором подслушиватель имеет сколь угодно экспоненциально малую информацию по параметру секретности.

Требование секретности ключа сводится к тому, что взаимная информация данной битовой строки v Евы длины n из множества всевозможных строк V относительно множества битовых строк W Алисы и Боба, которые уже равны, должна быть экспоненциально мала по заданному параметру секретности s:

$$I(W;V=v) < \frac{2^{-s}}{\ln 2}, \qquad (86)$$

или в терминах условной энтропии

$$H(W|V=v) > n - \frac{2^{-s}}{\ln 2}. \qquad (87)$$

Напомним, что величина $I(W;V=v)=0$ отвечает вероятности того, что Ева не имеет никакой информации о ключе, это эквивалентно самому плохому случаю для подслушивателя — простому угадыванию ключа.

Сжатие (хэширование) ключа называется усилением секретности и основано на замечательной теореме [11], использующей свойства энтропии Реньи второго порядка и универсальных функций хэширования [12].

Введем необходимые определения. Универсальной функцией хэширования второго порядка называется функция $g(x) : \{0,1\}^n \to \{0,1\}^r$ $(X \to Y)$, такая что для любых $x_1, x_2 \in X$ и $x_1 \neq x_2$ вероятность того, что $y_1 = y_2$ ($y_1 = g(x_1)$ и $y_2 = g(x_2)$) не более, чем $1/|Y| = 1/2^r$ ($|Y|$ — объем пространства r-битовых строк). Множество случайных функций $g \in G$ есть множество универсальных хэш-функций второго порядка, если при случайном выборе с равномерным распределением на G найдется не более $|G|/|Y|$ функций, для которых возможна коллизия значений функций при разных аргументах. Другими словами, если функции выбираются случайно в соответствии с равномерным распределением, то для данной выбранной функции вероятность для двух различных n-битовых строк иметь одно и то же хэш-значение функции не более, чем 2^{-r}.

Применительно к задачам криптографии (в том числе и квантовой) это означает, что если подслушиватель имеет n-битовую строку, отличную от n-битовых строк легитимных пользователей, то после хэширования (сжатия) случайно выбранной и известной всем хэш-функцией вероятность того, что r-битовая строка совпадает со строками легитимных пользователей, не превышает 2^{-r}.

Теорема об усилении секретности позволяет связать параметры n, r, s и свойства универсальных функций хэширования через энтропию Реньи второго рода, которая определяется через условные вероятности $\Pr(W|v)$.

Для этого потребуются следующие определения.

Пусть $x \in X$ — случайная величина с распределением $P_X(x)$ на множестве X. Вероятностью коллизий по определению называется величина

$$P_c(X) = \sum_{x \in X} P_X^2(x), \tag{88}$$

которая представляет собой вероятность того, что в двух независимых испытаниях случайная величина x примет одно и то же значение. Энтропия Реньи второго порядка по определению есть

$$R(X) = -\log P_c(X). \tag{89}$$

Аналогичные соотношения имеют место для условных распределений вероятности:

$$P_c(X|Y=y) = \sum_{x \in X} P^2_{X=x|Y=y}(y), \tag{90}$$

$$R(X|Y=y) = -\log P_c(X|Y=y). \tag{91}$$

Среднее значение энтропии Реньи есть

$$R(X|Y) = \sum_{y \in Y} P_Y(y) R(X|Y=y). \tag{92}$$

Для дальнейшего изложения полезно отметить, что при вычислении взаимной информации подслушивателя о ключе важны следующие соотношения между энтропией Реньи и энтропией Шеннона:

$$R(X) \le H(X), \tag{93}$$

$$H(X) = -\sum_{x \in X} P_X(x) \log P_X(x).$$

Имеет место соотношение для любого совместного распределения:

$$R(X|Y) \le H(X|Y). \tag{94}$$

Данное свойство условной энтропии Реньи используется в дальнейшем. Пусть подслушиватель имеет случайную величину Y. Цель Евы узнать случайную величину X. Условная энтропия Шеннона интерпретируется как количество бит, которых не хватает подслушивателю, если он имеет Y, для того, чтобы знать X. Грубо говоря, чем больше $H(X|Y)$, тем подслушивателю хуже. Для условной энтропии Реньи проще получить необходимые неравенства.

Следующая теорема играет фундаментальную роль в криптографии [11].

Теорема об усилении секретности (privacy amplification theorem)

Пусть $x \in X$ — случайная величина с распределением $P_X(x)$ и $R(X)$ — энтропия Реньи второго порядка. Пусть $g \in G$ — случайная величина с равномерным распределением на множестве универсальных хэш-функций второго порядка G, $g : X \to \to \{0,1\}^r$, и $K = G(X)$. Тогда имеют место неравенства

$$H(K|G) \ge R(K|G) \ge r - \log(1 + 2^{r-R(X)}) \ge \ge r - \frac{2^{r-R(X)}}{\ln 2}, \tag{95}$$

где $H(K|G) = H(G(X)|G)$ — средняя условная энтропия Шеннона. Хэш-функция здесь сама является случайной величиной.

Применительно к задачам квантовой криптографии важно следующее следствие теоремы [11]. Пусть имеется совместное распределение вероятностей P_{WV}, вообще говоря, неизвестное. Если энтропия Реньи ограничена снизу некоторым значением c ($R(W|V=v) \ge c$) и если Алиса и Боб выбирают хэш-значения от своих (одинаковых) строк $K = G(X)$ в качестве секретного ключа, причем хэш-функция из $\{0,1\}^n \to \{0,1\}^r$ выбирается случайно и равновероятно из G, то имеет место соотношение

$$H(K|G, W_E = w_E) \ge r - \log(1 + 2^{r-c}) \ge \ge r - \frac{2^{r-c}}{\ln 2}. \tag{96}$$

Для дальнейшего принципиально важно, что степень сжатия ключа зависит от конкретной процедуры коррекции ошибок в первичном ключе, которую используют легитимные пользователи. Поэтому задача легитимных пользователей состоит не только в исправлении ошибок, но и в установлении того, как изменяется условная энтропия Реньи.

Следующая замечательная теорема дает универсальный способ оценить уменьшение энтропии Реньи, если известна условная энтропия до процедуры коррекции ошибок.

Теорема об уменьшении энтропии Реньи [19]

Пусть W — случайная величина из алфавита W и пусть v и u — частичные значения двух коррелированных случайных величин V и U с алфавитами соответственно V и U. Пусть размерность алфавита $|U|$ и пусть $k = \log|U|$ (логарифм берется по основанию 2). Далее пусть s — параметр секретности. Тогда с вероятностью не менее $1 - 2^{-s}$ величина U

принимает частичное значение u такое, что уменьшение энтропии Реньи второго порядка при данном значении u не более

$$R(W|V=v,U=u) > R(W|V=v) - \\ -(k+s+2). \quad (97)$$

Условная энтропия Реньи будет ограничена величиной (здесь учтено, что множество строк Алисы равномерно распределено на W)[11)]

$$R(W|V=v) \geq \\ \geq n\left(1-\left(\overline{C}(Q)\frac{n_Q}{n_Q+n_{>1}}+\frac{n_{>1}}{n_Q+n_{>1}}\right)\right). \quad (98)$$

Данное неравенство дает оценку числа бит в строке Евы длины n, которых ей не хватает для того, чтобы знать, из какой строки Алисы произошла частичная строка v. Отметим, что эта оценка относится к стадии до коррекции ошибок Бобом через открытый канал связи посредством обмена информацией с Алисой.

Пусть далее происходит коррекция ошибок при помощи случайных шенноновских кодов. Для исправления ошибок Алисе и Бобу при ошибке Q требуется передать через открытый канал не менее

$$n(1-C_{clas}(\tilde{Q}(Q))) \quad (99)$$

бит информации для исправления ошибок с вероятностью единица, поэтому через открытый канал связи между Алисой и Бобом будет выдано не менее

$$k = n(1-C_{clas}(\tilde{Q}(Q)))$$

бит информации. Таким образом, уменьшение энтропии Реньи второго порядка у Евы после исправления ошибок составит

$$R(W|V=v,U=u) \geq n\left(C_{clas}(\tilde{Q}(Q)) - \right. \\ \left. -\left(\overline{C}(Q)\frac{n_Q}{n_Q+n_{>1}}+\frac{n_{>1}}{n_Q+n_{>1}}\right)\right). \quad (100)$$

Далее, если после коррекции ошибок Алиса и Боб проводят сжатие (хэширование) своих, уже одинаковых строк при помощи случайно выбранной в соответствии с равномерным распределением универсальной хэш-функции G второго порядка до размера

$$r = n\left(1-H(\tilde{Q}(Q))-H(Q)\frac{n_Q}{n_Q+n_{>1}}- \right. \\ \left. -\frac{n_{>1}}{n_Q+n_{>1}}\right)-s-2, \quad (101)$$

где s — параметр секретности, который Алиса и Боб выбирают по своим требованиям, то взаимная информация Евы о ключе, как это гарантирует теорема об усилении секретности, не более

$$I(K;GV) \leq \frac{2^{-s}}{\ln 2}. \quad (102)$$

Напомним, что хэш-функция выбирается Алисой и Бобом через открытый канал связи и считается известной Еве.

Формула (101) дает длину финального ключа.

2.14. Достижимая скорость распределения ключей в реальных оптоволоконных системах квантовой криптографии

Ниже приводятся расчеты критической ошибки и длины секретного ключа в шенноновском пределе (коррекции ошибок случайными кодами), а также при использовании каскадного метода коррекции ошибок. Как отмечалось выше, коррекция ошибок случайными шенноновскими кодами не является практически реализуемой, возможно лишь приблизиться к этому пределу.

На рис. 4 приведены зависимости взаимной информации о ключе между легитимными пользователями и подслушивателем. Рисунок 4*а* относится к идеальному случаю (строго однофотонный источник состояний, идеальные фотодетекторы, канал связи без затухания). В этом случае критическая ошибка протокола составляет $\tilde{Q}(Q)=Q\approx 11\%$ при коррекции ошибок случайными кодами.

На рис. 4*б* приведены расчеты для случая, когда коррекция ошибок осуществляется каскадным методом. В этом случае из-за бóльшей избыточности по сравнению со случайными кодами в открытый канал выдается больше информации. «Изъятие» этой информации на стадии хэширования приводит к большему сжатию ключа и, соответственно, меньшей критической наблюдаемой ошибке на приемной стороне. Критическая ошибка для идеального случая составляет $\tilde{Q}(Q)=Q\approx 8.9\,\%$, что достаточно близко к шенноновскому пределу.

[11)] Вычисление условной энтропии Реньи представляет собой отдельную техническую задачу, данные вычисления здесь не приводятся.

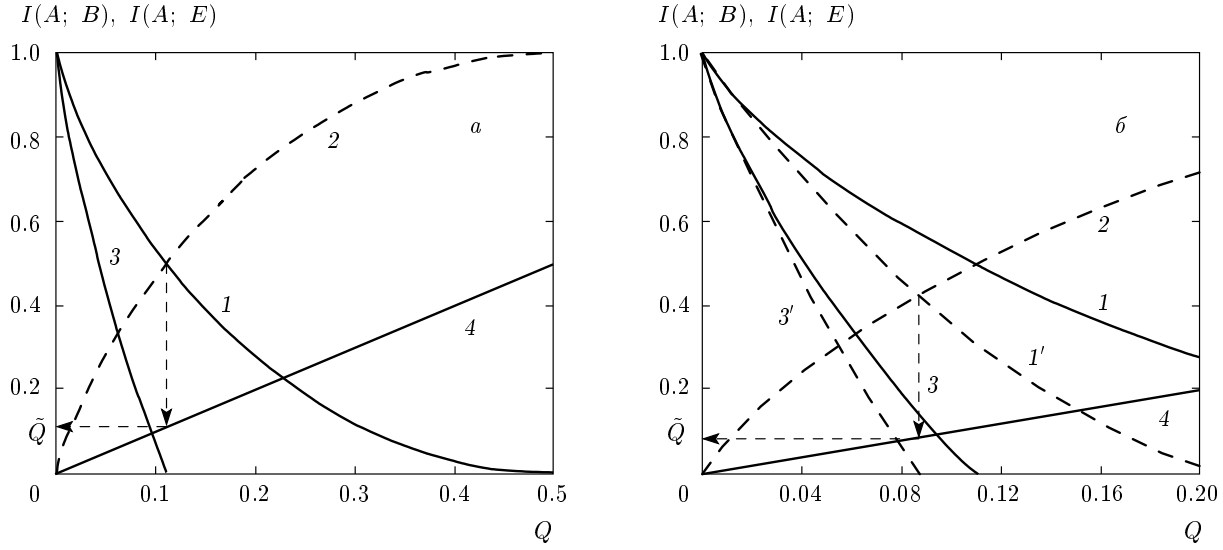

Рис. 4. Взаимные информации $I(A;B)$, $I(A;E)$ и наблюдаемая ошибка на приемной стороне $\tilde{Q}$ как функции параметра Q. В идеальном случае $\tilde{Q}(Q) \equiv Q$. *а* — случай исправления ошибок случайными кодами; *б* — случай исправления ошибок как случайными кодами, так и каскадной процедурой. Кривые *1* и $1'$ — $I(A;B)$ для случайных кодов (*1*) и каскадной процедуры ($1'$). Кривая *2* — $I(A;E)$. Линии *3* и $3'$ — максимально возможная длина финального секретного ключа ($I(A;B)(Q) - I(A;E)(Q)$ при параметре секретности $s = 0$) в битах в пересчете на одну позицию для случайных кодов (*3*) и каскадного метода ($3'$). Кривая 4 — $\tilde{Q}(Q)$. Критическая ошибка находится путем определения точки Q, где $I(A;B)(Q_c) = I(A;E)(Q_c)$, затем по этому значению вычисляется реально наблюдаемая ошибка $\tilde{Q}(Q_c)$. Такое графическое вычисление показано штриховыми линиями со стрелками

Если параметры источника, фотодетекторов заданы фактическим сегодняшним технологическим уровнем, то увеличение длины и скорости передачи ключей могут быть улучшены только за счет использования более эффективных процедур коррекции ошибок, т. е. кодов распределенной коррекции ошибок, обладающих меньшей избыточностью (выдающей меньше бит информации в открытый канал при исправлении ошибок). Из опубликованных данных наиболее эффективной процедурой коррекции ошибок является каскадный метод [20]. Данный метод конструктивно реализуем, поэтому границы по допустимой критической ошибке и длине ключей, соответственно, скорости распределения ключей оказываются несколько меньше теоретического предела. Ниже приводятся расчеты критической ошибки и длины ключа при использовании каскадного метода коррекции ошибок. На сегодняшний день неизвестно аналитической формулы, дающей избыточность каскадного метода. Длина секретного ключа, которая может быть получена при использовании каскадного метода коррекции ошибок, аналогична (101) и имеет вид

$$r = n\left(1 - H_{Cascade}(\tilde{Q}(Q)) - H(Q)\frac{\tilde{n}_Q}{n_Q + n_{>1}} - \right.$$
$$\left. - \frac{\tilde{n}_{>1}}{n_Q + n_{>1}}\right) - s - 2, \quad (103)$$

где $H_{Cascade}(\tilde{Q}(Q))$ — энтропийная функция для каскадной процедуры, для нее известна численная интерполяция. Численная интерполяция использована при построении зависимостей на рис. 4, 5.

На рис. 5 приведены зависимости взаимных информаций и длины ключа от параметра Q для реальных систем для двух разных длин квантового канала связи 50 км (рис. 5*а*) и 100 км (рис. 5*б*). Здесь важно отметить, что при распределении ключей на расстояние 50 км можно использовать ослабление лазерного излучения до уровня $\mu = 0.1$ фотона в импульсе, а также типичные средние значения квантовой эффективности $\eta = 0.2$ и вероятности темновых отсчетов $p_{dark} = 10^{-5}$. Однако для передачи ключей на расстояние 100 км требуется ослабление излучения до уровня в среднем одной сотой фотона в импульсе, $\mu = 0.01$, и использование фотодетекторов с рекордными показателями темновых шумов $p_{dark} = 10^{-7}$, что находится на пределе современ-

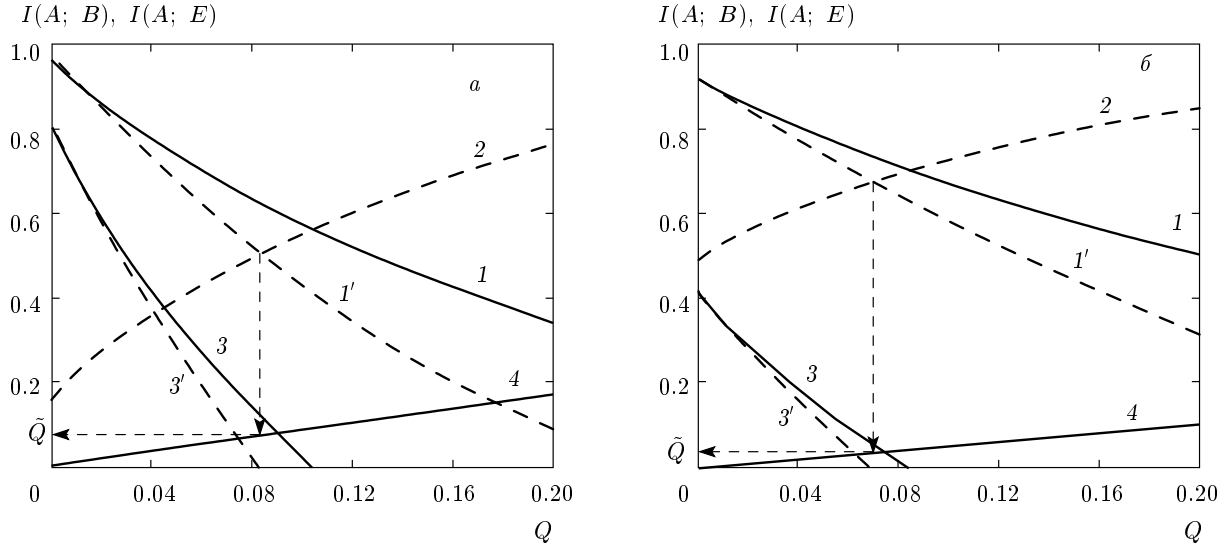

Рис. 5. Взаимные информации $I(A;B)$, $I(A;E)$ и наблюдаемая ошибка на приемной стороне $\tilde{Q}$ как функции параметра Q, когда источником квантовых состояний является сильно ослабленное лазерное излучение, а фотодетекторы не являются идеальными. Среднее число фотонов в импульсе $\mu = 0.1$ (*а*), 0.01 (*б*), квантовая эффективность фотодетекторов $\eta = 0.2$, вероятность темновых отсчетов в стробе $p_{dark} = 10^{-5}$ (*а*), 10^{-7} (*б*). Использовано стандартное значение коэффициента затухания в оптоволокне SMF-28 — $\alpha = 0.2$ дБ/км. Квантовые эффективности фотодетекторов, а также вероятности темновых отсчетов взяты одинаковыми: $\eta_1 = \eta_2 = \eta$, $p_1 = p_2 = p_{dark}$ (ср. с (68)–(72)). Кроме того, учтено, что в реальные расчеты входит половина от квантовой эффективности, поскольку на приемной станции перед детектированием происходит преобразование состояний на интерферометре Маха – Цандера, что уменьшает вероятность детектирования вдвое (см. рис. 2). Длина канала связи $L = 50$ км (*а*), 100 (*б*) км. Соответствие номеров кривых зависимостям $I(A;B)$, $I(A;E)$, $I(A;B) - I(A;E)$ и $\tilde{Q}(Q)$ такое же, как и на рис. 5. Вычисление наблюдаемой критической ошибки, до которой возможно распределение ключей, осуществляется графически, аналогично рис. 5

ных технологических возможностей, по крайней мере, для лавинных детекторов на основе InGaAs. При этом требуется охлаждение до азотных температур. При худших показателях невозможно обеспечить передачу ключей на такое расстояние[12)].

Для практических целей самым важным параметром является скорость генерации новых ключей в реальном времени. На рис. 6 приведены зависимости длины секретного ключа в битах на одну посылку (строб-импульс) в зависимости от длины оптоволоконного канала связи. Для коррекции ошибок используется каскадная процедура.

При вероятности темновых отсчетов $p_{dark} = 10^{-5}$ критическая длина канала связи не превышает 60 км. Например, при длине канала 35 км (средний диаметр г. Москвы) на одну посылку приходится $1 \cdot 10^{-3}$ бит, если $\eta = 0.2$ (рис. 6*а*) и соответственно $2 \cdot 10^{-3}$ бит, если $\eta = 0.4$ (рис. 6*б*).

Характерные частоты следования импульсов составляют 100 кГц – 10 МГц, соответственно, скорость генерации ключа в реальном времени равна 100–10000 бит/с. Если в дальнейшем данные ключи используются, например, для алгоритма ГОСТ 28147-89, это означает, что при такой длине канала связи возможна смена ключей раз в несколько секунд.

При передаче ключей на 100 км, во-первых, требуются детекторы с вероятностью темновых отсчетов на уровне $p_{dark} = 10^{-7}$, а также ослабление лазерного излучения до уровня $\mu = 0.01$–0.001 в среднем фотона в импульсе (см. рис. 6*в,г*). При этом число бит на посылку (рис. 6*г*) на 100 км составляет 10^{-6}. Скорость генерации ключей в реальном времени равна, соответственно, 0.01–10 бит/с. Поэтому достижимая скорость смены ключей на таком расстоянии — не более одного раза в минуту.

Интересно сравнить наши результаты с данными, полученными в работе [9].

Для критической ошибки, до которой возможно

[12)] Отметим, что это согласуется с совсем грубой оценкой длины канала связи (см. рис. 1).

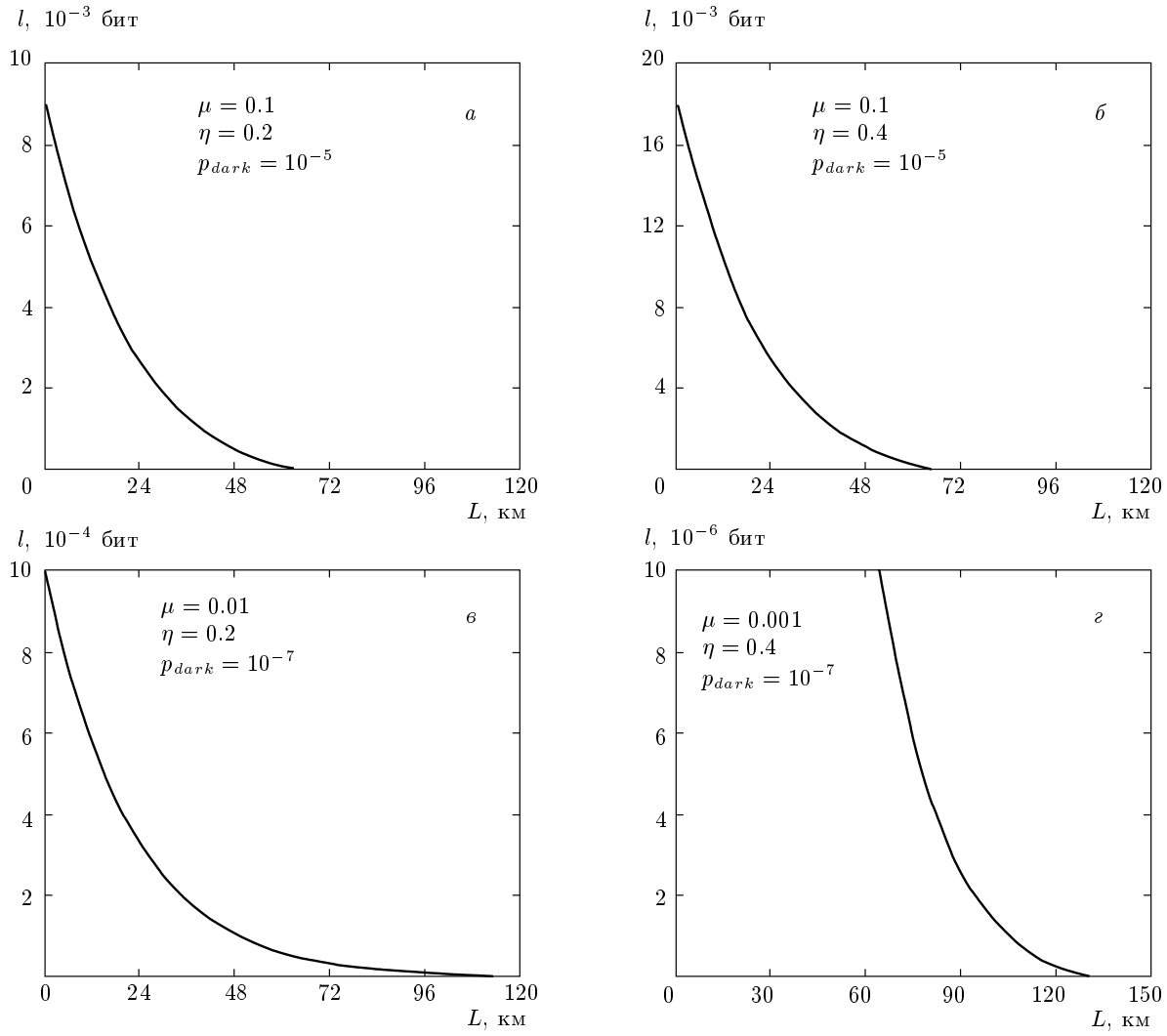

Рис. 6. Длина l секретного ключа в битах на одну посылку как функция длины оптоволоконного канала связи. Параметры фотодетекторов и среднее число фотонов в импульсе указаны на вставках. Параметр секретности s и параметр Q положены равными нулю

распределение ключей, было получено уравнение

$$\left(1-\frac{p_M}{p_D}\right)\times \\ \times\left[1-H\left(\frac{2Q'}{1-p_M/p_D}\right)-H(Q')\right]=0, \quad (104)$$

где p_D — доля детектируемых состояний на приемной стороне, p_M — доля многофотонной компоненты, Q' — наблюдаемая ошибка на приемной стороне.

Выразим наблюдаемую ошибку на приемной стороне через параметр Q у подслушивателя:

$$Q=Q'\left(1-\frac{p_M}{p_D}\right). \quad (105)$$

После этого уравнение приобретает вид

$$1-\frac{1}{1+\zeta}H\left(Q\frac{1}{1+\zeta}\right)-H(2Q)=0, \\ \zeta=\frac{p_M}{p_D-p_M}, \quad (106)$$

что совпадает с точностью до множителя 2 в аргументе $H(2Q)$, если перейти к нашим обозначениям $p_D \to n_Q+n_{>1}$ — полное число детектируемых состояний, $p_M \to n_{>1}$ — доля многофотонной компоненты. Происхождение этого множителя 2 в уравнении (106) связано с тем, что в доказательстве процедуры коррекции ошибок и усиления секретности по сути совмещены, что завышает возможности подслуши-

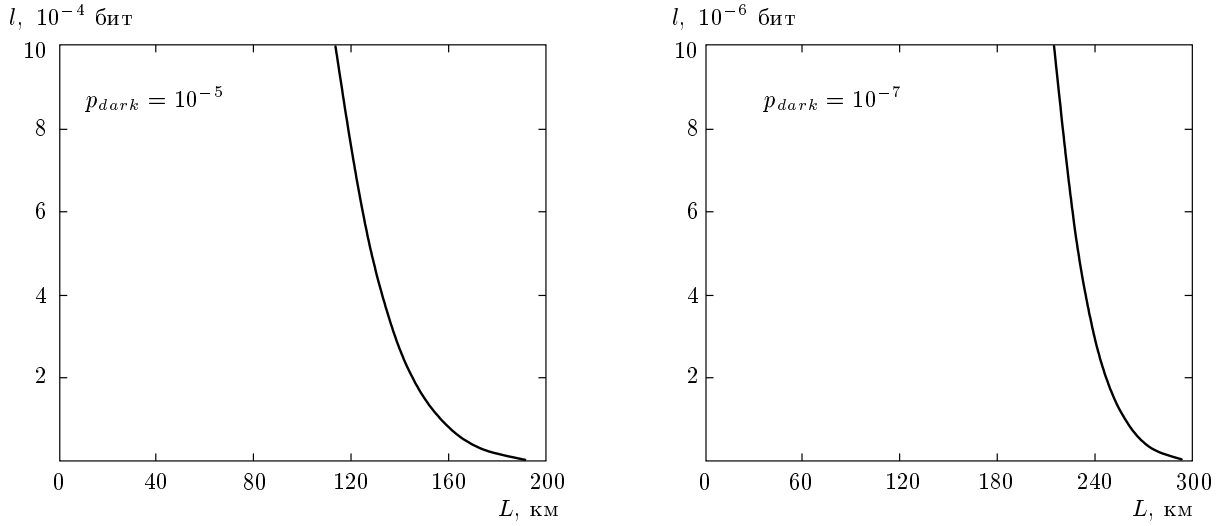

Рис. 7. Зависимости длины секретного ключа в битах на одну посылку в зависимости от длины оптоволоконного канала связи для случая строго однофотонного источника квантовых состояний, $\eta = 0.2$. Параметр секретности s и параметр Q положены равными 0

вателя[13)].

Видно, что формулы (104), (106) являются частным случаем, поскольку уравнение (106) не учитывает темновые отсчеты и конечную эффективность фотодетекторов.

Отметим также, что наши результаты верны и в случае, если статистика источника квантовых состояний не является пуассоновской. В этом случае, как видно по нашему выводу, вместо n_Q и $n_{>1}$ должны использоваться вероятности однофотонной и многофотонной компонент для используемого источника излучения.

3. ЗАКЛЮЧЕНИЕ

Темновые отсчеты и не 100 %-я квантовая эффективность фотодетекторов являются критическими параметрами системы, которые вместе с не строго однофотонным источником и затуханием в канале связи определяют криптографическую стойкость системы в целом.

Приведем в заключение скорость генерации ключей для строго однофотонного источника (рис. 7). Как следует из расчетов, даже при уровне темновых отсчетов 10^{-5}, достижимая критическая длина оказывается приблизительно равной 200 км. При вероятности темновых отсчетов 10^{-7} критическая длина оказывается уже около 300 км. Такая вероятность темновых отсчетов достигнута на сегодняшний день при охлаждении фотодетекторов до азотных температур.

Для передачи ключей на большие расстояния требуется использование более совершенных элементов системы, а также других квантовых протоколов распределения ключей, которые в идеальном случае имеют большую критическую ошибку. Одним из таких протоколов является метод фазово-временного кодирования, который на сегодняшний день имеет наибольшую критическую ошибку из всех известных протоколов передачи ключей.

Основными недостатками лавинных фотодетекторов на основе InGaAs для детектирования на длине волны 1.3–1.55 мкм являются темновые фотоотсчеты и достаточно низкая частота повторения посылок из-за эффектов после импульса (afterpulsing). На сегодняшний день имеются лабораторные разработки сверхпроводящих детекторов (см., например, [21]). Уже достигнут уровень темновых отсчетов на уровне 10^{-4} $с^{-1}$ (или эквивалентно 10^{-13} $нс^{-1}$, причем данные детекторы не требуют стробирования) при квантовой эффективности около 30 %. Достигнутая частота работы таких детекторов на сегодняшний день 100–1000 МГц, что на два–три порядка выше, чем у лавинных фотодетекторов.

[13)] Отметим, как упоминалось во Введении, метод доказательства [2] для идеального случая также приводит к дополнительной двойке в уравнении (1). Данный результат был усилен до критической ошибки, равной 11 %, в работе [5].

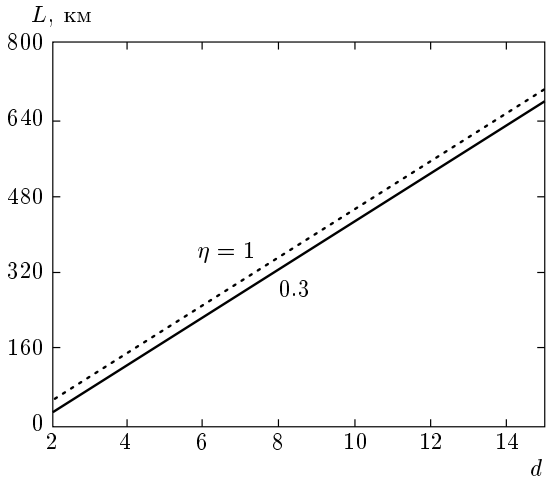

Рис. 8. Зависимости критической длины от показателя экспоненты вероятности темновых отсчетов (p_{dark} [нс$^{-1}$] $= 10^{-d}$) для двух разных значений квантовой эффективности и каскадной коррекции ошибок. Константа затухания в одномодовом волокне $\alpha = 0.2$ дБ/км

При строго однофотонном источнике квантовых состояний и затухании в канале связи основную роль начинают играть темновые отсчеты. Выведем предельную зависимость критической длины линии связи, до которой гарантируется секретность передаваемых ключей. Как следует из формулы (101), связь критической длины определяется из уравнения

$$\frac{p_{dark}}{\eta(L)+2p_{dark}} = Q_c, \quad \eta(L) = \eta\cdot 10^{-\alpha L/10},$$
$$L = \frac{10}{\alpha}\left(d - \log_{10}\left(\frac{1-2Q_c}{\eta Q_c}\right)\right), \tag{107}$$

где Q_c — критическая ошибка протокола ($Q_c \approx 11\,\%$ и $Q_c \approx 8.9\,\%$ при коррекции ошибок соответственно случайными кодами и каскадным методом). Удобно представить вероятность темновых отсчетов как $p_{dark} = 10^{-d}$. Зависимость критической длины от показателя экспоненты вероятности темновых отсчетов ($L(d)$) приведена на рис. 8. Как следует из рис. 8, при достигнутых на сегодняшний день параметрах сверхпроводящих детекторов длина линии связи может доходить до 550 км. При частоте следования посылок 1000 МГц скорость генерации ключа составит 0.1–1 бит/с.

Таким образом, показано, что даже в случае, когда действия подслушивателя не лимитируются никакими техническими возможностями, а ограничены лишь фундаментальными запретами квантовой механики на различимость квантовых состояний, и при этом легитимные пользователи могут использовать лишь средства, доступные на современном технологическом уровне (не строго однофотонные источники квантовых состояний, неидеальные лавинные фотодетекторы, оптоволоконный канал связи с затуханием), обеспечивается безусловно (unconditional) секретное распределение ключей. Получена связь параметров системы с длиной канала связи, до которой гарантируется передача ключей.

Выражаю благодарность Академии криптографии РФ за поддержку. Работа выполнена при частичной поддержке РФФИ (грант № 08-02-00559). Выражаю также благодарность С. П. Кулику за обсуждения.

ЛИТЕРАТУРА

1. C. H. Bennett and G. Brassard, in *Proc. of IEEE Int. Conf. on Comp. Syst. and Signal Proces.*, Bangalore, India (1984), p. 175.
2. D. Mayers, arXiv:quant-ph/9802025.
3. E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, arXiv:quant-ph/9912053.
4. P. W. Shor and J. Preskill, arXiv:quant-ph/0003004.
5. S. Watanabe, R. Matsumoto, and T. Uyematsu, arXiv:quant-ph/0412070.
6. С. Н. Молотков, А. В. Тимофеев, Письма в ЖЭТФ **85**, 632 (2007).
7. G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
8. N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
9. H. Inamori, N. Lütkenhaus, and D. Mayers, arXiv:quant-ph/0107017.
10. А. В. Тимофеев, Д. И. Помозов, А. П. Маккавеев, С. Н. Молотков, ЖЭТФ **131**, 771 (2007).
11. C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
12. J. L. Carter and M. N. Wegman, J. Comp. Syst. Sci. **18**, 143 (1979).
13. C. A. Fuchs, N. Gisin, R. Griffiths, Chi-Sheng Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
14. C. E. Shannon, Bell Syst. Tech. J. **27**, 397; **27**, 623 (1948).

15. K. Kraus, *States, Effects and Operations*, Springer-Verlag, Berlin (1983).

16. А. С. Холево, *Введение в квантовую теорию информации*, сер. *Современная матем. физ.*, вып. 5, МЦНМО, Москва (2002); А. С. Холево, Проблемы передачи информации **8**, 63 (1972); **15**, 3 (1979); УМН **53**, 193 (1998).

17. B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).

18. I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).

19. C. Cachin, Dissertation of Swiss Federal Inst. of Technology of Zürich, Diss. ETH № 12187 (1997).

20. G. Brassard and L. Salvail, Lect. Notes Comp. Sci. **765**, 410 (1994).

21. Book of Abstracts, *Single-Photon Workshop 2007, Source, Detectors, Applications and Measurements Methods*, INRIM, Torino, Italy (2007).