ЖЭТФ, 2017, том 151, вып. 3, стр. 476–493

МЕЗОСКОПИЧЕСКАЯ КВАНТОВАЯ КРИПТОГРАФИЯ

С. Н. Молотков*

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

Академия криптографии Российской Федерации
121552, Москва, Россия

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

Поступила в редакцию 19 сентября 2016 г.

Поскольку строго однофотонный источник пока отсутствует, в системах квантовой криптографии в качестве информационных квантовых состояний используют ослабленное до квазиоднофотонного уровня когерентное излучение лазера со средним числом фотонов $\mu \approx 0.1$–0.5 в импульсе. Линейная независимость набора информационных когерентных квазиоднофотонных состояний приводит к возможности измерений с определенным исходом (Unambiguous Measurements), которые при наличии потерь в линии ограничивают дальность передачи секретных ключей. С определенной величины критических потерь (длины линии) подслушиватель знает весь ключ, не производит ошибок и не детектируется — распределение секретных ключей становится невозможным. Данная проблема решается введением дополнительного контрольного реперного состояния со средним числом фотонов $\mu_{cl} \approx 10^3$–10^6, в зависимости от длины линии связи. Показано, что использование контрольного реперного состояния не позволяет подслушивателю проводить измерения с определенным исходом и при этом оставаться недетектируемым. Реперное состояние гарантирует детектирование подслушивателя в канале с большими потерями. При этом информационные состояния могут содержать мезоскопическое среднее число фотонов в диапазоне $\mu_q \approx 0.5$–10^2. Предлагаемый протокол технически просто реализуем, допускает гибкую настройку параметров под длину линии связи, прост и прозрачен для доказательства секретности ключей.

DOI: 10.7868/S000445101703004X

1. ВВЕДЕНИЕ

Цель квантовой криптографии (квантового распределения ключей) — передача секретных ключей между пространственно удаленными пользователями при помощи квантовых состояний по открытому квантовому каналу связи [1]. Секретность ключей и детектирование любых попыток подслушивания при передаче квантовых состояний основаны на фундаментальных запретах квантовой теории. Квантовая механика запрещает достоверное (с вероятностью единица) копирование неизвестного квантового состояния $|\psi\rangle$ (no cloning, теорема о запрете клонирования [2]). Иначе говоря, следующий процесс запрещен:

$$U(|\psi\rangle \otimes |E\rangle) = |\psi\rangle \otimes |\psi\rangle \otimes |E'\rangle,$$

где $|E\rangle$, $|E'\rangle$ — вспомогательная квантовая система до и после копирования, U — унитарный оператор.

Второй фундаментальный запрет квантовой теории [3], тесно связанный с первым, — это запрет на достоверное различение неортогональных квантовых состояний $|\psi_0\rangle$, $|\psi_1\rangle$. Следующий процесс запрещен:

$$U(|\psi_0\rangle \otimes |E\rangle) = |\psi_0\rangle \otimes |E'_0\rangle,$$

$$U(|\psi_1\rangle \otimes |E\rangle) = |\psi_1\rangle \otimes |E'_1\rangle,$$

где $|E'_0\rangle$ и $|E'_1\rangle$ — состояния вспомогательной квантовой системы после совместной эволюции ($|E'_0\rangle \neq |E'_1\rangle$), если входными состояниями были $|\psi_0\rangle$ либо $|\psi_1\rangle$. Оба запрета являются фактически следствием линейности квантовой механики. При этом не требуется, чтобы квантовые состояния были однофотонными.

* E-mail: sergei.molotkov@gmail.com

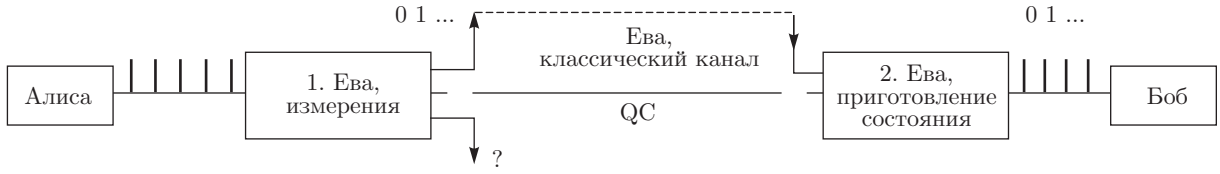

Рис. 1. Иллюстрация атаки с измерениями с определенным исходом

Не существует измерений, которые бы позволяли различать с вероятностью единица неортогональные квантовые состояния. Ситуация существенно меняется, если требуется различать однозначно, но с вероятностью успеха меньше единицы, неортогональные состояния. Такие измерения называются измерениями с определенным исходом (unambiguous measurements — UM) и существуют для произвольного числа N линейно независимых квантовых состояний [4]. Измерение имеет $N+1$ исход. При появлении одного из N исходов состояния идентифицируются однозначно, а $N+1$-й исход неопределен и может произойти при измерении любого из N квантовых состояний. Для пары состояний измерение имеет три исхода и дается разложением единицы [4]:

$$I = \mathcal{M}_0 + \mathcal{M}_1 + \mathcal{M}_?, \quad \mathcal{M}_0 = c(I - |\psi_1\rangle\langle\psi_1|),$$

$$\mathcal{M}_1 = c(I - |\psi_0\rangle\langle\psi_0|), \quad \mathcal{M}_? = I - \mathcal{M}_0 - \mathcal{M}_1,$$

$$c = (1 + |\langle\psi_0|\psi_1\rangle|)^{-1},$$

где $\mathcal{M}_{0,1,?}$ — операторно-значные меры. Данное измерение является оптимальным в смысле минимизации вероятности неопределенного исхода «?». Вероятности определенных исходов равны

$$\Pr(\mathcal{M}_0||\psi_0\rangle) = \Pr(\mathcal{M}_1||\psi_1\rangle) = 1 - |\langle\psi_0|\psi_1\rangle|,$$

$$\Pr(\mathcal{M}_0||\psi_1\rangle) = \Pr(\mathcal{M}_1||\psi_0\rangle) = 0,$$

$$\Pr(\mathcal{M}_?||\psi_{0,1}\rangle) = |\langle\psi_0|\psi_1\rangle|.$$

Строго однофотонный источник отсутствует и, возможно, вряд ли будет создан[1)]. Поэтому на практике используются квазиоднофотонные состояния сильно ослабленного когерентного лазерного излучения. Набор сильно ослабленных когерентных состояний $\{|\alpha_i\rangle\}_{i=1}^N$ ($|\alpha_i|^2 = \mu_i \ll 1$ — среднее число фотонов в состоянии), в которые кодируются биты ключа, является линейно независимым, поэтому существует UM-измерение, позволяющее различать данные состояния, но с вероятностью успеха меньшей единицы. Применительно к квантовой криптографии последнее означает, что в канале с потерями подслушиватель может использовать данные измерения для различения состояний. Для этого подслушиватель разрывает линию связи в двух местах (см. рис. 1, напомним, что в квантовой криптографии квантовый канал связи не контролируется) и проводит UM-измерения. При неопределенном исходе «?» подслушиватель не знает передаваемое состояние и блокирует канал связи, чтобы не производить ошибок на приемной стороне. Если вероятность потерь в линии связи $\Pr(\text{Loss}) > \Pr(?)$, то исчезновение состояния можно списать на потери в линии. В остальных случаях, когда имеет место определенный исход, подслушиватель знает определенно передаваемое квантовое состояние и может перепослать через второй разрыв в линии правильные состояния на приемную сторону (см. рис. 1). При такой атаке подслушиватель знает с определенностью все зарегистрированные на приемной стороне квантовые состояния, не производит ошибок, сохраняет общее число зарегистрированных состояний при данных потерях в линии и его вторжение не детектируется. Для такой атаки не требуется наличие у подслушивателя долговременной квантовой памяти, т. е. атака может быть реализована при существующем на сегодняшний день уровне технологий. Поэтому, начиная с некоторых потерь в линии связи, весь ключ будет известен подслушивателю, который при этом даже не производит ошибок на приемной стороне. Длина линии, при которой можно передавать ключи и гарантировать их секретность, определяется структурой набора информационных сильно ослабленных когерентных состояний. Сама по себе линейная независимость когерентных состояний происходит из-за присутствия в состоянии вакуумной компоненты поля при любом среднем числе фотонов.

[1)] Под строго однофотонным источником понимается источник, для которого корреляционная функция второго порядка имеет провал строго до нуля. Сегодняшние источники, называемые в ряде экспериментов однофотонными, такому требованию не удовлетворяют. Однако если такой источник будет создан, существуют протоколы квантового распределения ключей, например, протокол с фазово-временным кодированием, у которых критическая ошибка, до которой гарантируется секретное распределение ключей, приближается к шенноновскому теоретическому пределу в 50%. Данный протокол при существующих лавинных детекторах обеспечивает дальность передачи ключей до 500 км и существенно превосходит по дальности остальные протоколы [5].

Чем больше вероятность неопределенного исхода Pr(?), тем большую дальность передачи секретных ключей можно обеспечить.

Возможны несколько вариантов решения данной проблемы.

Можно увеличить Pr(?), уменьшая среднее число фотонов в информационном состоянии μ. Для двух состояний $\Pr(?) \propto e^{-\mu}$, поэтому формально при $\mu \to 0$ соответственно $\Pr(?) \to 1$. Однако при этом число зарегистрированных посылок на приемной стороне уменьшается в той же пропорции, $N_{reg} \approx \eta\mu \to 0$ (η — квантовая эффективность лавинного однофотонного детектора (APD), $\eta \approx 10$–$30\,\%$). При малых μ критичными становятся темновые шумы самого лавинного детектора. При этом на приемной стороне фактически происходит регистрация случайных темновых шумов APD, что дает большую наблюдаемую ошибку, при которой также нельзя гарантировать секретность ключей. Поскольку принципиально невозможно отличить ошибки на приемной стороне от вторжений в канал связи и собственных шумов аппаратуры, все ошибки приходится списывать на действия подслушивателя. Большой поток ошибок будет означать вторжение в канал связи и утечку информации о передаваемом ключе к подслушивателю, что не позволит получить секретный ключ при большой вероятности ошибки.

Другой способ увеличения вероятности неопределенного исхода состоит в увеличении числа базисов [6]. Для N геометрически однородных когерентных информационных состояний имеется точное решение [4]. Вероятность неопределенного исхода зависит от числа состояний как $\Pr(?) \propto 1 - e^{-\mu N}$. При этом эффективность регистрации на приемной стороне зависит от числа информационных состояний как обратная степень: $N_{reg} \propto 1/N$. При учете реальных параметров системы возможно увеличение числа состояний до $N = 8$. Дальнейшее увеличение числа базисов и состояний также начинает приводить к тому, что уменьшается эффективность регистрации, и возрастает доля темновых шумов. Поэтому увеличение числа состояний — это тоже только частичное решение проблемы.

Еще один способ состоит в использовании распределенного кодирования и реализуется в протоколах DPS (Differential Phase Shift) [7] и COW (Coherent One Way) [8]. Распределенное кодирование приводит к необходимости различать целые серии квантовых состояний как целое. При этом вероятность неопределенного исхода зависит как $\Pr(?) \propto \propto 1 - e^{-\mu N}$ (N — длина последовательности). В этом случае роль UM-измерений практически полностью нивелируется. При большой вероятности неопределенного исхода подслушивателю придется выкидывать много состояний, а это требует больших потерь, т. е. большой длины линии связи. Поэтому, казалось бы, что проблема решена. Однако распределенное кодирование приводит к тому, что возникает другая принципиальная трудность — доказать секретность ключей достаточно сложно. До сих пор полное доказательство секретности данных протоколов отсутствует. Есть доказательства только для отдельных атак. Трудность связана именно с распределенным кодированием. Ошибка в одном состоянии приводит к ошибкам в соседних состояниях. Все посылки связаны между собой, поэтому получить верхнюю границу утечки информации к подслушивателю при данной наблюдаемой вероятности ошибки на приемной стороне до сих пор никому не удалось. Последнее означает, что длина линии связи, до которой можно гарантировать секретность передаваемых ключей, также неизвестна. Более того, неизвестна критическая ошибка, до которой гарантируется секретность ключей, даже в канале без потерь. Оценки ошибки для протокола DPS в однофотонном случае дают критическую ошибку порядка $4\,\%$, поэтому для канала с потерями и квазиоднофотонных информационных состояний критическая ошибка заведомо будет еще меньше.

Другой подход, применяемый в ряде групп, состоит в использовании состояний ловушек (Decoy State Protocol) [9]. В предыдущих, описанных выше протоколах использовалось фазовое кодирование, когда информация о битах ключа кодировалась в относительную фазу когерентных состояний. Удобнее и короче пояснить данный подход, когда используется кодирование битов ключа в поляризационные степени свободы. Хотя эти рассуждения могут быть перенесены и на протоколы с фазовым кодированием [10]. Ослабленное когерентное состояние имеет также поляризационные степени свободы $|\alpha_i, \sigma_j\rangle$ (σ_j — состояние поляризации). Поскольку пространство состояний двумерное, при числе информационных состояний больше двух такие состояния не являются линейно независимыми по состояниям поляризации, поэтому UM-измерения поляризационных степеней свободы не существуют. Однако это не означает, что подслушиватель не может блокировать линию связи. Вместо UM-атаки возникает PNS-атака (Photon Number Splitting Attack) [10], которая выглядит следующим образом. Поскольку фаза самого когерентного состояния (фаза α) несущественна и меняется произвольно от посылки к по-

сылке, подслушиватель «видит» в канале статистическую смесь по числу фотонов

$$\rho(\mu,\sigma_i)=e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}|n,\sigma_i\rangle\langle n,\sigma_i|, \qquad (1)$$

где σ_j — n-фотонные фоковские состояния с поляризацией σ_j. Неформально (1) означает, что в канале в каждой отдельной посылке присутствует состояние с k фотонами с вероятностью $e^{-\mu}\mu^k/k!$. Квантовая механика допускает неразрушающие измерения по числу фотонов (nondemolishing measurements). Данные измерения даются следующим разложением единицы:

$$I=\sum_{n=0}^{\infty}\left(|n,v\rangle\langle n,v|+|n,h\rangle\langle n,h|\right),$$

где v и h — вертикальное и горизонтальное базисные состояния поляризации. Такое измерение имеет $k=0,1,2,\ldots,\infty$ исходов, которые нумеруются числом фотонов. Если произошел исход k, то это означает, что в канале присутствуют k фотонов. Но поляризация при этом неизвестна.

Если обнаружен один фотон в линии $k=1$, то линия блокируется. Если $k>2$, то часть фотонов подслушиватель сохраняет в квантовой памяти, остальные через канал с меньшими потерями (в идеале без потерь) посылает на приемную сторону. Например, для протокола BB84 состояния внутри каждого базиса ортогональны, поэтому для достоверного различения состояний достаточно однофотонного фоковского состояния. Дождавшись стадии раскрытия базисов, подслушиватель проводит измерения над состояниями в своей квантовой памяти в известном базисе и получает определенный результат с вероятностью единица. Число отводимых фотонов в квантовую память зависит от протокола. Например, в известном протоколе SARG из-за неортогональности состояний внутри базиса требуется два фотона в квантовой памяти для различения состояния поляризации с вероятностью единица [10].

Начиная с некоторого уровня потерь подслушиватель знает весь ключ, не производит ошибок и не детектируется. Передавать ключи, начиная с такой длины линии связи, и гарантировать их секретность нельзя.

Для противодействия данной атаке было предложено использовать состояния с различным средним числом фотонов μ_1 и μ_2 — $\rho(\mu_1,\sigma_i)$ и $\rho(\mu_2,\sigma_i)$ ($\mu_{1,2}<$ <1), которые посылаются в канал случайно [9]. PNS-атака не позволяет различить данные состояния, поскольку каждое из них может давать исход с числом фотонов k. Хотя такие исходы имеют разную вероятность для состояний $\rho(\mu_1,\sigma_i)$ и $\rho(\mu_2,\sigma_i)$, но сказать, от какого состояния, $\rho(\mu_1,\sigma_i)$ или $\rho(\mu_2,\sigma_i)$, исход имел место в каждой посылке, невозможно. Поэтому подслушиватель не знает, сколько фотонов оставить у себя в квантовой памяти. Иначе говоря, оставляя определенное число фотонов в квантовой памяти, на приемную сторону будет отправлено состояние с другим числом фотонов, которое изменит темп отсчетов, поскольку темп отсчетов пропорционален числу фотонов, достигающих приемной стороны.

Данный протокол противоречив по своей сути с самого начала. Однофотонные детекторы не различают число фотонов. Измерение темпа отсчетов явно закладывает в протокол предположения о том, что темп отсчетов пропорционален числу фотонов и что свойства детекторов, включая их квантовую эффективность, не меняются во время передачи ключей. Квантовая эффективность детектора подвержена случайным флуктуациям и реально меняется во время передачи серии состояний. Поэтому для серьезных систем квантовой криптографии использовать ключи, полученные на таких зыбких предположениях, крайне проблематично. Последовательно доказать секретность ключей для данного протокола также нельзя.

2. ФОРМУЛИРОВКА ПРОБЛЕМЫ

Как видно из изложенного выше обсуждения, проблема с передачей ключей на большие расстояния по волоконным линиям связи заключается в том, что когерентные состояния допускают либо UM-измерения, либо PNS-измерения, которые приводят к тому, что, начиная с некоторой критической длины линии связи (соответственно потерь), подслушиватель знает весь ключ и остается недетектируемым. При этом невозможно гарантировать секретность ключей. Ряд протоколов нивелируют UM-измерения, однако возникают проблемы с доказуемостью секретности ключей, ввиду сложности протоколов с распределенным кодированием.

Хотелось бы иметь такой протокол, когда UM-измерения, проводимые подслушивателем, неизбежно и гарантированно приводили бы к возникновению ошибок на приемной стороне даже при больших потерях в линии связи, т. е. протокол не должен оставлять подслушивателя недетектируемым. Кроме того, хотелось бы сохранить простоту анализа криптостойкости протокола и доказуемую секретность

ключей. Важно также сохранить гибкость и простоту технической реализации, а также настраиваемость протокола при передаче ключей через линии связи разной длины. Ниже будет показано, что этим требованиям удовлетворяет протокол с контрольным реперным состоянием, которое само по себе не несет никакой информации, а служит «запретом» на блокирование линии связи. Протокол использует вместе с реперным состоянием два информационных неортогональных состояния, которые могут содержать мезоскопическое среднее число фотонов.

3. МЕЗОСКОПИЧЕСКАЯ КВАНТОВАЯ КРИПТОГРАФИЯ

Предлагаемый подход состоит в запрете UM-измерений в том смысле, что протокол гарантирует возникновение ошибок и детектирование подслушивателя при попытке проведения им UM-измерений. Протокол использует пару неортогональных состояний, что восходит к незаслуженно забытой идее [3]. Кроме того, каждая посылка индивидуальна, что позволяет строго доказать секретность ключей. Протокол может настраиваться на разные длины линии связи и использует мезоскопическое среднее число фотонов в когерентном состоянии (μ может принимать значения от единиц до сотни фотонов в информационном когерентном состоянии). Таким образом, информационные состояния занимают промежуточное число между классическими когерентными состояниями с макроскопически большим числом фотонов и квазиоднофотонными когерентными состояниями со средним числом фотонов меньше единицы. Обычно такие средние числа используют в упомянутых выше протоколах. Мезоскопическое среднее число фотонов уменьшает ошибки на приемной стороне до долей процента, что, в свою очередь, позволяет использовать эффективное исправление ошибок в первичных ключах.

И наконец, в нашем подходе используется консервативная оценка для длины секретного ключа. В квантовой криптографии для вычисления длины секретного ключа требуется связать наблюдаемую ошибку на приемной стороне с утечкой информации к подслушивателю. Достаточно прозрачно и надежно удается связать утечку информации с ошибкой только в строго однофотонном случае, используя фундаментальные энтропийные соотношения неопределенностей [11]. Данные соотношения позволяют, зная только наблюдаемую ошибку на приемной стороне, связать с ней утечку информации к подслушивателю и не перебирать отдельные атаки. К сожалению, данный способ не переносится на случай когерентных состояний, поэтому требуется уметь напрямую оценивать утечку информации для различных атак и их комбинаций, что проблематично, поскольку нет гарантии, что какие-то атаки не пропущены. В нашем подходе, поскольку UM-измерения запрещены (точнее, всегда приводят к ошибкам), можно развязать ошибку на приемной стороне с утечкой информации к подслушивателю. Для верхней границы утечки, независимо от ошибки, необходимо использовать максимальное количество классической информации (границу Холево), которое можно извлечь из квантового ансамбля информационных состояний (см. ниже). Данная граница есть фундаментальный верхний предел информации, извлекаемой из источника квантовых состояний, она не зависит от типа атаки и ошибок на приемной стороне. Разумеется, что такая оценка консервативна в пользу подслушивателя, т. е. завышает полученную им информацию.

4. ПРОТОКОЛ МЕЗОСКОПИЧЕСКОЙ КВАНТОВОЙ КРИПТОГРАФИИ. ПРИМЕР ВОЛОКОННОЙ РЕАЛИЗАЦИИ ПРОТОКОЛА — ОДНОПРОХОДНЫЙ ВАРИАНТ

Протокол может быть реализован как в однопроходных, так и в двупроходных волоконных системах. Приведем для примера лишь однопроходный вариант с интерферометрами Маха – Цандера (рис. 2). Возможны также варианты с другими типами интерферометров.

Передающая часть состоит из лазера, который формирует с определенной тактовой частотой когерентные состояния $|\alpha\rangle$. Далее состояние поступает на волоконный интерферометр Маха – Цандера с разной длиной плеч. Поскольку весь оптический тракт передающей части собран на поляризационно-сохраняющих волокнах, состояние поляризации когерентного состояния остается неизменным от выхода лазера до входа в канал связи. По этой причине символ состояния поляризации в когерентном состоянии опускаем. В коротком плече интерферометра Маха – Цандера имеется управляемый волоконный аттенюатор, также с сохранением поляризации. Его коэффициент ослабления выставляется таким образом, чтобы на выходе интерферометра пара состояний имела следующее среднее число фотонов. Пер-

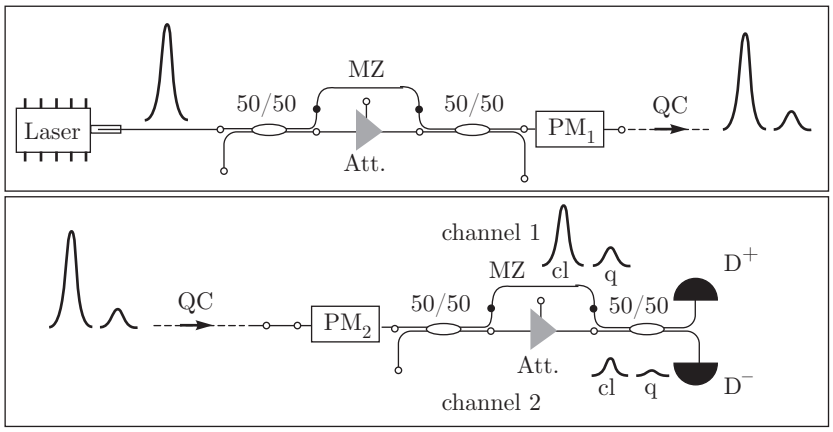

Рис. 2. Функциональная схема волоконной части системы. Обозначения: Laser — источник когерентных состояний, 50/50 — симметричные светоделители, MZ — идентичные интерферометры Маха–Цандера с разной длиной плеч, $PM_{1,2}$ — фазовые модуляторы, cl, q — состояния, происходящие из классического интенсивного и ослабленного когерентных состояний, Att. — управляемый аттенюатор, D^+ — лавинный детектор реперного состояния, D^- — лавинный детектор информационного состояния, QC — квантовый канал связи

вое по времени состояние, прошедшее по короткому пути через аттенюатор, является информационным и содержит мезоскопическое среднее число фотонов $\mu_q = |\alpha_q|^2 \approx 5$–$100$. Второе по времени состояние, прошедшее по длинному пути, является реперным и содержит большее число фотонов по сравнению с первым, и оно тоже является мезоскопическим: $\mu_{cl} = |\alpha_{cl}|^2 \approx 10^2$–$10^6$. Число фотонов зависит от длины линии и подбирается таким образом, чтобы реперный импульс после ослабления в канале связи всегда вызывал срабатывание лавинного однофотонного детектора для проверки наличия реперного состояния. Как показывает опыт, для того чтобы однофотонный лавинный детектор срабатывал на каждое реперное состояние, последнее должно содержать на приемной стороне после канала связи 50–100 фотонов. Это означает, что при длине линии связи в 100 км на стандартном одномодовом волокне с потерями 0.18–0.2 дБ/км число фотонов в реперном состоянии на выходе передающей части должно быть $5 \cdot 10^3$–10^4.

Далее, в момент прохождения информационным состоянием $|\alpha_q\rangle_1$ фазового модулятора прикладывается импульс напряжения, который приводит к сдвигу фазы в зависимости от передаваемого бита ключа.

В итоге в канал поступает длинная серия отдельных независимых посылок. Каждая посылка состоит из пары сдвинутых по времени при помощи интерферометра Маха–Цандера (см. рис. 2) состояний — информационного $|e^{i\varphi}\alpha_q\rangle_1$ и более интенсивного реперного состояния $|\alpha_{cl}\rangle_2$: $|e^{i\varphi}\alpha_q\rangle_1 \otimes |\alpha_{cl}\rangle_2$. Информация о битах ключа кодируется в фазу квантового состояния: $0 \to \varphi_A = 0$, $1 \to \varphi_A = \Delta\varphi$. Значения фаз для 0 и 1 выбираются на передающей и приемной стороне в соответствии с таблицей.

Таблица

Бит	Алиса	Боб
0	$\varphi_A = 0$	$\varphi_B = \Delta\varphi$
1	$\varphi_A = \Delta\varphi$	$\varphi_B = 0$

Потери в канале связи могут меняться во время передачи ключей. Коэффициент ослабления в линии связи длиной L есть $T(L) = 10^{-\delta L/10}$ ($\delta = 0.18$–0.2 дБ/км — коэффициент линейных потерь в одномодовом волокне). При прохождении через канал связи с линейными потерями когерентные состояния ослабляются самоподобным образом:

$$|e^{i\varphi_A}\alpha_q\rangle_1 \otimes |\alpha_{cl}\rangle_2 \to |e^{i\varphi_A}\alpha(T(L))_q\rangle_1 \otimes \otimes |\alpha(T(L))_{cl}\rangle_2.$$

На приемной стороне происходит декодирование — на состояние $|\exp(i\varphi_A)\alpha_q(T(L))/\sqrt{2}\rangle_1$ фазовым модулятором PM2 (см. рис. 2) случайным образом прикладывается компенсирующая фаза φ_B ($0 \to \varphi_B = \Delta\varphi$ либо $1 \to \varphi_B = \Delta\varphi$).

Затем пара состояний направляется на идентичный интерферометр Маха – Цандера, на выходе которого интерферирует друг с другом (конструктивно и деструктивно на двух выходах). Информационные состояния регистрируются в центральном временном окне лавинным однофотонным детектором D^-. Принципиально важно, что интерферируют друг с другом исходное информационное квантовое когерентное состояние и ослабленное до того же уровня интенсивное реперное когерентное состояние.

В интерферометре после первого светоделителя (см. рис. 2) состояния разделяются на два канала:

$$|e^{i\varphi_A}\alpha(T(L))_q\rangle_1 \otimes |\alpha(T(L))_{cl}\rangle_2 \to \left(\begin{array}{c} \left| e^{i(\varphi_A-\varphi_B)}\dfrac{\alpha(T(L))_q}{\sqrt{2}}\right\rangle_1 \otimes \left|\dfrac{\alpha(T(L))_{cl}}{\sqrt{2}}\right\rangle_2 \\ \left| -e^{i(\varphi_A-\varphi_B)}\dfrac{\alpha(T(L))_q}{\sqrt{2}}\right\rangle_1 \otimes \left|-\dfrac{\alpha(T(L))_{cl}}{\sqrt{2}}\right\rangle_2 \end{array} \right) \begin{array}{l} \text{channel 1} \\ \text{channel 2} \end{array}.$$

Поскольку соотношение амплитуд когерентных состояний ($\zeta = |\alpha_{cl}|^2/|\alpha_q|^2$) не меняется по ходу прохождения канала связи и других частей оптического тракта, коэффициент ослабления аттенюатора в приемном интерферометре Маха – Цандера выставляется таким же, как и на передающей стороне, на все время работы протокола. В верхнем и нижнем плечах интерферометра после прохождения аттенюатора и сдвига по времени состояния становятся равными

$$\left(\begin{array}{c} |\mathrm{vac}\rangle_1 \otimes \left| e^{i(\varphi_A-\varphi_B)}\dfrac{\alpha(T(L))_q}{\sqrt{2}}\right\rangle_2 \otimes \left|\dfrac{\alpha(T(L))_{cl}}{\sqrt{2}}\right\rangle_3 \\ \left| -e^{i(\varphi_A-\varphi_B)}\dfrac{\alpha(T(L))_q}{\sqrt{2\zeta}}\right\rangle_1 \otimes \left|-\dfrac{\alpha(T(L))_q}{\sqrt{2}}\right\rangle_2 \otimes |\mathrm{vac}\rangle_3 \end{array} \right) \begin{array}{l} \text{channel 1} \\ \text{channel 2} \end{array}.$$

На выходе интерферометра состояния на верхнем и нижнем выходах в трех временных окнах оказываются равными

$$\left(\begin{array}{c} \left| e^{i(\varphi_A-\varphi_B)}\dfrac{\alpha(T(L))_q}{2\zeta}\right\rangle_1 \otimes \left|(e^{i(\varphi_A-\varphi_B)}+1)\dfrac{\alpha(T(L))_q}{2}\right\rangle_2 \otimes \left|\dfrac{\alpha(T(L))_{cl}}{2}\right\rangle_3 \\ \left| -e^{i(\varphi_A-\varphi_B)}\dfrac{\alpha(T(L))_q}{2\zeta}\right\rangle_1 \otimes \left|(e^{i(\varphi_A-\varphi_B)}-1)\dfrac{\alpha(T(L))_q}{2}\right\rangle_2 \otimes \left|\frac{\alpha(T(L))_{cl}}{2}\right\rangle_3 \end{array} \right) \begin{array}{l} \text{channel 1} \\ \text{channel 2} \end{array}.$$

Информация о битах ключа возникает при измерениях при помощи однофотонного лавинного детектора D^- во временном окне 2 состояния

$$\left|\left(e^{i(\varphi_A-\varphi_B)}-1\right)\frac{\alpha(T(L))_q}{2}\right\rangle_2.$$

Наличие реперного состояния проверяется при измерении лавинным однофотонным детектором D^+ во временно́м окне 3 состояния $|\alpha(T(L))_{cl}/2\rangle_3$. Поскольку однофотонные лавинные детекторы работают в стробируемом режиме, требуется сигнал синхронизации, который может передаваться с передающей станции на приемную либо по отдельной волоконной линии, либо по той же самой через WDM (Wave Length Demultiplexer) на другой длине волны (например, 1310 нм, если информационные состояния передаются на длине волны 1550 нм, и наоборот).

Через открытый канал проверяется число посланных и зарегистрированных классических импульсов. При обнаружении несовпадения их числа вся серия отбрасывается. При совпадении числа посланных и зарегистрированных реперных импульсов обработка первичных ключей продолжается аналогично другим протоколам квантового распределения ключей.

5. НЕФОРМАЛЬНЫЕ ПРИЧИНЫ СЕКРЕТНОСТИ КЛЮЧЕЙ

Поясним неформальные причины, по которым подслушиватель не может проводить UM-измерения, не создавая при этом ошибок на приемной стороне.

Поскольку информация о ключе кодируется в фазу ослабленных когерентных состояний, подслушиватель должен различать одно из неортогональных состояний $|e^{(\varphi_A=0)}\alpha_q\rangle$ и $|e^{(\varphi_A=\Delta\varphi)}\alpha_q\rangle$ (считаем в пользу подслушивателя, что фаза α_q известна, например, из реперного состояния). Подслушиватель, в случае неопределенного исхода «?» при различении информационных квантовых состояний, не может блокировать интенсивное реперное состояние (иначе вся серия будет отброшена). Поэтому вместо истинного ослабленного информационного квантового состояния подслушиватель вынужден будет послать, например, состояние $|e^{(\varphi_A=0)}\alpha_q\rangle$, состояние наугад ($|e^{(\varphi_A=0)}\alpha_q\rangle$ или $|e^{(\varphi_A=\Delta\varphi)}\alpha_q\rangle$, или любое другое, например, вакуумное, т. е. ничего не посылать), что при интерференции с ослабленным реперным импульсом приведет к ошибке. Таким образом, подслушиватель никогда не сможет знать весь ключ и не производить ошибок на приемной стороне. Если бы не было реперного импульса, с которым интерферирует информационное состояние, подслушиватель мог бы блокировать посылки, в которых получен неопределенный исход (?) при UM-измерениях.

При наличии реперного состояния UM-измерения гарантированно приводят к ошибкам на приемной стороне, поэтому исключается ситуация, которая имеет место в других протоколах, приведенных выше, когда начиная с некоторых потерь подслушиватель знает весь ключ, не производит ошибок на приемной стороне и не детектируется.

6. ВЫЧИСЛЕНИЕ ДЛИНЫ СЕКРЕТНОГО КЛЮЧА: КОНСЕРВАТИВНАЯ ОЦЕНКА

Критерием секретности в квантовой криптографии является следовое расстояние между реальной и идеальной ситуациями, когда корреляции между квантовой системой подслушивателя и секретным ключом отсутствуют [12]:

$$\frac{1}{2}||\rho_{XE}-\rho_U\otimes\rho_E||_1<\varepsilon,$$

где следовое расстояние $||\rho||_1=\mathrm{Tr}\{|\rho|\}$.

Протокол ε-секретен, если длина секретного ключа R удовлетворяет условию

$$R\le H^{\varepsilon}_{min}(X|E)-\mathrm{leak}-2\log_2\left(\frac{1}{\varepsilon}\right).$$

Здесь $X=\{0,1\}^n$ — битовая последовательность легитимных пользователей, n — число зарегистрированных посылок на приемной стороне, leak — количество битов классической информации, раскрытой через аутентичный классический канал связи при коррекции ошибок в сырой последовательности длины n. Далее, $H^{\varepsilon}_{min}(X|E)$ — сглаженная минимальная энтропия [12]

$$H^{\varepsilon}_{min}(X|E)=\sup_{\overline{\rho}_{XE}}H_{min}(X|E),$$

где супремум берется по всем матрицам плотности, лежащим внутри шара $||\overline{\rho}_{XE}-\rho_{XE}||_1<\varepsilon$, и по определению

$$H_{min}(X|E)=-\log_2\lambda,$$

где λ минимальное число, такое что $\lambda I_X\otimes\rho_E-\rho_{XE}\ge$ ≥ 0, $I_X=\sum_{x\in X}|x\rangle\langle x|$ — единичный оператор.

Оценим величину сглаженной условной энтропии $H^{\varepsilon}_{min}(X|E)$. Матрица плотности, коррелированная с битовой строкой легитимных пользователей, имеет вид

$$\rho_{XE}=\sum_{x\in X}P_X(x)|x\rangle\langle x|\otimes\rho^x_E,\quad |x\rangle=|x_1\rangle\otimes|x_2\rangle\ldots|x_n\rangle.$$

Матрица плотности на входе в канал связи есть

$$\rho^x_E=\rho^{x_1}_E\otimes\rho^{x_2}_E\otimes\ldots\rho^{x_n}_E.$$

Для условной сглаженной минимальной энтропии для тензорного произведения имеет место оценка (см. детали в [12])

$$H^{\varepsilon}_{min}(\rho^{\otimes n}_{XE}|\rho^{\otimes n}_E)\ge n\left(H(\rho_{XE})-H(\rho_E)-\delta_n\right),$$

$$\delta_n=(2H_{max}(\rho_X)+3)\sqrt{\frac{\log_2\left(\dfrac{1}{\varepsilon}\right)}{n}+1},$$

здесь $H_{max}(\rho_X)=\log_2(\mathrm{rank}(\rho_X))$.

Консервативная оценка в пользу подслушивателя состоит в следующем. Поскольку UM-измерения запрещены, остается одна возможность — атаковать передаваемые состояния унитарно. Таким образом, подслушиватель в каждой посылке независимо использует свою вспомогательную квантовую систему, которую запутывает с передаваемым состоянием. Искаженное информационное состояние передается далее на приемную сторону, а искаженная и коррелированная с информационным состоянием квантовая система сохраняется в квантовой памяти. После посылки всей серии и коррекции ошибок через классический канал подслушиватель делает коллективные измерения над всем регистром квантовой памяти при помощи измерений, максимизирующих классическую информацию, извлекаемую из квантового регистра. Запутывание и искажение информационного квантового состояния приводит к ошибкам на

приемной стороне. Цель такой атаки для подслушивателя — подобрать взаимодействие таким образом, чтобы при заданной вероятности ошибки на приемной стороне получить максимум классической информации при коллективных измерениях — граница Холево [13]. Консервативный подход состоит в том, чтобы развязать поток ошибок на приемной стороне с количеством информации, получаемой подслушивателем. Существует фундаментальная верхняя граница для классической информации, которую можно извлечь из квантового анасамбля состояний. Поэтому консервативно будем считать, что подслушиватель получает этот максимум информации. А утечка информации при коррекции ошибок (leak) определяется по факту при коррекции ошибок.

Фактически это означает, что в качестве состояний, доступных для измерений подслушивателя, надо использовать сами информационные состояния на входе в канал с передающей стороны:

$$\begin{aligned}\rho_E^{x=0} &= |e^{i\varphi_0}\alpha_q\rangle_{11}\langle e^{i\varphi_0}\alpha_q|,\\ \rho_E^{x=1} &= |e^{i\varphi_1}\alpha_q\rangle_{11}\langle e^{i\varphi_1}\alpha_q|.\end{aligned} \tag{2}$$

С учетом сказанного и (2) получаем

$$H(\rho_{XE}) = H(\rho_X) - \sum_{x=0,1} p_X(x) H(\rho_E^x),$$

$$H(\rho_E) = H\left(\frac{\rho_E^{x=0}+\rho_E^{x=1}}{2}\right),$$

$$\rho_X = \frac{1}{2}\sum_{x=0,1}|x\rangle\langle x|, \quad \rho_E = \frac{\rho_E^{x=0}+\rho_E^{x=1}}{2}.$$

Считая, что биты ключа выбираются на передающей стороне равновероятно, $p_x(x=0) = p_X(x=1) = 1/2$, а также что выходные состояния чистые, получаем

$$H(\rho_{XE}) - H(\rho_E) = 1 - \chi(\rho_E),$$

$$\chi(\rho_E) = H\left(\frac{\rho_E^{x=0}+\rho_E^{x=1}}{2}\right) = \overline{C}(\rho_E),$$

$\chi(\rho_E)$ — в точности величина фундаментальной границы Холево для ансамбля чистых состояний [13], которая также равна классической пропускной способности идеального квантового канала связи с входными состояниями (2).

В итоге для консервативной оценки длины секретного ключа получаем

$$R \le n\left(1 - \overline{C}(\rho_E) - \delta_n\right) - \text{leak} - 2\log_2\left(\frac{1}{\varepsilon}\right),$$

где классическая пропускная способность идеального квантового канала связи [13]

$$\overline{C}(\rho_E) = -\frac{1-\zeta}{2}\log_2\left(\frac{1-\zeta}{2}\right) - \frac{1+\zeta}{2}\log_2\left(\frac{1+\zeta}{2}\right),$$

где

$$\zeta = \exp\left\{-2|\alpha_q|^2\sin^2\left(\frac{\Delta\varphi}{2}\right)\right\} = \exp\left\{-2\mu_q\sin^2\left(\frac{\Delta\varphi}{2}\right)\right\}. \tag{3}$$

Данные формулы имеют простую качественную интуитивную интерпретацию. Пусть на приемной стороне зарегистрировано n состояний, возможно, с некоторой вероятностью ошибки. Пусть при коррекции ошибок раскрыто leak битов классической корректирующей информации через открытый аутентичный канал связи. Данная информация доступна подслушивателю. Легитимный пользователь на приемной стороне после коррекции ошибок знает все n битов. Из n квантовых состояний подслушиватель (имея доступ напрямую к источнику) может получить не более $n\overline{C}(\rho_E)$ битов классической информации. В итоге подслушиватель из n битов знает не более $n\overline{C}(\rho_E)$ + leak битов информации, соответственно, не знает $n(1-\overline{C}(\rho_E))$ – leak битов, которые и составляют секретный ключ. Слагаемые с δ_n и ε учитывают флуктуации, связанные с поправками на конечную длину передаваемой последовательности.

7. СВЯЗЬ ПАРАМЕТРОВ ПРОТОКОЛА С ДЛИНОЙ ЛИНИИ СВЯЗИ

Для вычисления дальности и скорости передачи ключей нам потребуется связь параметров протокола с длиной линии. Существует оптимальное соотношение между средним числом фотонов в информационном когерентном состоянии, углом $\Delta\varphi$ между состояниями, отвечающими информационным битам ключа 0 и 1, вероятностью темновых шумов лавинного детектора на строб p_d и длиной линии. Среднее число фотонов в реперном состоянии будет определяться из требования гарантированного детектирования реперных состояний при заданной длине линии. Кроме того, число фотонов в реперном состоянии должно быть минимально возможным для избежания дополнительных засветок в линии.

7.1. Число регистрируемых состояний на приемной стороне

Определим сначала число регистрируемых информационных состояний. Информационные состояния регистрируются одним однофотонным лавинным детектором (второй служит для регистрации реперных состояний), поэтому отсчеты в информационном детекторе (channel 2, см. рис. 2) имеют место только в том случае, когда Алиса выбрала значение $\varphi_A = 0$, отвечающее 0, и Боб также выбрал значение, отвечающее 0, $\varphi_B = \Delta\varphi$. И соответственно, наоборот, Алиса выбрала $\varphi_A = \Delta\varphi$, Боб — $\varphi_B = 0$. В других случаях срабатывания детектора в канале 2 (channel 2, см. рис. 2) не происходит. Именно по тем посылкам, где срабатывания детектора не должно быть, а оно имело место, происходит детектирование подслушивателя. Отсчеты могут также происходить из-за темновых шумов. Данные ошибки также списываются на действия подслушивателя. В ряде работ [14] для увеличения дальности темновые шумы вычитаются, что принципиально неверно и приводит к завышению длины линии, до которой гарантируется секретность ключей.

Информационные состояния регистрируются во временном окне 2 однофотонным лавинным детектором. С учетом того, что детектор не реагирует на вакуумную компоненту состояния

$$\left| \left(e^{i(\varphi_A - \varphi_B)} - 1 \right) \frac{\alpha(T(L))_q}{2} \right\rangle_2,$$

вероятность регистрации детектором имеет место, если $\varphi_A - \varphi_B = \Delta\varphi$. Имеем

$$\begin{aligned} \mathrm{Eff}(\mu_q, \Delta\varphi, \eta, L) &= \\ &= 1 - \exp\left\{ -\eta |\alpha_q(T(L))|^2 \sin^2\left(\frac{\Delta\varphi}{2}\right) \right\} = \\ &= 1 - \exp\left\{ -\eta \mu_q T(L) \sin^2\left(\frac{\Delta\varphi}{2}\right) \right\} \approx \\ &\approx \eta \mu_q T(L) \sin^2\left(\frac{\Delta\varphi}{2}\right). \end{aligned} \quad (4)$$

Как видно из формулы (4), вероятность регистрации посланного информационного состояния при заданной длине линии L и квантовой эффективности лавинного детектора η определяется произведением среднего числа фотонов на квадрат синуса угла относительной фазы между ними. Это два независимых параметра, которые должны выбираться из соображений максимальной скорости и дальности передачи ключей. Для определения оптимального соотношения между этими параметрами нам потребуется выражение для ошибки за счет темновых шумов лавинного детектора.

7.2. Наблюдаемая ошибка на приемной стороне

Поскольку любые наблюдаемые ошибки на приемной стороне приходится списывать на действие подслушивателя, для определения дальности передачи ключей необходимо получить выражение для ошибки. Система должна передавать ключи и в отсутствие подслушивателя. В этом случае все ошибки на приемной стороне определяются несовершенством аппаратуры: темновыми шумами лавинных детекторов, неидеальной видностью интерферометра и т. д. Утечка информации при исправлении ошибок (leak) однозначно связана с уровнем ошибок при выбранной процедуре коррекции ошибок. Считая, что все ошибки возникают за счет темновых шумов, для определения предельной дальности передачи секретных ключей необходимо использовать выражение для вероятности ошибок, которое зависит от длины линии. Длина линии L, при которой длина секретного ключа обращается в нуль, определяет предельное расстояние, до которого можно гарантировать секретность ключей.

Наблюдаемая ошибка от темновых шумов на приемной стороне есть

$$Q(\mu_q, \Delta\varphi, \eta, p_d, L) = \frac{1}{2} \frac{p_d}{p_d + \mathrm{Eff}(\mu_q, \Delta\varphi, \eta, L)}. \quad (5)$$

Данное выражение имеет простую интерпретацию. При длинной переданной последовательности отсчеты от информационных состояний составят долю $\mathrm{Eff}(\mu_q, \Delta\varphi, \eta, L)$. Эти отсчеты будут в тех посылках, где Алиса и Боб синхронно выбрали значения фаз, отвечающих либо 0, либо 1. Если были выбраны противоположные значения фаз, например, Алиса для 0, а Боб для 1, и наоборот, то отсчета от информационных состояний не будет. Однако отсчет может произойти из-за темновых шумов с вероятностью p_d. Все отсчеты — редкие события, поэтому даже при синхронном выборе значений фаз отсчет от информационного состояния будет иметь место далеко не в каждой посылке. Поэтому в половине посылок значения фаз синхронны, а в половине — нет. И половина отсчетов за счет темновых шумов будет иметь место в тех посылках, где фазы Алисы и Боба были синхронны, а половина — в посылках, где фазы противоположны. Полная вероятность отсчетов от информационных состояний и шумов есть $p_d + \mathrm{Eff}(\mu_q, \Delta\varphi, \eta, L)$. В доле посылок $p_d/2$ темновые

шумы приведут к ошибкам. В итоге возникает формула (5).

Данные рассуждения справедливы с точностью до квадратичных членов по p_d и $\mathrm{Eff}(\mu_q, \Delta\varphi, \eta, L)$. Таким образом, вероятность события, когда происходит темновой отсчет и регистрация информационного состояния в одном временном окне, крайне ничтожна (например, при длине линии 100 км вероятность такого события $p_d\mathrm{Eff}(\mu_q, \Delta\varphi, \eta, L) < 10^{-10}$).

7.3. Среднее число фотонов в реперном состоянии

Сформулируем требования к среднему числу фотонов в реперном состоянии. Среднее число фотонов зависит от длины линии. Требуется, чтобы на приемной стороне каждое реперное состояние вызывало отсчет контрольного однофотонного детектора, который следит за сохранением числа реперных импульсов. Как показывает опыт, однофотонный лавинный детектор срабатывает на каждый импульс, если среднее число фотонов $\mu_{cl} \approx 50$–100. При малых числах фотонов темп отсчетов лавинного детектора, работающего в счетном режиме, пропорционален среднему числу фотонов $\mu_{cl}T(L)$. Поэтому при типичной квантовой эффективности $\eta \approx 20\,\%$ вероятность срабатывания детектора $\Pr \approx 1$, т. е. срабатывание происходит на каждый импульс.

Для гарантированной регистрации реперного состояния число фотонов на входе лавинного детектора должно быть приблизительно равно 100. Например, при длине линии 100 км потери в линии $T(L = 100) = 10^{-0.2L/10} = 10^{-2}$ и среднее число фотонов на входе в линию связи должно быть примерно 10^4. Соответственно, при длине линии $L = 50$ км достаточно 10^3 фотонов в реперном состоянии. При длине линии $L = 250$ км требуется среднее число фотонов $\mu_{cl} \approx 10^7$.

Отметим, что среднее число фотонов в информационном когерентном состоянии на входе в линию должно каждый раз быть одинаково. Оптимальное значение определяется ниже.

Отметим важный технический момент. Перепад по числу фотонов в реперном и информационном состояниях при длине линии $L = 250$ км имеет порядок $\mu_{cl}/\mu_q = 10^7/50 = 2{\cdot}10^5$. Стандартные электронно-управляемые варьируемые волоконные аттенюаторы дают ослабление 60 дБ, что достаточно для достижения данного перепада по среднему числу фотонов в реперном и информационном состояниях.

7.4. Предел бесконечных последовательностей

Эффективная длина секретного ключа на каждую зарегистрированную посылку вычисляется как

$$r = \mathrm{Eff}(\mu_q, \Delta\varphi, \eta, L)\left(1 - \overline{C}(\zeta(L)) - \mathrm{leak}\right)$$

и нормированная длина секретного ключа

$$R = \left(1 - \overline{C}(\zeta(L)) - \mathrm{leak}\right),$$

здесь leak — количество раскрытых битов при коррекции ошибок в пересчете на зарегистрированную посылку, которое зависит от используемой процедуры. В асимптотическом шенноновском пределе при вероятности ошибки $Q = 0.05\%$ после исправления ошибок остается $1 - \mathrm{leak} = 1 - h(Q) = 0.955$ битов в пересчете на посылку, где

$$h(Q) = -Q\log_2(Q) - (1 - Q)\log_2(1 - Q)$$

— шенноновская бинарная энтропийная функция. При наблюдаемой вероятности ошибки (4) (рис. 3, 4) можно использовать корректирующие коды Хэмминга с такой длиной блока, чтобы в каждом кодовом слове в среднем была одна ошибка. Если использовать код с длиной кодового слова в 127 бит ($2^m - 1$, $m = 7$, соответственно, проверочных $m = 7$), то скорость кода

$$\frac{2^m - 1 - m}{2^m - 1} = 0.945.$$

Поэтому в данной области ошибок можно воспользоваться интерполяционной формулой для величины утечки информации при коррекции ошибок:

$$1 - fh(Q) = 0.945,$$

где $f = 1.22$.

8. ОСЛАБЛЕНИЕ КОНСЕРВАТИВНОЙ ОЦЕНКИ ДЛЯ ДЛИНЫ СЕКРЕТНОГО КЛЮЧА

При консервативной оценке информации, доступной подслушивателю, мы считали, что подслушиватель извлекает максимум доступной информации из квантового ансамбля, допускаемый квантовой механикой, при этом не искажая самих состояний. Такая оценка является завышенной в пользу подслушивателя, и ее можно несколько ослабить. Хотя данная граница Холево [13] и достижима, но только при наличии кодовой таблицы.

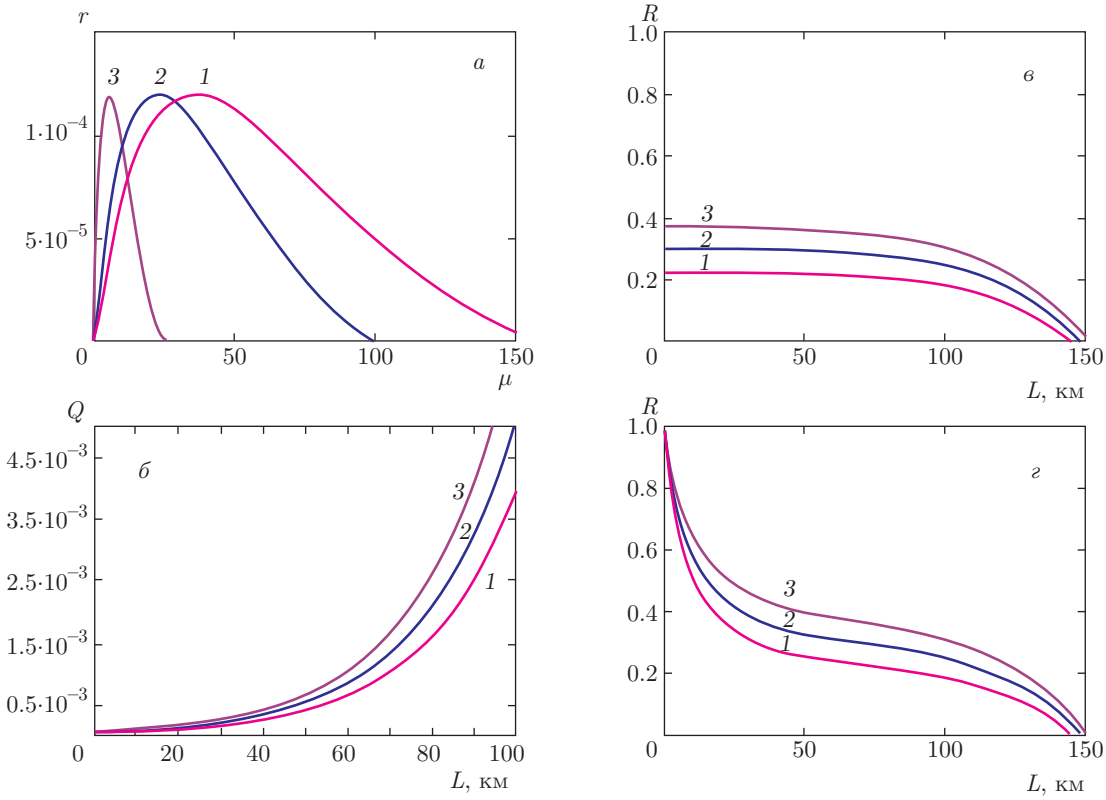

Рис. 3. *а*) Зависимости доли секретных битов на посылку как функции среднего числа фотонов в информационном состоянии при длине линии связи 100 км. *б*) Зависимости наблюдаемой ошибки на приемной стороне за счет темновых шумов в сыром ключе от длины линии связи. *в*) Зависимости нормированной длины секретного ключа при консервативной оценке от длины линии связи. *г*) Зависимости нормированной длины секретного ключа в случае ослабленной консервативной оценки от длины линии связи. Общие параметры для кривых: $\Delta\varphi = \pi/20$ (*1*), $\pi/16$ (*2*), $\pi/8$ (*3*), среднее число фотонов в информационном состоянии для кривых рис. *а, б* равно $\mu_q = 50$ (*1*), 25 (*2*), 5 (*3*). Вероятность темновых шумов на строб для всех рисунков $p_d = 5 \cdot 10^{-6}$, квантовая эффективность однофотонного детектора $\eta = 20\,\%$, потери в волокне $\delta = 0.2$ дБ/км

Неформально это означает следующее. Передающая сторона оглашает публично, что из всех возможных 2^n последовательностей информационных состояний (0 и 1 выбираются равновероятно в нашем случае) случайно заранее будут сгенерированы только $2^{n\overline{C}(\rho_E)}$ последовательностей. И только эти последовательности будут передаваться. В этом случае максимальное количество битов классической информации в пересчете на посылку будет $\overline{C}(\rho_E)$. В этой ситуации подслушиватель в асимптотическом пределе длинных последовательностей может идентифицировать каждую кодовую последовательность безошибочно и перепослать ее на приемную сторону.

В реальности никакой кодовой таблицы при передаче информационных состояний нет. Поэтому консервативное допущение, что подслушиватель может различить достоверно (в асимптотическом смысле) каждую передаваемую последовательность является слишком жестким.

В реальной ситуации подслушиватель может через светоделитель отвести в квантовую память часть когерентных состояний — реперное и информационные (рис. 5), а остальную часть направить на приемную сторону через канал без потерь, чтобы состояния целиком дошли до приемника. Поскольку интенсивность реперного состояния подобрана таким образом, чтобы после потерь в линии связи оно давало гарантированный отсчет, подслушиватель не может отвести долю более, чем $1 - T(L)$.

Это означает, что для более реалистичной ослабленной оценки нужно использовать следующее выражение вместо (2):

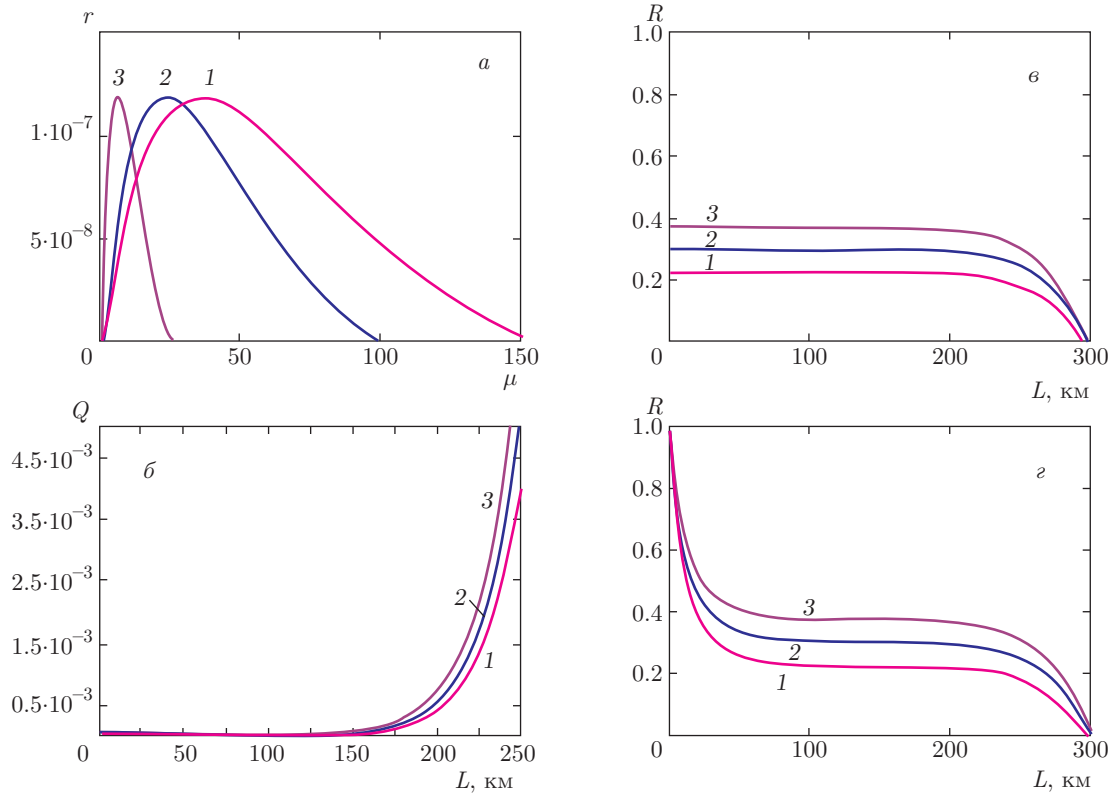

Рис. 4. *а*) Зависимости доли секретных битов на посылку как функции среднего числа фотонов в информационном состоянии при длине линии связи 250 км. *б*) Зависимости наблюдаемой ошибки на приемной стороне за счет темновых шумов в сыром ключе от длины линии связи. *в*) Зависимости нормированной длины секретного ключа при консервативной оценке от длины линии связи. *г*) Зависимости нормированной длины секретного ключа в случае ослабленной консервативной оценки от длины линии связи. Общие параметры для кривых: $\Delta\varphi = \pi/20$ (*1*), $\pi/16$ (*2*), $\pi/8$ (*3*), среднее число фотонов в информационном состоянии для кривых рис. *а, б,* равно $\mu_q = 50$ (*1*), 25 (*2*), 5 (*3*). Вероятность темновых шумов на строб для всех рисунков $p_d = 5 \cdot 10^{-9}$, квантовая эффективность однофотонного детектора $\eta = 20\,\%$, потери в волокне $\delta = 0.2$ дБ/км

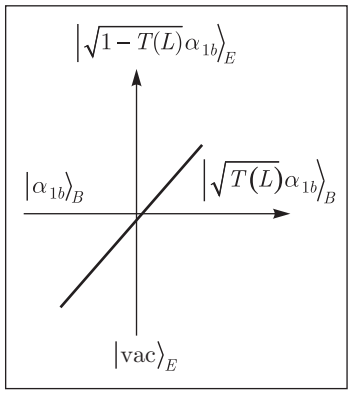

Рис. 5. Атака со светоделителем

$$\zeta(L) = \exp\left\{-2|\alpha_q|^2 \sin^2\left(\frac{\Delta\varphi}{2}\right)(1-T(L))\right\} = \exp\left\{-2\mu_q \sin^2\left(\frac{\Delta\varphi}{2}\right)(1-T(L))\right\}.$$

Однако отметим, что расчеты длины ключа и скорости передачи при консервативной оценке и оценке в более реалистической ситуации мало различаются. Различие наблюдается только на малых длинах линии связи, где потери малы и подслушиватель практически ничего не может отвести через светоделитель. Для сравнения данные приведены на рис. 3, 4. На длине финального ключа это сказывается только через величину $\overline{C}(\rho_E)$.

9. ДАЛЬНОСТЬ И СКОРОСТЬ ПЕРЕДАЧИ СЕКРЕТНЫХ КЛЮЧЕЙ. КОНЕЧНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ

Обсудим теперь эффект конечных передаваемых последовательностей на длину секретного ключа. Параметром секретности является ε — следовое рас-

стояние реальной ситуации до идеальной, когда финальный ключ и квантовая система подслушивателя полностью не коррелированы. Данный параметр выбирается в зависимости от использования секретных ключей. Этот параметр определяет изменение сложности перебора ε-секретных ключей, которые используются в алгоритмах шифрования, по сравнению с идеальными ключами. Параметр также определяет число шифрсообщений, каждое из которых шифруется на своем ε-секретном ключе, до дешифрования первого сообщения (см. подробности в работе [15]).

Будем исходить из значения параметра $\varepsilon = 2^{-32} \approx 10^{-9}$. Вопрос, на который требуется ответить, состоит в том, сколько нужно передать посылок при заданных параметрах системы и длине линии, чтобы получить ε-секретный ключ длиной 256 бит. Ключ такой длины используется в прежнем Российском стандарте шифрования ГОСТ 28147-89 и новом стандарте шифрования ГОСТ 32.11-15 («Кузнечик»).

10. УСТОЙЧИВОСТЬ ПРОТОКОЛА ПО ОТНОШЕНИЮ К UM-АТАКЕ БЕЗ БЛОКИРОВАНИЯ КВАНТОВОГО КАНАЛА

Обсудим для полноты картины один из вариантов UM-атаки, при которой подслушиватель не блокирует линию связи, если им получен неопределенный исход «?», при котором подслушиватель не знает передаваемого состояния.

Возможна ли UM-атака, при которой канал не блокируется в случае исхода «?», сохраняется число зарегистрированных реперных импульсов на приемной стороне, подслушиватель знает весь ключ и никак не детектируется? Оказывается, что такая атака, при которой подслушиватель никак не детектируется, невозможна.

UM-атака, когда канал не блокируется, состоит в следующем. При большой длине линии связи подслушиватель отводит часть передаваемых состояний через асимметричный светоделитель с коэффициентом деления $(\sqrt{1-T(L)}, \sqrt{T(L)})$. Состояния $|\alpha\sqrt{T(L)}\rangle$ в канале светоделителя подслушиватель сохраняет в квантовой памяти до момента получения результата UM-измерений над состояниями $|\alpha\sqrt{1-T(L)}\rangle$ на втором выходе светоделителя. Если получен определенный исход, то подслушиватель посылает на приемную сторону правильные состояния, но большей интенсивности чем исходные, чтобы они были гарантированно зарегистрированы на приемной стороне. В этих посылках, где был определенный исход, подслушиватель знает все состояния и не производит ошибок.

Если получен неопределенный исход «?», подслушиватель посылает через идеальный канал на приемную сторону состояния $|\alpha\sqrt{T(L)}\rangle$. Здесь важно подчеркнуть следующее. Без подслушивателя из-за потерь в линии связи на приемной стороне будут регистрироваться состояния $|\alpha\sqrt{T(L)}\rangle$. Если послано n состояний, то будет зарегистрировано

$$n\mathrm{Eff}(\mu_q, \Delta\varphi, \eta, L) \approx n\eta\mu_q T(L)\sin^2\left(\frac{\Delta\varphi}{2}\right)$$

состояний (см. формулу (4)). Важно, что это полное число информационных состояний, регистрируемых на приемной стороне без подслушивателя.

При обсуждаемой атаке число регистрируемых информационных состояний оказывается равным

$$\begin{aligned} &n(1-\Pr(?)) + n\Pr(?)\overline{\mathrm{Eff}} \gg n\overline{\mathrm{Eff}}, \\ &\overline{\mathrm{Eff}} = \mathrm{Eff}(\mu_q, \Delta\varphi, \eta, L), \end{aligned} \tag{6}$$

где

$$\begin{aligned} \Pr(?) = \zeta(L) &= \\ &= \exp\left\{-2|\alpha_q|^2\sin^2\left(\frac{\Delta\varphi}{2}\right)(1-T(L))\right\} = \\ &= \exp\left\{-2\mu_q\sin^2\left(\frac{\Delta\varphi}{2}\right)(1-T(L))\right\} \end{aligned}$$

— вероятность неопределенного исхода. Это существенно больше, чем должно быть зарегистрировано в отсутствие подслушивателя. При этом, естественно, реперный импульс регистрируется в каждой посылке. Таким образом, все реперные импульсы регистрируются, а число регистрируемых информационных состояний радикально увеличивается. На рис. 6*a* показано изменение числа регистрируемых информационных состояний при такой атаке как функция длины линии связи. Как видно на рис. 6*a*, при длине линии в 100 км происходит увеличение темпа отсчетов от квантовых информационных импульсов в 10^4 раз, что легко детектируется.

Покажем теперь, что при такой атаке всегда будет происходить изменение темпа отсчетов информационных состояний. Рассуждения проведем от противного. Пусть подслушиватель проводит UM-измерения только в ξn посылках из полного числа. Допустим, что при этом число регистрируемых информационных посылок сохраняется. Тогда вместо (6) получим

$$\begin{aligned} \xi n(1-\Pr(?)) + \xi n\Pr(?)\overline{\mathrm{Eff}} + n(1-\xi)\overline{\mathrm{Eff}} = \\ = n\overline{\mathrm{Eff}}. \end{aligned} \tag{7}$$

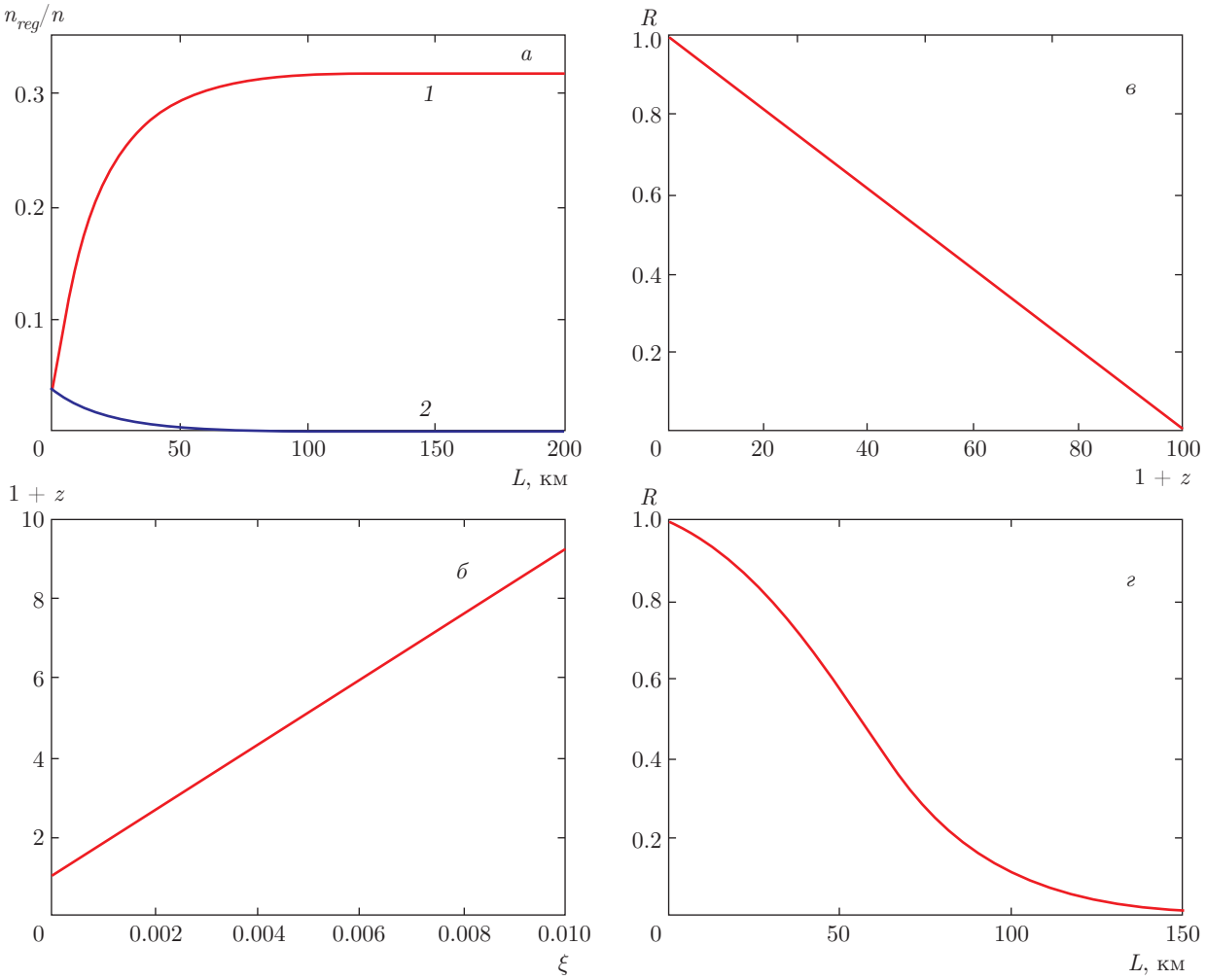

Рис. 6. *а*) Зависимости доли n_{reg}/n регистрируемых информационных состояний как функции длины линии связи. Кривая *1* — доля зарегистрированных посылок по отношению к посланным как функция длины линии связи в случае, когда подслушиватель перепосылает «яркие» состояния в посылках, где был получен определенный исход. Кривая *2* — доля регистрируемых состояний по отношению к посланным в отсутствие подслушивателя (порядок величины составляет 10^{-4}). *б*) Зависимость доли превышения регистрируемых информационных состояний над номинальным значением как функция доли атакуемых посылок при помощи UM-измерений. Длина линии связи $L = 100$ км. *в*) Зависимость нормированной длины ключа (формула (11)) как функция доли превышения регистрируемых информационных состояний над номинальным значением. Параметр $L = 100$ км. *г*) Зависимость нормированной длины секретного ключа как функция длины линии связи. Параметры: $\xi = 0.01$, $1 + z = 10$. Общие параметры: $\mu_q = 5$, $\Delta\varphi = \pi/8$, $p_d = 5 \cdot 10^{-6}$ отсч./строб, $\eta = 20\,\%$, потери в волокне $\delta = 0.2$ дБ/км

Из (7) видно, что имеется единственное решение $\xi = 0$. Таким образом, проведение UM-атаки неизбежно будет приводить к изменению числа регистрируемых информационных состояний по отношению к правильному числу $n\mathrm{Eff}(\mu_q, \Delta\varphi, \eta, L)$.

Пусть подслушиватель проводит UM-атаку только над долей ξ состояний из полного числа посланных n. Напомним, что в числе посылок $n(1 - \Pr(?))$ подслушиватель посылает «яркие» состояния, которые заведомо будут зарегистрированы. Остальные посылки подслушивателю неизвестны. При этом возникнет превышение числа регистрируемых информационных состояний $n(1 + z)\mathrm{Eff}(\mu_q, \Delta\varphi, \eta, L)$, где z — доля превышения. Найдем связь между ξ и z. Получаем

$$\xi n(1 - \Pr(?)) + \xi n \Pr(?)\overline{\mathrm{Eff}} + n(1 - \xi)\overline{\mathrm{Eff}} = \\ = n(1 + z)\overline{\mathrm{Eff}}, \quad (8)$$

откуда

$$z(\xi) = \xi \frac{(1 - \Pr(?))(1 - \overline{\mathrm{Eff}})}{\overline{\mathrm{Eff}}}. \qquad (9)$$

На рис. 6*б* показана зависимость доли превышения регистрируемых информационных состояний $1 + z(\xi)$ как функция доли атакуемых посылок ξ. Как видно на рис. 6*б*, проведение UM-измерений в 1 % посылок приводит к увеличению числа регистрируемых информационных состояний в 10 раз, что легко детектируется.

Найдем теперь длину секретного ключа. Несложно видеть, что длина секретного ключа с учетом (8), (9) равна

$$r = n(1 - \xi(1 - \Pr(?)))\overline{\mathrm{Eff}}, \qquad (10)$$

соответственно, нормированная длина секретного ключа в пересчете на число зарегистрированных информационных состояний $n(1 + z(\xi))\overline{\mathrm{Eff}}$ равна

$$R = \frac{1 - \xi(1 - \Pr(?))}{1 + z(\xi)}. \qquad (11)$$

Пусть обнаружено превышение числа регистрируемых посылок в $1 + z(\xi)$ раз по отношению к номинальному значению. Число зарегистрированных посылок $n(1+z(\xi))\overline{\mathrm{Eff}}$, номинальное число зарегистрированных посылок $n\overline{\mathrm{Eff}}$. На рис. 6*в* показана нормированная длина секретного ключа R как функция наблюдаемой доли превышения регистрируемых информационных состояний $1 + z$. Как видно на рис. 6*в*, длина секретного ключа обращается в нуль, если наблюдаемое превышение составляет 100 раз. Это означает, что если обнаружено, например, превышение в 10 раз, то длина секретного ключа составляет 0.9 бит на каждую зарегистрированную посылку. Данное значение $1 + z(\xi)$ отвечает значению $\xi = 0.01$ (см. рис. 6*б*), т. е. подслушиватель знает не более 0.1 из каждой зарегистрированной на приемной стороне посылки.

Найдем длину секретного ключа в зависимости от длины линии связи. Пусть подслушиватель проводит UM-атаку в ξ посылках. При этом ошибки на приемной стороне возникают только в числе посылок $\xi n \Pr(?)\overline{\mathrm{Eff}} + n(1 - \xi)\overline{\mathrm{Eff}}$ от темновых шумов однофотонного лавинного детектора. В числе посылок $\xi n(1 - \Pr(?))$ подслушиватель посылает «яркие» состояния, которые не дают ошибок от темновых шумов. Наблюдаемая вероятность ошибки есть

$$Q(\xi) = \frac{p_d}{2} \frac{1 - \xi(1 - \Pr(?))}{1 + z(\xi)}. \qquad (12)$$

Минимальное число битов в пересчете на каждую зарегистрированную посылку, необходимое для исправления ошибок в асимптотическом пределе, равно $h(Q(\xi))$. В этом случае длина секретного ключа в пересчете на посылку равна

$$R = \frac{1 - \xi(1 - \Pr(?))}{1 + z(\xi)} - h(Q(\xi)). \qquad (13)$$

Зависимость нормированной длины секретного ключа от длины линии связи приведена на рис. 6*г*. Подслушиватель атакует при помощи UM-измерений 1 % передаваемых состояний, при этом подслушиватель увеличивает наблюдаемое число регистрируемых информационных состояний в 10 раз.

Таким образом, в данной системе подслушиватель лишен возможности проводить UM-измерения и оставаться недетектируемым. При этом, как видно из данного раздела и разд. 2–9, UM-атака без блокирования канала является для подслушивателя менее эффективной, поскольку при атаке со светоделителем подслушиватель не изменяет номинальное число регистрируемых информационных состояний.

11. ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Обсудим полученные результаты. На рис. 3*а* приведены зависимости эффективности (вероятности) регистрации информационных состояний от среднего числа фотонов в состоянии при трех различных значениях относительной фазы. Использованы типичные значения вероятности темновых шумов и квантовой эффективности лавинных однофотонных детекторов на основе InGaAs:P. При заданном среднем числе фотонов относительная фаза определяет степень неортогональности информационных состояний. Эффективность при фиксированной фазе зависит от среднего числа фотонов. Однако максимальное значение эффективности при разных значениях фазы оказывается одинаковым. При этом максимум достигается при различных значениях среднего числа фотонов. Чем меньше угол, тем при большем среднем числе фотонов достигается максимум. Максимума эффективности можно добиться при любой относительной фазе.

На рис. 3*б* приведены зависимости вероятности ошибки на приемной стороне для трех различных значений относительной фазы как функции длины линии связи. Среднее число фотонов в состоянии бралось в области максимума эффективности регистрации. Из рис. 3*б* видно, что, чем меньше

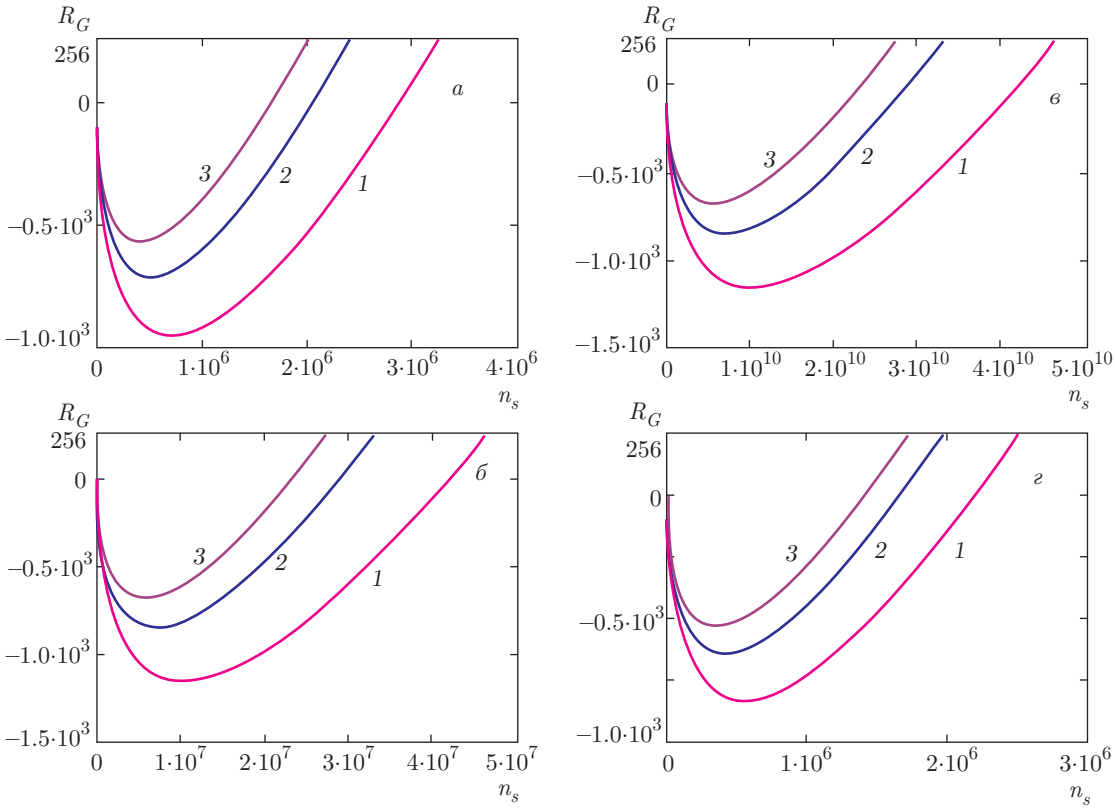

Рис. 7. Зависимости длины секретного ключа при параметре секретности $\varepsilon = 2^{-32}$ как функции числа переданных состояний (n_s). Зависимости на рис. *а,б,в* отвечают консервативной оценке длины ключа, зависимости на рис, *г* — ослабленной консервативной оценке длины ключа. Параметры для всех кривых следующие: вероятность темновых шумов $p_d = 5\cdot10^{-5}$ (*а,б,г*), $5\cdot10^{-9}$ (*в*), длина линии связи $L = 50$ км (*а,г*), 100 км (*б*), 250 км (*в*). Значения других параметров для кривых *1*, *2*, *3* такие же, как параметры для кривых *1*, *2*, *3* на рис. 3

относительная фаза, тем в более широком диапазоне в окрестности максимума можно брать значение среднего числа фотонов в состоянии, поскольку зависимость эффективности от среднего числа фотонов при малых углах более плавная в окрестности максимума. При данных значениях параметров при длине линии 100 км вероятность ошибок на приемной стороне составляет величину примерно 0.05 %, что позволяет использовать простые коды коррекции ошибок с большой длиной кодового слова (см. выше).

На рис. 3*в,г* приведены зависимости нормированной длины секретного ключа в случае консервативной оценки (рис. 3*в*) и ослабленной оценки (рис. 3*г*) в пределе бесконечных передаваемых последовательностей как функции длины линии связи. Как видно из рисунков, предельная длина передачи секретных ключей при используемых параметрах составляет 150 км в обоих случаях. Отличие в длине секретного ключа имеет место только при малых длинах линии связи до 50 км. Это связано с тем, что при малых длинах линии связи подслушиватель может отвести через светоделитель лишь небольшую долю когерентного состояния. При больших длинах линии (> 50 км) длины секретного ключа практически совпадают в обоих случаях. Предельная дальность (150 км) передачи секретных ключей лимитируется темновыми шумами.

На рис. 4*а,б,в,г* приведены зависимости, аналогичные зависимостям на рис. 3*а,б,в,г* при вероятности темновых шумов $p_d = 5\cdot10^{-9}$ отсч./строб, которая достигается для твердотельных лавинных однофотонных детекторов при глубоком охлаждении [14]. Все сказанное выше справедливо и в этом случае, кроме предельной дальности передачи ключей, которая при таких темновых шумах составляет рекордное значение в 300 км.

Обсудим теперь скорость передачи ключей в случае конечных передаваемых последовательностей. Зависимости длины ε-секретного ключа как функции длины посланной последовательности (n_s) приведены на рис. 7. Скорость передачи определяется

тактовой частотой и количеством переданных посылок, которых достаточно для получения секретного ключа заданной длины. Исходим из длины ключа в 256 бит (см. выше).

Для консервативной и ослабленной консервативной оценок длины последовательностей практически совпадают. Например, при длине линии 50 км для получения секретного ключа в 256 бит требуется передать примерно $2 \div 3 \cdot 10^6$ посылок. Из этих посылок будет зарегистрировано порядка 10^3 бит. При тактовой частоте, например, 10 МГц за одну секунду можно передать 10 ключей. При длине линии в 100 км за секунду можно сгенерировать один ключ. При длине в 250 км при той же тактовой частоте требуется 10 с для передачи одного ключа. Скорость генерации ключей прямо пропорциональна тактовой частоте.

12. ЗАКЛЮЧЕНИЕ

Таким образом, предложен протокол с контрольным реперным состоянием, который гарантирует, что при проведении UM-измерений подслушиватель будет производить ошибки на приемной стороне. Данная гарантия вытекает из невозможности блокировать реперное состояние, которое само по себе не несет информации о ключе, но используется при детектировании совместно с информационным состоянием. Информационное состояние может содержать мезоскопическое среднее число фотонов. Даже при мезоскопическом числе фотонов информационные состояния остаются неортогональными, т. е. достоверно неразличимыми. Например, даже при среднем числе фотонов в информационном состоянии $\mu_q = 50$ и относительной фазе между парой состояний $\varphi = \pi/20$ вероятность определенного исхода меньше единицы. Из n посылок подслушиватель может знать не более $n\overline{C}(\rho_E) = 0.775n$ бит. При этом на приемной стороне известно n битов за вычетом информации на коррекцию ошибок (leak). Различимость состояний регулируется как средним числом фотонов μ_q, так и углом между когерентными состояниями $\Delta\varphi$. Данные два параметра могут варьироваться в зависимости от длины линии и требуемой наблюдаемой ошибки за счет темновых шумов лавинного детектора.

Автор выражает благодарность К. А. Балыгину, А. Н. Климову, С. П. Кулику за многочисленные и конструктивные обсуждения, Д. А. Кронбергу, обратившему внимание на устойчивость протокола по отношению к атаке разд. 10, а также коллегам по Академии криптографии Российской Федерации за постоянную поддержку и обсуждения. Работа выполнена при поддержке Российского научного фонда (грант № 16-12-00015).

ЛИТЕРАТУРА

1. C. H. Bennett and G. Brassard, *Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces.*, Bangalore, India (1984), p. 175.

2. W. K. Wotters and W. H. Zurek, Nature **299**, 802 (1982).

3. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

4. A. Chefles, Phys. Lett. A **239**, 339 (1998); A. Chefles and S. M. Barnett, Phys. Lett. A **250**, 223 (1998).

5. С. Н. Молотков, Письма в ЖЭТФ **102**, 530 (2015).

6. С. Н. Молотков, Письма в ЖЭТФ **101**, 579 (2015).

7. K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002); Phys. Rev. A **68**, 022317 (2003).

8. D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Appl. Phys. Lett. **87**, 194108 (2005).

9. Won-Young Hwang, Phys. Rev. Lett. **91**, 057901-1 (2003).

10. V. Scarani, V. H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

11. M. Tomamichel, C. Ci Wen Lim, N. Gisin, and R. Renner, Nature Commun. **3**, 634 (2011).

12. R. Renner, PhD Thesis, ETH Zürich (2005); arXiv/quant-ph:0512258.

13. А. С. Холево, *Введение в квантовую теорию информации*, сер. *Современная математическая физика*, вып. 5, МЦНМО, Москва (2002); УМН **53**, 193 (1998).

14. B. Korzh, C. Ci Wen Lim, R. Houlmann, N. Gisin, Ming Jun Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nature Photon. **9**, 163 (2014).

15. С. Н. Молотков, ЖЭТФ **150**, 903 (2016).