ЖЭТФ, 2019, том 156, вып. 2 (8), стр. 205–238

СОСТОЯНИЯ «ЛОВУШКИ», КОДЫ КОРРЕКЦИИ ОШИБОК С НИЗКОЙ ПЛОТНОСТЬЮ ПРОВЕРОК НА ЧЕТНОСТЬ В КВАНТОВОЙ КРИПТОГРАФИИ С ФАЗОВО-ВРЕМЕННЫМ КОДИРОВАНИЕМ

И. В. Синильщиков [a,e], ***С. Н. Молотков*** [b,c,d,e*]

[a] *Физический факультет, Московский государственный университет им. М. В. Ломоносова 119899, Москва, Россия*

[b] *Институт физики твердого тела Российской академии наук 142432, Черноголовка, Московская обл., Россия*

[c] *Академия криптографии Российской Федерации 121552, Москва, Россия*

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

[e] *Центр квантовых технологий, Московский государственный университет им. М. В. Ломоносова 119899, Москва, Россия*

Поступила в редакцию 31 января 2019 г.,
после переработки 17 февраля 2019 г.
Принята к публикации 18 февраля 2019 г.

Исследована криптостойкость квантового распределения ключей с фазово-временны́м кодированием относительно атаки с расщеплением по числу фотонов (PNS-атаки). Длина линии, до которой гарантируется секретное распределение ключей, определяется как самим протоколом, так и эффективностью коррекции ошибок в сырых ключах. Исследовано влияние разных параметров лавинных однофотонных детекторов на длину линии секретного распределения ключей. Для коррекции ошибок рассмотрены различные варианты кодов с низкой плотностью проверок на четность (LDPC-кодов), которые являются на сегодняшний день наиболее близкими по эффективности к теоретическому шенноновскому пределу.

DOI: 10.1134/S0044451019080029

1. ВВЕДЕНИЕ

Квантовое распределение секретных ключей (синоним термина квантовая криптография) должно гарантировать безусловную секретность распределяемых ключей по открытым и доступным для прослушивания и любой модификации квантовым каналам связи. Квантовая криптография должна гарантировать секретность ключей, которая базируется только на фундаментальных ограничениях, диктуемых квантовой теорией и не содержит никаких предположений о технических или вычислительных возможностях подслушивателя [1]. Подслушиватель ничем не ограничен в своих действиях при атаках на распределяемые ключи, кроме одного — он не может нарушать законы природы, в частности квантовой механики.

Распределение ключей происходит по некоторому протоколу — набору действий по приготовлению квантовых состояний на передающей стороне, их передаче через квантовый канал связи, преобразованию и измерению на приемной стороне, оценке вероятности ошибки в первичных ключах, коррекции ошибок через открытый аутентичный классический канал связи, который также доступен для прослушивания третьей стороной, и усилению секретности «очищенных» ключей — хешированию через открытый канал связи при помощи универсальных хеш-функций второго порядка.

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

Принципиальный результат теории состоит в том, что для строго однофотонного источника квантовых состояний удается через фундаментальные энтропийные соотношения неопределенностей связать верхнюю границу утечки информации к подслушивателю с величиной наблюдаемой ошибки на приемной стороне [2].

На сегодняшний день строго однофотонный источник квантовых состояний отсутствует, поэтому в реальных системах квантовой криптографии в качестве информационных состояний используется сильно ослабленное когерентное состояние лазерного излучения. Ослабление происходит до уровня в несколько десятых среднего числа фотонов в когерентном квантовом состоянии

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

где μ — среднее число фотонов в когерентном состоянии, $|n,\sigma\rangle$ — фоковское состояние с n фотонами с поляризацией σ, $|0\rangle = |\mathrm{vac}\rangle$ отвечает вакуумному состоянию поля. Когерентное состояние (1) имеет пуассоновскую статистику по числу фотонов. Вероятность обнаружить n фотонов вне зависимости от состояния поляризации σ в состоянии (1) равна

$$P(n) = e^{-\mu}\frac{\mu^n}{n!}. \tag{2}$$

В квантовой криптографии используется в основном два метода кодирования:

1) поляризационное кодирование — информация о битах ключа кодируется в поляризацию σ когерентного состояния (1);

2) фазовое кодирование — информация о битах ключа кодируется в относительную фазу φ пары когерентных состояний $|\alpha\rangle_1 \otimes |e^{i\varphi}\alpha\rangle_2$, сдвинутых по времени и пространству[1)]. Стандартное одномодовое волокно не сохраняет поляризацию, поэтому практически все системы квантовой криптографии используют фазовое кодирование.

Во всех известных системах как с фазовым, так и поляризационным кодированием для устойчивой работы системы требуется подстройка состояния поляризации на выходе из линии связи, что требует определенных технических решений и приводит к дополнительным временны́м расходам, а это снижает скорость генерации ключей и усложняет конструкцию системы. Необходимость подстройки поляризации на выходе из линии связи связана с тем, что приемная часть в системах как с фазовым, так и с поляризационным кодированием содержит поляризационно чувствительные элементы — фазовые модуляторы, модуляторы поляризации, для правильной работы которых требуется определенное входное состояние поляризации по отношению к оптической оси элемента.

Наш интерес к фазовому кодированию связан с тем, что имеется способ фазового кодирования, точнее, способ фазово-временного кодирования, реализация которого не требует подстройки поляризации на выходе из линии связи [3]. Отметим, что сказанное выше относится к однопроходным системам квантовой криптографии. Имеются реализации двухпроходных волоконных систем квантовой криптографии, в которых не требуется подстройка поляризации. Проблема в том, что практически невозможно обеспечить требуемый уровень защиты двухпроходных систем относительно атак активного зондирования. Уязвимость к таким атакам была неоднократно продемонстрирована экспериментально.

Есть еще одно веское соображение в пользу систем квантовой криптографии с фазовым кодированием. Как было показано в работе [4], системы с фазовым кодированием более устойчивы по отношению к атаке с ослеплением лавинных детекторов [5]. Системы с поляризационным кодированием, использующие стандартные протоколы типа BB84 или Decoy States BB84, остаются уязвимыми к такой атаке, и их неуязвимость обеспечивается лишь техническими мерами, по сути, техническими «заплатками».

2. АТАКА С РАСЩЕПЛЕНИЕМ ПО ЧИСЛУ ФОТОНОВ — PNS-АТАКА

Нестрогая однофотонность источника квантовых информационных состояний приводит к появлению ряда атак, которые ограничивают дальность передачи секретных ключей. Потери в канале связи и пуассоновская статистика приводят к возможности так называемой PNS-атаки (Photon Number Splitting attack), которая ограничивает дальность передачи ключей в канале с потерями даже при идеальных однофотонных детекторах без темновых шумов на приемной стороне.

[1)] Отметим, что состояние (1) является одномодовым, формально бесконечно протяженным. В реальной ситуации используются пакеты, локализованные во временном окне с характерной длительностью примерно 1 нс и шириной спектра 10^9 Гц. Поскольку оптические элементы в системах квантовой криптографии являются в этом диапазоне практически линейными и бездисперсионными (компоненты состояний с разными частотами преобразуются одинаково), достаточно рассмотреть состояния только с одной длиной волны.

Для широко известного протокола квантовой криптографии BB84, PNS-атака, начиная с некоторой критической длины линии связи, соответственно, критической величины потерь, приводит к тому, что подслушиватель знает весь ключ, не производит ошибок на приемной стороне и не детектируется. При длине линии выше критической из-за PNS-атаки нельзя передавать ключи и гарантировать их секретность.

Впервые PNS-атака для протокола BB84 была предложена в 1999 г. [6]. При этом подразумевался протокол квантовой криптографии с поляризационным кодированием. Поскольку фаза когерентного состояния (фаза θ, $\alpha\sqrt{\mu}e^{i\theta}$ в (1)) меняется случайно от посылке к посылке, подслушиватель «видит» в канале связи не чистое квантовое состояние, а статистическую смесь — матрицу плотности

$$\rho(\mu) = \int\limits_0^{2\pi} \frac{d\theta}{2\pi} |e^{i\theta}|\alpha|, \sigma\rangle\langle e^{i\theta}|\alpha|, \sigma| = \\ = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n, \sigma\rangle\langle n, \sigma|. \quad (3)$$

Квантовая механика допускает неразрушающие измерения числа фотонов (nondemolishing measurements). Данные измерения позволяют определить число фотонов, при этом не возмущая состояние поляризации фотона. После определения числа фотонов, их состояние поляризации остается неизвестным.

При PNS-атаке подслушиватель разрывает квантовый канал связи и определяет число фотонов в каждой посылке. На этой стадии подслушивателю еще неизвестно, какому биту ключа отвечает измеренное неразрушающим способом квантовое состояние. Если обнаружен один фотон, то канал блокируется, исчезновение состояния списывается на потери в линии. Если обнаружено два или более фотонов, то один фотон подслушиватель оставляет в своей квантовой памяти, остальные через канал с меньшими потерями (в идеале без потерь) направляет на приемную сторону. Поскольку в протоколе BB84 внутри базиса состояния ортогональны, дождавшись раскрытия базисов, подслушиватель проводит измерения своего квантового состояния в уже известном базисе и достоверно узнает передаваемое состояние.

Таким образом, начиная с определенного уровня потерь в линии подслушиватель знает весь передаваемый ключ, не производит ошибок на приемной стороне, сохраняет число состояний, достигающих приемной стороны, и не детектируется. Секретные ключи при длине линии выше критической передавать нельзя.

Проиллюстрируем PNS-атаку на примере протокола квантовой криптографии BB84, хотя она применима и для ряда других протоколов. В протоколе BB84 с поляризационным кодированием используется два базиса $+$ и $\times$. В каждом базисе состояниям 0 и 1 сопоставляются ортогональные внутри данного базиса состояния поляризации σ_0^+ и σ_1^+,

$$0 \to |\alpha, \sigma_0^+\rangle, 1 \to |\alpha, \sigma_1^+\rangle, \quad \langle\alpha, \sigma_0^+|\alpha, \sigma_1^+\rangle = 0. \quad (4)$$

Аналогично в сопряженном базисе:

$$0 \to |\alpha, \sigma_0^\times\rangle, \quad 1 \to |\alpha, \sigma_1^\times\rangle, \quad \langle\alpha, \sigma_0^\times|\alpha, \sigma_1^\times\rangle = 0. \quad (5)$$

Состояния 0 и 1 при известном базисе из-за ортогональности состояний достоверно различимы. Состояния из разных базисов попарно неортогональны:

$$0 \to |\alpha, \sigma_0^\times\rangle, \quad 1 \to |\alpha, \sigma_1^\times\rangle, \\ |\langle\alpha, \sigma_{0,1}^\times|\alpha, \sigma_{0,1}^+\rangle| = \frac{1}{\sqrt{2}}, \quad (6)$$

т. е. различимы с вероятностью $1/2$, если базис неизвестен.

Рассмотрим неразрушающие измерения на более формальном уровне. Любое измерение в квантовой механике дается разложением единицы I. Неразрушающее измерение по числу фотонов дается проекционным (ортогональным) измерением

$$I = \sum_{n=0}^{\infty} \mathcal{P}_n, \quad \mathcal{P}_n = \sum_{\sigma=0,1} |n, \sigma\rangle\langle\sigma, n|, \quad (7)$$

где индекс n нумерует результат измерения — обнаружение числа фотонов n. Такое измерение не позволяет определить состояние поляризации фотонов, но позволяет определить число фотонов, и при этом оставляет значение поляризации невозмущенным:

$$\mathcal{P}_{n'}|n, \sigma_{0,1}^+\rangle = \delta_{n,n'}|n, \sigma_{0,1}^+\rangle, \\ \mathcal{P}_{n'}|n, \sigma_{0,1}^\times\rangle = \delta_{n,n'}|n, \sigma_{0,1}^\times\rangle. \quad (8)$$

Если обнаружен один фотон в линии ($n = 1$), то подслушиватель блокирует канал связи. Если обнаружено два или более фотонов ($n \geq 2$ — состояние $|n, \sigma_{0,1}^\times\rangle$ или $|n, \sigma_{0,1}^+\rangle$, поляризация пока неизвестна), то подслушиватель оставляет часть фотонов в своей квантовой памяти, а остальные посылает на приемную сторону через канал с меньшими потерями, в идеале без потерь.

Детекторы не регистрируют вакуумную компоненту поля, поэтому вероятность зарегистрировать на приемной стороне передаваемые состояния в отсутствие подслушивателя есть

$$1 - e^{-\mu\eta T(L)}, \tag{9}$$

где η — квантовая эффективность детектора, $T(L) = 10^{-\delta L/10}$ — пропускание канала, $\delta = 0.2$ дБ/км — коэффициент потерь для стандартного одномодового волокна, L — длина квантового канала связи.

Подслушиватель остается недетектируемым, если потери в линии связи таковы, что подслушиватель может обеспечить сохранение среднего числа регистрируемых посылок на приемной стороне, которое было без подслушивателя. Это оказывается возможным уже при длине линии несколько десятков километров.

3. ОСНОВНАЯ ИДЕЯ МЕТОДА С СОСТОЯНИЯМИ «ЛОВУШКАМИ»

Decoy state-метод представляет собой случайную модуляцию интенсивности когерентных состояний и может быть использован для любого протокола.

Исходно Decoy state-метод был предложен для противодействия PNS-атаке для протокола BB84. Данному методу посвящено большое число теоретических и экспериментальных работ (например, [7–19]). В этом методе кроме информационных квантовых состояний с фиксированным средним числом фотонов используются дополнительные (decoy states) когерентные состояния с другой интенсивностью.

Основная идея Decoy state-метода основана на следующем факте. Если в канал связи посылаются когерентные состояния с разным средним числом фотонов, то, как следует из (3), фоковское состояние с некоторым заданным числом фотонов может произойти из разных когерентных состояний, например, $|\alpha\rangle$ или $|\nu\rangle$. Вероятность появления заданного фоковского числа фотонов зависит от среднего числа фотонов в состоянии, которое подслушивателю неизвестно. Например, блокирование фоковских состояний с одним фотоном будет изменять общую статистику отсчетов для состояний с разной интенсивностью. Таким образом, вторжение в линию связи детектируется. Дальнейшая задача состоит в установлении связи между наблюдаемым изменением статистики фотоотсчетов на приемной стороне с утечкой информации к подслушивателю.

Определив среднее число фотонов k в конкретной посылке, подслушиватель принципиально не может определить, из какого когерентного состояния $|\alpha\rangle$ или $|\nu\rangle$ было получено данное число фотонов k в посылке. Блокирование доли однофотонных состояний $|1\rangle\langle 1|$ в линии, которые произошли из разных когерентных состояний $|\alpha\rangle$ и $|\nu\rangle$ изменяет статистику фотоотсчетов в посылках, в которых посылались состояния ловушки и информационные состояния.

Отметим, что изменения статистики фотоотсчетов можно обнаружить даже при существующих фотодетекторах, которые не различают число фотонов, а дают только интегральный темп фотоотсчетов. Изменение статистики фотоотсчетов позволяет определить долю однофотонной компоненты в состояниях, которые подслушиватель не блокировал, и тем самым определить длину секретного ключа, если изменение статистики фотоотсчетов не превышает критическую величину [7–19].

Несмотря на то что использованию и исследованию данного метода посвящены десятки теоретических и экспериментальных работ, не все принципиальные вопросы выяснены. Исходно Decoy state-метод был развит для поляризационного кодирования. В дальнейшем уравнения и анализ стали применяться без какой-либо модификации напрямую к протоколам с фазовым кодированием. Однако структуры состояний в канале связи, как будет видно ниже, для поляризационного и фазового кодирования оказываются разными. Поэтому анализ секретности систем, использующих фазовое кодирование, основанный на анализе систем для поляризационного кодирования, неприменим. PNS-атака при фазовом кодировании выглядит иначе, чем при поляризационном кодировании. Поэтому нужен адекватный метод для анализа PNS-атаки при фазовом кодировании.

Кроме того, существуют протоколы, которые обеспечивают большую дальность в однофотонном случае [20, 21] по сравнению с протоколом BB84 [6]. Одним из таких протоколов является протокол квантового распределения ключей с фазово-временны́м кодированием, который является двухпараметрическим протоколом, где детектирование вторжений в квантовый канал связи происходит по двум параметрам: ошибкам в информационных временных окнах и отсчетам в контрольных временных окнах, что позволяет достичь большей дальности передачи секретных ключей. Более того, данный протокол допускает эффективную волоконно-оптическую реализацию приемной части, которая не использует поляризационно чувствительных активных оптических элементов (фазовых модуляторов, контроллеров поляризации и т. д.), поэтому не требует подстройки поляризации на выходе из линии связи [3]. Данный протокол является единственным протоколом, который обладает такими преимуществами в случае однопроходных систем.

Работа имеет следующую структуру. Сначала будут получены выражения для состояний в канале связи для фазово-временно́го кодирования. Затем будут получены совместные состояния Алиса–Боб–Ева до измерений на приемной стороне. Измерения на приемной стороне изменяют состояния Евы. Далее будут получены квантовые состояния Алиса–Ева после измерений Боба. Данные состояния необходимы для подсчета утечки информации к подслушивателю. Состояния Алиса–Боб требуются для подсчета вероятности ошибки и вероятности отсчетов в контрольных временны́х окнах. В итоге будет получено выражение для длины секретного ключа как функции наблюдаемых параметров на приемной стороне.

Здесь нужно отметить, что Decoy state-метод предназначен для детектирования PNS-атаки. Атака со светодилителем рассматривалась в работе [22].

В данной работе будет сделан анализ Decoy state-метода для протокола с фазово-временны́м кодированием и получены формулы для длины секретного ключа для случая различных детекторов и с использованием коррекции ошибок в первичных ключах при помощи кодов с низкой плотностью проверок на четность — LDPC-кодов (low density parity check codes) [23, 24].

4. ИНФОРМАЦИОННЫЕ КОГЕРЕНТНЫЕ СОСТОЯНИЯ

В протоколе используются два базиса. В каждом базисе имеется пара ортогональных состояний, отвечающих 0 и 1. Состояния из разных базисов попарно неортогональны. Информационные состояния в протоколе фазово-временно́го кодирования имеют вид (обратим внимание на расстановку фазового множителя в базисах L и R, такой выбор фазового множителя принципиален для сохранения одинакового суммарного регистрируемого числа 0 и 1 в обоих базисах при различных детекторах)

$$0_L \to |\alpha\rangle_1 \otimes |\alpha\rangle_2, \quad 1_L \to |\alpha\rangle_1 \otimes |e^{i\pi}\alpha\rangle_2, \tag{10}$$

$$0_R \to |\alpha\rangle_2 \otimes |e^{i\pi}\alpha\rangle_3, \quad 1_R \to |\alpha\rangle_2 \otimes |\alpha\rangle_3, \tag{11}$$

$$|\alpha\rangle_i = e^{-\mu/2} \sum_{n=0}^{\infty} \frac{e^{i\theta n}|\alpha|^n}{\sqrt{n!}} |n\rangle_i, \tag{12}$$

где индекс i отвечает когерентному состоянию, локализованному в i-м временно́м окне на входе в линию связи (см. разд. 9, рис. 1), индексы L и R обозначают базисы, сдвинутые по времени, μ — среднее число фотонов в когерентном состоянии, $|n\rangle_i$ — фоковское состояние с n фотонами, $|0\rangle$ отвечает вакуумному состоянию поля. Индекс поляризации σ опущен как несущественный для нашего протокола. Состояние поляризации оказывается несущественным при фазовом кодировании (см. детали реализации в работе [3]).

Поскольку фаза θ самого когерентного состояния в разных посылках является случайной, матрица плотности информационных состояний, которую «видит» подслушиватель в базисе L имеет вид

$$\begin{aligned}\rho^L(\mu,\varphi) &= \int_0^{2\pi} \frac{d\theta}{2\pi} \left(|e^{i(\theta+\varphi)}\sqrt{\mu}\rangle_1 \otimes |e^{i\theta}\sqrt{\mu}\rangle_2 \right) \times \\ &\times \left({}_2\langle e^{i\theta}\sqrt{\mu}| \otimes {}_1\langle e^{i(\theta+\varphi)}\sqrt{\mu}| \right) = \\ &= \sum_{k=0}^{\infty} e^{-2\mu}\mu^k |\Theta_k^L(\varphi)\rangle\langle\Theta_k^L(\varphi)| = \\ &= \sum_{k=0}^{\infty} \tilde{P}(k,\mu)\rho_k^L(\mu,\varphi), \quad \tilde{P}(k,\mu) = e^{-2\mu}\mu^k \frac{2^k}{k!}, \end{aligned} \tag{13}$$

$$\begin{aligned}\rho_k^L(\mu,\varphi) &= |\Theta_k^L(\varphi)\rangle\langle\Theta_k^L(\varphi)|, \\ |\Theta_k^L(\varphi)\rangle &= \sqrt{\frac{k!}{2^k}} \sum_{m=0}^{k} e^{i\varphi m} \frac{|m\rangle_1 \otimes |k-m\rangle_2}{\sqrt{m!}\sqrt{(k-m)!}}. \end{aligned} \tag{14}$$

Для состояний в базисе R находим

$$\begin{aligned}\rho^R(\mu,\varphi) &= \int_0^{2\pi} \frac{d\theta}{2\pi} \left(|e^{i(\theta+\varphi)}\sqrt{\mu}\rangle_2 \otimes |e^{i\theta}\sqrt{\mu}\rangle_3 \right) \times \\ &\times \left({}_3\langle e^{i\theta}\sqrt{\mu}| \otimes {}_2\langle e^{i(\theta+\varphi)}\sqrt{\mu}| \right) = \\ &= \sum_{k=0}^{\infty} e^{-2\mu}\mu^k 2^k |\Theta_k^R(\varphi)\rangle\langle\Theta_k^R(\varphi)| = \\ &= \sum_{k=0}^{\infty} \tilde{P}(k,\mu)\rho_k^R(\mu,\varphi), \end{aligned} \tag{15}$$

$$\begin{aligned}\rho_k^R(\mu,\varphi) &= |\Theta_k^R(\varphi)\rangle\langle\Theta_k^R(\varphi)|, \\ |\Theta_k^R(\varphi)\rangle &= \sqrt{\frac{k!}{2^k}} \sum_{m=0}^{k} e^{i\varphi m} \frac{|m\rangle_2 \otimes |k-m\rangle_3}{\sqrt{m!}\sqrt{(k-m)!}}. \end{aligned} \tag{16}$$

Фаза φ выбирается Алисой в зависимости от посылаемого информационного состояния. Для логического 0 (в базисе L и R) значение фазы $\varphi = 0$ и для логической 1 (в базисе L и R) $\varphi = \pi$. Отметим, что состояния $|\Theta_k^{L,R}(\varphi)\rangle$ при разных индексах k внутри одного базиса (для подслушивателя при известном базисе) являются ортогональными и играют роль состояний с заданным «числом фотонов».

Этот факт потребуется при построении PNS-атаки для фазового кодирования. Вакуумная компонента состояний имеет вид

$$\rho^L(\mu, k=0) = e^{-2\mu}(|0\rangle_1 \otimes |0\rangle_2)({}_2\langle 0| \otimes {}_1\langle 0|),$$

аналогично для состояний в базисе R. Соответственно, вероятность обнаружить в линии связи 0 фотонов ($k=0$) есть $e^{-2\mu}$.

Как видно из (13)–(16), структура матрицы плотности информационных состояний на выходе передающей станции в квантовый канал связи отличается от структуры матрицы плотности при поляризационном кодировании (3).

5. НЕРАЗРУШАЮЩЕЕ ИЗМЕРЕНИЕ «ЧИСЛА ФОТОНОВ» ПРИ ФАЗОВОМ КОДИРОВАНИИ

Стандартная статистическая интерпретация матрицы плотности (13), (15) сводится к следующему. В каждой посылке подслушиватель с вероятностью $\tilde{P}(k,\mu) = e^{-2\mu}\mu^k 2^k/k!$ «видит» чистое состояние $|\Theta_k^L(\varphi)\rangle$ в базисе L или $|\Theta_k^R(\varphi)\rangle$ в базисе R, но базис подслушивателю на данный момент неизвестен.

Подслушиватель проводит неразрушающее измерение с целью определить «число фотонов» в линии, т. е. определить, какое состояние в линии — $|\Theta_k^L(\varphi)\rangle$ или $|\Theta_k^R(\varphi)\rangle$.

Неразрушающее измерение позволяет определить только индекс k. Далее везде для краткости будем говорить «число фотонов». Измерение позволяет узнать число фотонов в каждой посылке, но не позволяет определить фазу φ. Фаза однозначно дает информацию о передаваемом бите ключа 0 или 1, если базис L или R подслушивателю известен.

Принципиально важно для дальнейшего подчеркнуть, что состояния в (14), (16) не зависят от интенсивности μ когерентного состояния. Подслушиватель не может определить, из какого когерентного состояния произошло состояние с данным «числом фотонов», т. е. не может различить когерентные состояния с разными средними числами фотонов.

Любое измерение в квантовой механике дается разложением единичного оператора. В данном случае каждому исходу k — числу фотонов, приписывается проекционный оператор $\mathcal{P}_k$ в пространстве состояний $\mathcal{H} = \oplus_{k=0}^{\infty}\mathcal{H}_k$, где $\mathcal{H}_k$ — фоковское пространство с числом фотонов k.

Еще раз отметим, что структура неразрушающих измерений числа фотонов при фазовом кодировании принципиально отличается от структуры измерений при поляризационном кодировании.

Измерение описывается разложением единицы:

$$I_{\mathcal{H}} = I_1 \otimes I_2 \otimes I_3 = \left(\sum_{n_1=0}^{\infty} |n_1\rangle_{11}\langle n_1|\right) \otimes \left(\sum_{n_1=0}^{\infty} |n_2\rangle_{22}\langle n_2|\right) \otimes \left(\sum_{n_1=0}^{\infty} |n_3\rangle_{33}\langle n_3|\right) = \sum_{k=0}^{\infty}\mathcal{P}_k, \quad (17)$$

$$\mathcal{P}_k = \sum_{m=0}^{k}\sum_{l=0}^{m}(|k-m\rangle_1 \otimes |m-l\rangle_2 \otimes |l\rangle_3) \times ({}_3\langle l| \otimes {}_2\langle m-l| \otimes {}_1\langle k-m|). \quad (18)$$

В формуле (17) единичный оператор I_i ($i=1,2,3$) — проектор на подпространство фоковских состояний, локализованных во временно́м окне i, соответственно, $I_{\mathcal{H}}$ — проектор на фоковское пространство состояний, локализованных во всех временны́х окнах *1*, *2* и *3*.

Проектор $\mathcal{P}_k$ в формуле (18) имеет простой физический смысл — это проектор на фоковское подпространство, содержащее суммарное число фотонов во всех временны́х окнах, равное k. Проекция состояния на подпространство, содержащее k фотонов, равна

$$\mathcal{P}_{k'}\rho_k^{L,R}(\mu,\varphi^A)\mathcal{P}_{k'} = \delta_{k,k'}\rho_k^{L,R}(\mu,\varphi^A) = \tilde{P}(k,\mu)|\Theta_k^{L,R}(\varphi)\rangle\langle\Theta_k^{L,R}(\varphi)|. \quad (19)$$

Условие нормировки состояний на единицу выполнено, поскольку

$$\langle\Theta_k^{L,R}(\varphi)|\Theta_k^{L,R}(\varphi)\rangle = \frac{k!}{2^k}\sum_{m=0}^{k}\frac{1}{m!(k-m)!} = 1. \quad (20)$$

Важно отметить, что сами состояния $|\Theta_k(\varphi)\rangle$ не зависят от среднего числа фотонов μ в когерентном состоянии, а зависят только от суммарного числа фотонов k во всех временны́х окнах.

При PNS-атаке подслушиватель действует следующим образом. Проводит измерение (17)–(19) с бесконечным числом исходов, которые нумеруются индексом k. Исход k зависит о того, какое состояние присутствует в данной посылке в канале связи. После измерения числа фотонов в данной посылке подслушиватель знает принадлежность состояний (14),

(16) к подпространству с данным числом фотонов и не производит искажений этого состояния. Фаза φ остается неизвестной.

Если получен исход k, то подслушиватель имеет в своем распоряжении состояние $|\Theta_k^{L,R}(\varphi)\rangle$ с известным числом фотонов k. Напомним еще раз, что базис L или R неизвестен и знание базиса не требуется для проведения неразрушающего измерения (17)–(19). Вероятность такого исхода равна $\tilde{P}(k,\mu)$. При этом фаза $\varphi = 0$ или $\varphi = \pi$, несущая информацию о бите ключа, подслушивателю неизвестна. Для проведения неразрушающего измерения (17)–(19) знание фазы φ не требуется, см. (19).

Далее стратегия подслушивателя определяется тем, какое число фотонов обнаружено в данной посылке. Цель подслушивателея — получить максимум информации о ключе и произвести минимум детектируемых ошибок на приемной стороне.

Если обнаружена вакуумная компонента состояния, то подслушиватель не предпринимает никаких действий, поскольку данная компонента не несет никакой информации о ключе. При обнаружении однофотонной компоненты при неизвестном базисе нельзя получить достоверную информацию о состоянии без его искажения. Наиболее общая атака в однофотонном случае сводится к запутыванию передаваемого состояния со вспомогательным состоянием Евы (ancilla). После этого искаженное информационное состояние отправляется на приемную сторону, а искаженное вспомогательное состояние Евы остается в квантовой памяти до разглашения базисов и проведения измерений Бобом. Состояние анциллы в квантовой памяти будет коррелировано с результатом измерений Боба. После проведения измерений Бобом Ева делает коллективные измерения над всей квантовой памятью. Такая атака называется коллективной атакой и, как было доказано, является самой общей атакой [25], которую допускают законы квантовой механики в однофотонном случае. Когерентная атака, когда Ева использует вспомогательное состояние в пространстве большой размерности и запутывает его сразу со всей передаваемой последовательностью, сводится к коллективной атаке, если состояния передаются Алисой в каждой посылке независимо друг от друга [25].

Для однопараметрических протоколов, например протокола BB84, такая атака параметризуется одним параметром — наблюдаемой ошибкой Q на приемной стороне, которая задается действиями подслушивателя. Более точно, совместная эволюция информационного состояния и вспомогательного состояния определяется действием запутывающего унитарного оператора, который находится в руках подслушивателя. Данный оператор строится явно и зависит только от одного параметра Q — наблюдаемой ошибки на приемной стороне. Унитарный оператор строится из соображений, чтобы при данной наблюдаемой ошибке Q на приемной стороне Ева получала максимум информации о передаваемом ключе.

Исследуемый в данной работе протокол с фазово-временны́м кодированием является двухпараметрическим протоколом [20, 21]. На приемной стороне при измерениях Боба возникают два наблюдаемых параметра: вероятность ошибки Q при измерении в информационных временны́х окнах (временно́е окно *2* в базисе L или временно́е окно *3* в базисе R, см. разд. 9, рис. 1) и вероятность отсчетов q в контрольных временны́х окнах (временно́е окно *4* в базисе L или временно́е окно *1* в базисе R, см. разд. 9, рис. 1). Данные параметры находятся в руках подслушивателя. Ранее была построена коллективная унитарная атака для случая строго однофотонного источника информационных состояний [20, 21]. Эти результаты нам потребуются для конструирования атаки Евы, если она обнаружила однофотонную компоненту когерентного состояния в канале связи.

6. ДЕЙСТВИЯ ПОДСЛУШИВАТЕЛЯ ПОСЛЕ НЕРАЗРУШАЮЩИХ ИЗМЕРЕНИЙ

Рассмотрим квантовые состояния, которые возникают после неразрушающих измерений числа фотонов Евой, но до измерений Бобом на приемной стороне.

Действие подслушивателя зависит от того, какое число фотонов обнаружено в линии связи. После обнаружения конкретного числа фотонов происходит преобразование состояния $|\Theta_k^{L,R}(\varphi)\rangle\langle\Theta_k^{L,R}(\varphi)|$. Любое преобразование входного квантового состояния (эрмитова положительного оператора со следом единица) в некоторое другое квантовое состояние со следом, меньшим или равным единице, дается линейным вполне положительным отображением, которое часто называется супероператором. Супероператор $\mathcal{T}[\ldots]$ полностью определяется Евой и действие его зависит от числа обнаруженных фотонов k. Супероператор действует в прямой сумме ортогональных подпространств с разным числом фотонов, имеем

$$\mathcal{T}[\ldots] = \oplus_{k=0}^{\infty}\mathcal{T}_k[\ldots]. \qquad (21)$$

6.1. Вакуумная компонента состояний

Регистрация квантовых состояний на приемной стороне происходит при помощи лавинных детекторов, которые работают в стробируемом режиме. Детекторы имеют неединичную квантовую эффективность и имеют темновые шумы. Неединичная квантовая эффективность означает, что однофотонное фоковское состояние может быть зарегистрировано лишь с вероятностью $\eta < 1$ во временно́м окне строба. Темновые шумы означают, что даже в отсутствие реальных фотонов детектор произведет отсчет с вероятностью p_d, т. е. регистрация вакуумной компоненты поля на приемной стороне вызовет отсчет с данной вероятностью.

Для дальнейшего важно, что в посылках, где имеет место вакуумная компонента поля, у подслушивателя нет никаких отсчетов. Считаем, что детекторы у Евы идеальные — единичной квантовой эффективности и без темновых шумов. На приемной стороне у Боба будут отсчеты в данной посылке за счет темновых шумов лавинного детектора с вероятностью p_d.

Действие супероператора подслушивателя на вакуумную компоненту сводится к тождественному действию, имеем

$$\mathcal{T}_0[|\Theta_0^{L,R}(0,1)\rangle_{BB}\langle\Theta_0^{L,R}(0,1)|] = \\ = |\Theta_0^{L,R}(0,1)\rangle_{BB}\langle\Theta_0^{L,R}(0,1)|, \quad (22)$$

где 0 отвечает фазе, равной 0, а 1 — фазе, равной π. На приемной стороне Боба в данной посылке может возникнуть темновой отсчет (см. ниже), который может дать правильный или неправильный результат при сравнении логических битов Алисы и Боба. Данная посылка будет фигурировать среди зарегистрированных посылок у Боба.

6.2. Однофотонная компонента состояний, унитарная коллективная атака

Если в результате неразрушающих измерений в канале связи обнаружена однофотонная компонента состояний, то подслушиватель может блокировать часть посылок, а для остальной доли посылок Y_1^E осуществить унитарную атаку. Посылки в доле Y_1^E выбираются подслушивателем и неизвестны легитимным пользователям. Задача Алисы и Боба состоит в определении величины Y_1^E. Из однофотонных посылок Ева не может получить достоверную информацию о передаваемом бите ключа без возмущения квантовых состояний. Неформально говоря, весь секретный ключ «набирается» только из доли однофотонных посылок, регистрируемых на приемной стороне.

Однофотонные информационные состояния для фазово-временно́го кодирования в базисе L имеют вид

$$0_L \to |0_L\rangle_B = \frac{|1\rangle_1 + |1\rangle_2}{\sqrt{2}}, \\ 1_L \to |0_L\rangle_B = \frac{|1\rangle_1 - |1\rangle_2}{\sqrt{2}}, \quad (23)$$

в базисе R —

$$0_R \to |0_R\rangle_B = \frac{|1\rangle_2 - |1\rangle_3}{\sqrt{2}}, \\ 1_R \to |0_R\rangle_B = \frac{|1\rangle_2 + |1\rangle_3}{\sqrt{2}}. \quad (24)$$

Принципиально важно обратить внимание на расстановку фаз в (23), (24). Состояние 0_L регистрируется детектором *1* в информационном временно́м окне *2*, а состояние 1_L регистрируется детектором *2* в информационном временно́м окне *2* (см. разд. 9, рис. 1).Состояние 0_R регистрируется детектором *2* в информационном окне *3*, а состояние 1_R регистрируется детектором *1* в информационном окне *3*. Это обеспечивает симметрию по полному количеству регистрируемых 0 и 1 в обоих базисах.

Самой общей атакой является унитарная коллективная атака (см., например, [25]), которая сводится к следующему. Ева в каждой посылке использует вспомогательное состояние $|E\rangle_E$, которое она запутывает с информационным. Свое состояние Ева оставляет в квантовой памяти и сохраняет до самой последней стадии — измерений Боба, согласования базисов, коррекции ошибок и сжатия очищенных ключей. После этого Ева проводит коллективные измерения над всей квантовой памятью. Запутывание передаваемого состояния с состоянием Евы возникает как результат действия унитарного оператора U_{BE}. Унитарный оператор и, соответственно, состояния Евы должны зависеть только от двух наблюдаемых параметров q_1 и Q_1 (см. ниже), которые определяются Евой. Введем обозначения

$$|\Psi_1^L(0_L)\rangle_{BE} = U_{BE}\,(|0_L\rangle_B \otimes |E\rangle_E) = |\Phi_L^0\rangle_E \otimes \\ \otimes |0_L\rangle_B + |\Omega_L^0\rangle_E \otimes |1_L\rangle_B + |\Lambda_L^0\rangle_E \otimes |3\rangle_B, \\ |\Psi_1^L(1_L)\rangle_{BE} = U_{BE}\,(|1_L\rangle_B \otimes |E\rangle_E) = |\Phi_L^1\rangle_E \otimes \\ \otimes |1_L\rangle_B + |\Omega_L^1\rangle_E \otimes |0_L\rangle_B + |\Lambda_L^1\rangle_E \otimes |3\rangle_B, \\ |\Psi_1^R(0_R)\rangle_{BE} = U_{BE}\,(|0_R\rangle_B \otimes |E\rangle_E) = |\Phi_R^0\rangle_E \otimes \\ \otimes |0_R\rangle_B + |\Omega_R^0\rangle_E \otimes |1_R\rangle_B + |\Lambda_R^0\rangle_E \otimes |1\rangle_B, \\ |\Psi_1^R(1_R)\rangle_{BE} = U_{BE}\,(|1_R\rangle_B \otimes |E\rangle_E) = |\Phi_R^1\rangle_E \otimes \\ \otimes |1_R\rangle_B + |\Omega_R^1\rangle_E \otimes |0_R\rangle_B + |\Lambda_R^1\rangle_E \otimes |1\rangle_B. \quad (25)$$

Формула (25) есть разложение состояния в тензорном произведении пространств состояний. Пусть ортонормированный базис в пространстве состояний Евы есть $\{|\mu\rangle_E\}_{\mu=1}^{\dim(H_E)}$, $\dim(H_E)$ — размерность пространства. Ортонормированный базис в пространстве Боба (размерность равна 3) может быть выбран разными способами. Поскольку остаются только те посылки, в которых базисы Алисы и Боба совпадают, удобно в качестве базиса разложения выбрать базис измерений, $\{|0_L\rangle_B, |1_L\rangle_B, |3\rangle_B\}$ для базиса L, аналогично для базиса R. Базисом в тензорном произведении является произведение всевозможных пар базисных векторов:

$$\{|\mu\rangle_E \otimes |0_L\rangle_B, \quad |\mu\rangle_E \otimes |1_L\rangle_B, \quad |\mu\rangle_E \otimes |3\rangle_B\}_{\mu=1}^{\dim(H_E)}.$$

Формула (25) представляет собой краткую запись, например, для 0_L:

$$|\Psi_1^L(0_L)\rangle_{BE} = U_{BE}\,(|0_L\rangle_B \otimes |E\rangle_E) =$$
$$= \sum_{\mu}^{\dim(H_E)} c_{\mu,0}|\mu\rangle_E \otimes |0_L\rangle_B + \sum_{\mu}^{\dim(H_E)} c_{\mu,1}|\mu\rangle_E \otimes |1_L\rangle_B + \sum_{\mu}^{\dim(H_E)} c_{\mu,3}|\mu\rangle_E \otimes |3\rangle_B,$$

где

$$|\Phi_L^0\rangle_E \otimes |0_L\rangle_B = \sum_{\mu}^{\dim(H_E)} c_{\mu,0}|\mu\rangle_E \otimes |0_L\rangle_B,$$

$$|\Omega_L^0\rangle_E \otimes |1_L\rangle_B = \sum_{\mu}^{\dim(H_E)} c_{\mu,1}|\mu\rangle_E \otimes |1_L\rangle_B,$$

$$|\Lambda_L^0\rangle_E \otimes |3\rangle_B = \sum_{\mu}^{\dim(H_E)} c_{\mu,3}|\mu\rangle_E \otimes |3\rangle_B.$$

Про состояния $|\Phi_{L,R}^{0,1}\rangle_E$, $|\Omega_{L,R}^{0,1}\rangle_E$ и $|\Lambda_{L,R}^{0,1}\rangle_E$ не делается пока никаких предположений. Матрица плотности, которую «видит» Боб до измерений, например, для 0_L равна

$$\rho_B^L(0,\text{before}) = \mathrm{Tr}_E\{(|\Phi_L^0\rangle_E \otimes |0_L\rangle_B + |\Omega_L^0\rangle_E \otimes |1_L\rangle_B + |\Lambda_L^0\rangle_E \otimes |3\rangle_B)({}_E\langle\Phi_L^0| \otimes {}_B\langle|0_L| + {}_E\langle\Omega_L^0| \otimes {}_B\langle 1_L| + {}_E\langle\Lambda_L^0| \otimes {}_B\langle 3|)\}. \quad (26)$$

После измерений над матрицей плотности $\rho_B^L(0,\text{before})$ в базисе $\{|0_L\rangle_B, |1_L\rangle_B, |3\rangle_B\}$ Боб получит результат 0 с вероятностью

$${}_E\langle\Phi_L^0|\Phi_L^0\rangle_E = \mathrm{Tr}_B\{|0_L\rangle_{BB}\langle 0_L|\rho_B^L(0,\text{before})\}.$$

При этом, согласно проекционному постулату фон Неймана–Людерса, у Боба будет состояние $\rho_B^L(0,\text{before}) \to |0_L\rangle_{BB}\langle 0_L|$. Подсистема Евы при таком исходе измерения у Боба окажется в состоянии

$$\mathrm{Tr}_B\{(|0_L\rangle_{BB}\langle 0_L|)(|\Psi_1^L(0_L)\rangle_{BEBE}\langle\Psi_1^L(0_L)|)\} = |\Phi_1^L(0_L)\rangle_{EE}\langle\Phi_1^L(0_L)|.$$

Аналогично для двух других исходов измерений.

Подсистема Боба после измерения с вероятностью ${}_E\langle\Omega_L^0|\Omega_L^0\rangle_E$ окажется в состоянии $|1_L\rangle_{BB}\langle 1_L|$. Ева будет «видеть» свою подсистему в состоянии $|\Omega_L^0\rangle_{EE}\langle\Omega_L^0|$. Вероятность исхода в контрольном временно́м окне *3* равна ${}_E\langle\Lambda_L^0|\Lambda_L^0\rangle_E$. Боб при этом «видит» состояние $|3\rangle_{BB}\langle 3|$, соответственно, у Евы будет состояние $|\Lambda_L^0|\rangle_{EE}\langle\Lambda_L^0|$.

В итоге Боб «видит» следующую матрицу плотности:

$$\rho_B^L(0) = {}_E\langle\Phi_L^0|\Phi_L^0\rangle_E\ |0_L\rangle_{BB}\langle 0_L| + {}_E\langle\Omega_L^0|\Omega_L^0\rangle_E \times |1_L\rangle_{BB}\langle 1_L| + {}_E\langle\Lambda_L^0|\Lambda_L^0\rangle_E\ |3\rangle_{BB}\langle 3|. \quad (27)$$

Матрица плотности, которую «видит» Ева, равна

$$\rho_E^L(0) = |\Phi_L^0|\rangle_{EE}\langle\Phi_L^0| + |\Omega_L^0|\rangle_{EE}\langle\Omega_L^0| + |\Lambda_L^0|\rangle_{EE}\langle\Lambda_L^0|. \quad (28)$$

Частичный след по подпространству Евы матрицы плотности Боб–Ева (26) до измерений содержит перекрестные слагаемые со скалярными произведениями ${}_E\langle\Phi_L^0|\Omega_L^0\rangle_E$ и т. д. и, соответственно, перекрестные слагаемые $|0_L\rangle_{BB}\langle 1_L|$ и т. д., которые пропадают после измерений Боба. Перекрестные слагаемые несущественны, и после измерений ситуация выглядит так, как если бы состояния Евы были ортогональны — отсутствуют перекрестные скалярные произведения в (27). Более того, ортогональность состояний гарантирует Еве сразу после измерений Боба, по состоянию, которое у нее возникает, достоверно знать, какой отсчет — правильный, ошибочный (по сравнению логических переменных у Алисы и Боба) или контрольный, был получен Бобом в данном измерении. После измерения Ева видит состояния $|\Phi_L^0|\rangle_{EE}\langle\Phi_L^0|$ или $|\Omega_L^0|\rangle_{EE}\langle\Omega_L^0|$ или $|\Lambda_L^0|\rangle_{EE}\langle\Lambda_L^0|$. Если состояния попарно ортогональны, то они достоверно различимы. Ева достоверно знает тип отсчета (но не сам логический отсчет 0 или 1, см. ниже) — правильный, неправильный или контрольный. Если состояния неортогональны, то достоверно этого сделать нельзя. Поэтому первое выражение в (25) является фактически разложением Шмидта [26], т. е. векторы базиса измерений Боба

являются собственными векторами частичной матрицы плотности Боба (27), по которым происходит разложение в (25).

Поскольку состояния в пространстве Боба, по которым происходит разложение в (25), являются собственными векторами частичной матрицы плотности Боба (27), теорема Шмидта гарантирует, что состояния в пространстве Евы также будут автоматически собственными состояниями частичной матрицы плотности Евы, т. е. будут ортогональными. Ненулевые собственные числа частичных матриц плотности Боба и Евы по теореме Шмидта совпадают.

Дальнейшие шаги по конструированию атаки Евы следующие. Имеются свойства симметрии по 0 и 1, а также симметрия между базисами. Состояния, отвечающие 0 и 1 внутри базиса и в разных базисах, посылаются равновероятно, поэтому вероятности правильного/ошибочного отсчета для 0 и 1 внутри одного базиса, а также в разных базисах естественно считать одинаковыми. Аналогично вероятности отсчетов в контрольном окне для 0 и 1 внутри одного базиса и в разных базисах должны быть одинаковыми. Это приводит к соотношениям для вероятностей

$$
\begin{aligned}
{}_E\langle\Phi_L^0|\Phi_L^0\rangle_E = {}_E\langle\Phi_L^1|\Phi_L^1\rangle_E = {}_E\langle\Phi_R^0|\Phi_R^0\rangle_E = \\
= {}_E\langle\Phi_R^1|\Phi_R^1\rangle_E = (1-q_1)(1-Q_1). \quad (29)
\end{aligned}
$$

Формула (29) дает вероятности правильного отсчета в информационных окнах Боба, которые удобно выразить через два наблюдаемых параметра на приемной стороне: q_1 и Q_1, где $1-q_1$ — полная вероятность отсчетов (правильных и неправильных) в информационных окнах, $1-Q_1$ — вероятность правильных отсчетов, Q_1 — вероятность неправильных отсчетов. Соответственно вероятности ошибочного отсчета

$$
\begin{aligned}
{}_E\langle\Omega_L^0|\Omega_L^0\rangle_E = {}_E\langle\Omega_L^1|\Omega_L^1\rangle_E = {}_E\langle\Omega_R^0|\Omega_R^0\rangle_E = \\
= {}_E\langle\Omega_R^1|\Omega_R^1\rangle_E = (1-q_1)Q_1. \quad (30)
\end{aligned}
$$

Вероятности контрольного отсчета — отсчеты в окне *3* базиса L (окне *1* базиса R)

$$
\begin{aligned}
{}_E\langle\Lambda_L^0|\Lambda_L^0\rangle_E = {}_E\langle\Lambda_L^1|\Lambda_L^1\rangle_E = {}_E\langle\Lambda_R^0|\Lambda_R^0\rangle_E = \\
= {}_E\langle\Lambda_R^1|\Lambda_R^1\rangle_E = q_1. \quad (31)
\end{aligned}
$$

Условие сохранения нормировки (следствие унитарности оператора U_{BE}) записывается как

$$
\begin{aligned}
{}_E\langle\Phi_L^0|\Phi_L^0\rangle_E + {}_E\langle\Omega_L^0|\Omega_L^0\rangle_E + {}_E\langle\Lambda_L^0|\Lambda_L^0\rangle_E = \\
= {}_E\langle\Phi_L^1|\Phi_L^1\rangle_E + {}_E\langle\Omega_L^1|\Omega_L^1\rangle_E + {}_E\langle\Lambda_L^1|\Lambda_L^1\rangle_E = \\
= {}_E\langle\Phi_R^0|\Phi_R^0\rangle_E + {}_E\langle\Omega_R^0|\Omega_R^0\rangle_E + {}_E\langle\Lambda_R^0|\Lambda_R^0\rangle_E = \\
= {}_E\langle\Phi_R^1|\Phi_R^1\rangle_E + {}_E\langle\Omega_R^0|\Omega_R^1\rangle_E + {}_E\langle\Lambda_R^1|\Lambda_R^1\rangle_E = 1. \quad (32)
\end{aligned}
$$

Унитарность оператора требует сохранения скалярных произведений. Для состояний в базисе L имеем

$$
\begin{aligned}
{}_B\langle 0_L|1_L\rangle_B = {}_{BE}\langle\overline{0}|\overline{0}_L\rangle_{BE} = ({}_E\langle\Phi_L^0|\Omega_L^1\rangle_E + \\
+ {}_E\langle\Omega_L^0|\Phi_L^1\rangle_E) + {}_E\langle\Lambda_L^0|\Lambda_L^1\rangle_E = 0. \quad (33)
\end{aligned}
$$

Первые два слагаемых в правой части (33) в скобках функционально зависят от двух наблюдаемых параметров — от доли отсчетов в информационных окнах $1-q_1$ и от вероятности ошибки в этих окнах Q_1. Последнее слагаемое зависит только от доли отсчетов в контрольном окне q_1 и не зависит от наблюдаемой вероятности ошибки Q_1. Причем это имеет место при любых значениях Q_1 и q_1. Поэтому по отдельности два слагаемых в скобках и последнее слагаемое, должны быть равны 0. Имеем ${}_E\langle\Lambda_L^0|\Lambda_L^1\rangle_E = 0$, т. е. данные векторы ортогональны. Аналогично в базисе R. Условия симметрии между 0 и 1, а также симметрии между базисами L и R дают ${}_E\langle\Omega_L^0|\Phi_L^1\rangle_E = {}_E\langle\Omega_L^1|\Phi_L^0\rangle_E$, далее ${}_E\langle\Omega_L^1|\Phi_L^0\rangle_E = ({}_E\langle\Phi_L^0|\Omega_L^1\rangle_E)^*$, что приводит к тому, что скалярное произведение является вещественным, $\mathrm{Re}({}_E\langle\Phi_L^0|\Omega_L^1\rangle_E)$. Таким образом, от мнимой части скалярного произведения нет зависимости, поэтому без ограничения общности можно считать скалярное произведение вещественным. Из формулы (33) следует ${}_E\langle\Phi_L^0|\Omega_L^1\rangle_E = 0$, что означает ортогональность состояний.

Из рассмотрения выше следует, что векторы $|\Phi_L^{0,1}\rangle_E$ и $|\Omega_L^{0,1}\rangle_E$ лежат в ортогональных подпространствах. Скалярные произведения между группами векторов $(|\Phi_L^{0,1}\rangle_E, |\Omega_L^{0,1}\rangle_E)$ и $|\Lambda_L^{0,1}\rangle_E$ не возникают, поэтому без ограничения общности можно считать векторы из разных групп ортогональными. Этот произвол — отсутствие скалярных произведений — возникает фактически из-за ортогональности информационных состояний Боба $|0_L\rangle_E, |1_L\rangle_E$ и контрольного состояния $|3\rangle_B$.

На данный момент имеем, что векторы $\{|\Phi_L^{0,1}\rangle_E\}$, $\{|\Omega_L^{0,1}\rangle_E\}$ и $\{|\Lambda_L^{0,1}\rangle_E\}$ лежат в ортогональных подпространствах. Требования симметрии по базисам (см. выше) диктуют только равенство следующих скалярных произведений, но не их величину:

$$
{}_E\langle\Phi_L^0|\Phi_L^1\rangle_E = {}_E\langle\Phi_R^0|\Phi_R^1\rangle_E, \quad (34)
$$

$$
{}_E\langle\Omega_L^0|\Omega_L^1\rangle_E = {}_E\langle\Omega_R^0|\Omega_R^1\rangle_E, \quad (35)
$$

$$ {}_E\langle\Lambda_L^0|\Lambda_L^1\rangle_E = {}_E\langle\Lambda_R^0|\Lambda_R^1\rangle_E = 0. \quad (36)$$

В (34)–(36) использовано условие симметрии по базисам. Ортогональность в (36) следует из (33) выше. Для дальнейшего продвижения удобно ортогональным преобразованием перейти от информационного базиса к базису временны́х окон. Ортогональное преобразование базиса в пространстве Боба индуцирует ортогональное преобразование состояний в пространстве Евы. Находим

$$ U_{BE}\left(|i\rangle_B \otimes |E\rangle_E\right) = |\tilde{i}\rangle_{BE} = \\ = \sum_{j=1,2,3} |a_{ij}\rangle_E \otimes |j\rangle_B, \quad (37)$$

где $|i\rangle_B$, $|j\rangle_B$ — базисные состояния Боба, индексы i, j обозначают временны́е окна $i, j = 1, 2, 3$. Ортогональный поворот от одного базиса к другому сохраняет ортогональность новых базисных векторов. Например, для 0_L векторы $|\Psi_L^0\rangle_E, |\Omega_L^0\rangle_E, |\Lambda_L^0\rangle_E$ (см. выше) — базис, новый набор векторов при фиксированном i $|a_{ij}\rangle_E$ $(j = 1, 2, 3)$ также ортогонален, т. е. образует базис. Разложение (37) также есть разложение Шмидта. Состояния в (37) и в (25) связаны линейными соотношениями:

$$ |\Phi_L^{0,1}\rangle_E = \frac{(|a_{11}\rangle + |a_{22}\rangle) \pm (|a_{12}\rangle + |a_{21}\rangle)}{2}, \\ |\Omega_L^{0,1}\rangle_E = \frac{(|a_{11}\rangle - |a_{22}\rangle) \mp (|a_{12}\rangle - |a_{21}\rangle)}{2}, \quad (38)$$

$$ |\Lambda_L^{0,1}\rangle_E = \frac{(|a_{23}\rangle \pm |a_{13}\rangle)}{\sqrt{2}}, \quad (39)$$

$$ |\Phi_R^{0,1}\rangle_E = \frac{(|a_{22}\rangle + |a_{33}\rangle) \pm (|a_{23}\rangle + |a_{32}\rangle)}{2}, \\ |\Omega_L^{0,1}\rangle_E = \frac{(|a_{22}\rangle - |a_{33}\rangle) \mp (|a_{23}\rangle - |a_{32}\rangle)}{2}, \quad (40)$$

$$ |\Lambda_L^{0,1}\rangle_E = \frac{(|a_{21}\rangle \pm |a_{31}\rangle)}{\sqrt{2}}. \quad (41)$$

Далее при выполнении условий (29)–(36) удобно пользоваться представлением (38)–(41). Существуют девять векторов $|a_{ij}\rangle_E$, которые не все являются линейно независимыми. Поскольку имеются семь условий (29)–(36), которые выражаются через данные векторы, в качестве семи линейно независимых векторов удобно выбрать семь ортогональных векторов, через линейные комбинации которых выражаются векторы $|a_{ij}\rangle_E$ и которые обозначим как $\{|xx\rangle, |xy\rangle, |zx\rangle, |yy\rangle, |yx\rangle, |zz\rangle, |xz\rangle\}$. Отметим, что условий (29)–(36) реально семь, поскольку соотношения для базисов L и R выражаются через одни и те же девять функций $|a_{ij}\rangle_E$.

Выражая состояния $|a_{ij}\rangle_E$ как линейные комбинации $\{|xx\rangle, |xy\rangle, |zx\rangle, |yy\rangle, |yx\rangle, |zz\rangle, |xz\rangle\}$ с некоторыми коэффициентами, затем подставляя $|a_{ij}\rangle_E$ в условия (29)–(36), получаем систему линейных уравнений, решение которой позволяет однозначно выразить коэффициенты разложения через наблюдаемые параметры $q_1 = \delta^2/2$, $Q_1 = (1 - \cos\alpha)/2$. Из-за ортогональности семи векторов в систему уравнений входят только квадраты модулей коэффициентов разложения по семи векторам. Линейно независимыми являются только семь векторов из девяти (42)–(45) (см. ниже), поэтому девять векторов можно разложить по ортогональному набору семи векторов. Формально коэффициенты разложения можно выбрать комплексными, но, поскольку при определении коэффициентов важны только их квадраты модулей, имеется произвол, поэтому без ограничения общности коэффициенты могут быть выбраны вещественными. С учетом (29)–(36) находим

$$ |a_{11}\rangle_E = \sqrt{1-\delta^2}|x\rangle \otimes |x\rangle, \\ |a_{12}\rangle_E = \frac{\delta}{\sqrt{2}}|x\rangle \otimes |y\rangle, \quad |a_{13}\rangle_E = \frac{\delta}{\sqrt{2}}|z\rangle \otimes |x\rangle, \quad (42)$$

$$ |a_{21}\rangle_E = \frac{\delta}{\sqrt{2}}(\cos\alpha|x\rangle \otimes |y\rangle + \sin\alpha|y\rangle \otimes |y\rangle), \\ |a_{22}\rangle_E = \sqrt{1-\delta^2}(\cos\alpha|x\rangle \otimes |x\rangle + \sin\alpha|y\rangle \otimes |x\rangle), \quad (43)$$

$$ |a_{23}\rangle_E = \frac{\delta}{\sqrt{2}}(\cos\alpha|z\rangle \otimes |z\rangle + \sin\alpha|x\rangle \otimes |z\rangle), \\ |a_{31}\rangle_E = \frac{\delta}{\sqrt{2}}|y\rangle \otimes |x\rangle, \quad |a_{32}\rangle_E = \frac{\delta}{\sqrt{2}}|z\rangle \otimes |z\rangle, \quad (44)$$

$$ |a_{33}\rangle_E = \sqrt{1-\delta^2}|x\rangle \otimes |x\rangle. \quad (45)$$

Действие супероператора Евы на однофотонную компоненту приводит к совместной матрице плотности Ева–Боб:

$$ \mathcal{T}_1[|\Psi_1^L(0)\rangle_{BB}\langle\Psi_1^L(0)|] = Y_1^E\left(|0_L\rangle_B \otimes |\Phi_L^0\rangle_E + \right. \\ \left. + |1_L\rangle_B \otimes |\Omega_L^0\rangle_E + |3c\rangle_B \otimes |\Lambda_L^0\rangle_E\right)\left({}_B\langle 0_L| \otimes {}_E\langle\Phi_L^0| + \right. \\ \left. + {}_B\langle 1_L| \otimes {}_E\langle\Omega_L^0| + {}_B\langle 3c| \otimes {}_E\langle\Lambda_L^0|\right), \quad (46)$$

$$ \mathcal{T}_1[|\Psi_1^L(1)\rangle_{BB}\langle\Psi_1^L(1)|] = Y_1^E\left(|1_L\rangle_B \otimes |\Phi_L^1\rangle_E + \right. \\ \left. + |0_L\rangle_B \otimes |\Omega_L^1\rangle_E + |3c\rangle_B \otimes |\Lambda_L^1\rangle_E\right)\left({}_B\langle 1_L| \otimes {}_E\langle\Phi_L^1| + \right. \\ \left. + {}_B\langle 0_L| \otimes {}_E\langle\Omega_L^1| + {}_B\langle 3c| \otimes {}_E\langle\Lambda_L^0|\right), \quad (47)$$

$$ \mathcal{T}_1[|\Psi_1^R(0)\rangle_{BB}\langle\Psi_1^R(0)|] = Y_1^E\left(|0_R\rangle_B \otimes |\Phi_R^0\rangle_E + \right. \\ \left. + |1_R\rangle_B \otimes |\Omega_R^0\rangle_E + |1c\rangle_B \otimes |\Lambda_R^0\rangle_E\right)\left({}_B\langle 0_R| \otimes {}_E\langle\Phi_R^0| + \right. \\ \left. + {}_B\langle 1_R| \otimes {}_E\langle\Omega_R^0| + {}_B\langle 1c| \otimes {}_E\langle\Lambda_R^0|\right), \quad (48)$$

$$\mathcal{T}_1[|\Psi_1^R(1)\rangle_{BB}\langle\Psi_1^R(1)|] = Y_1^E\left(|1_R\rangle_B\otimes|\Phi_R^1\rangle_E + \right.$$
$$+ |0_R\rangle_B\otimes|\Omega_R^1\rangle_E + |1c\rangle_B\otimes|\Lambda_R^1\rangle_E\left)\right.\left({}_B\langle 1_R|\otimes{}_E\langle\Phi_R^1| + \right.$$
$$\left. + {}_B\langle 0_R|\otimes{}_E\langle\Omega_R^1| + {}_B\langle 1c|\otimes{}_E\langle\Lambda_R^0|\right). \quad (49)$$

Отметим, что такой вид матрицы плотности Ева–Боб имеют до измерений Боба. Кроме того, матрицы плотности (46)–(49) нормированы на долю Y_1^E — не блокированных Евой однофотонных состояний.

6.3. Многофотонные компоненты

Атака Евы на однофотонную компоненту состояний всегда приводит к возмущению состояния. Для многофотонных компонент ситуация принципиально другая. Предполагается [6–11], что при обнаружении многофотонной компоненты подслушиватель часть фотонов оставляет в квантовой памяти, остальные невозмущенные через канал с меньшими потерями (в идеале без потерь) направляет на приемную сторону. Дождавшись раскрытия базисов, Ева проводит измерения над квантовой памятью уже в известном базисе и получает достоверный результат, поскольку внутри базиса состояния ортогональны. Однако явно не показано, как можно разделить многофотонную компоненту на пару факторизованных (независимых) состояний. Такое разделение является отнюдь не очевидным. Покажем, как можно разделить двухфотонное фоковское состояние на произведение однофотонных фоковских состояний.

Пусть обнаружено двухфотонное фоковское состояние $|2\rangle_B$. Ева использует симметричный светоделитель, а затем неразрушающее измерение числа фотонов на его выходах, определяет число фотонов на выходах. Если на одном из выходов обнаружено два фотона — состояние $|2\rangle_B$, то Ева повторяет процедуру, посылает это состояние опять на вход симметричного светоделителя. Такая ситуация реализуется с вероятностью $1/2$. Если на двух выходах при неразрушающих измерениях обнаружены однофотонные фоковские состояния $|1\rangle_B$ и $|1\rangle_E$, то состояние $|1\rangle_B$ направляется к Бобу, а состояние $|1\rangle_E$ Ева оставляет у себя в квантовой памяти и ждет разглашения базисов. Весь описанный выше набор действий — преобразование входного состояния в выходное — дается действием супероператора. Вид супероператора зависит от того, сколько фотонов обнаружено в линии.

Аналогично для многофотонных компонент состояний с $k > 2$, по-видимому, можно сконструировать соответствующий супероператор, который разделяет многофотонное состояние на произведение состояний. Однако вид супероператора для состояний с $k > 2$ не является очевидным в отличие от состояний с $k = 2$. Как будет видно ниже, явный вид супероператора не потребуется. Достаточно будет того факта, что Ева в принципе может разделить многофотонные состояния и оставить в квантовой памяти часть невозмущенных состояний из многофотонной компоненты поля.

Обозначим через Y_k^E долю посылок с многофотонной компонентой с $k \geq 2$, которую Ева направляет на приемную сторону. В пользу Евы считаем, что детекторы у Евы идеальные. В итоге для действия супероператора Евы для многофотонных компонент состояний получаем

$$\mathcal{T}_k[|\Theta_k^{L,R}(0,1)\rangle_{BB}\langle\Theta_k^{L,R}(0,1)|] =$$
$$= Y_k^E|\Theta_k^{L,R}(0,1)\rangle_{BEBE}\langle\Theta_k^{L,R}(0,1)|, \quad k\geq 2, \quad (50)$$

где состояние

$$|\Theta_k^{L,R}(0,1)\rangle_{BE} = |\Theta_{k_B}^{L,R}(0,1)\rangle_B\otimes|\Theta_{k_E}^{L,R}(0,1)\rangle_E$$

является факторизованным. В таком виде состояние записано лишь для краткости обозначений. При измерении такого состояния ошибки на приемной стороне будут возникать только за счет неидеальности аппаратуры Боба, например, неточной балансировки интерферометра Маха–Цандера и темновых шумов лавинных однофотонных детекторов (см. ниже). В итоге полная матрица плотности после PNS-атаки Евы имеет вид

$$\rho_{BE}^{L,R}(0,1) =$$
$$= \mathcal{T}\left[e^{-2\mu}\sum_{k=0}^{\infty} g_k\frac{\mu^k}{k!}|\Theta^{L,R}(0,1)\rangle_{BB}\langle\Theta^{L,R}(0,1)|\right] =$$
$$= e^{-2\mu}\sum_{k=0}^{\infty} Y_k^E g_k\frac{\mu^k}{k!}\times$$
$$\times|\Theta_k^{L,R}(0,1)\rangle_{BEBE}\langle\Theta_k^{L,R}(0,1)|, \quad (51)$$

где $g_k = 2^k$ и Y_k^E имеет смысл условной вероятности того, что Ева проведет действия, при которых исходное состояние перейдет в состояние $|\Theta_k^{L,R}(0,1)\rangle_{BE}$ — совместное состояние Ева–Боб.

7. ДЛИНА СЕКРЕТНОГО КЛЮЧА В АСИМПТОТИЧЕСКОМ ПРЕДЕЛЕ ДЛИННЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Нашей целью является вычисление длины секретного ключа как функции наблюдаемых параметров на приемной стороне, q_1 и Q_1. Длина секретного

ключа (ℓ_n) в асимптотическом пределе длинных последовательностей $n \to \infty$ выражается через условную энтропию фон Неймана совместной матрицы плотности Алиса–Ева и количество информации в битах, расходуемое на коррекцию ошибок [25]. Данная утечка выражается через условную классическую энтропию Шеннона для состояния Алиса–Боб. Приведем сначала формулу для длины секретного ключа, а затем перейдем к вычислению энтропий фон Неймана и Шеннона для соответствующих состояний. Формула для длины секретного ключа в пределе бесконечно длинных последовательностей ($n \to \infty$ — число зарегистрированных на приемной стороне посылок в одинаковых базисах) имеет вид (см. подробности в [25])

$$\lim_{n\to\infty}\left(\frac{\ell_n}{n}\right) = \lim_{n\to\infty}\frac{H(\rho_{XE}^{(n)}|\rho_E^{(n)}) - \overline{\text{leak}}_n}{n}, \qquad (52)$$

где $\overline{\text{leak}}_n$ — информация в битах, расходуемая на исправление ошибок в первичном ключе длины n. Поскольку PNS-атака в целом является атакой прием–перепосыл, матрица плотности Алиса–Ева $\rho_{XE}^{(n)}$ имеет структуру тензорного произведения $\rho_{XE}^{(n)} = \rho_{XE}^{n\otimes}$. Соответственно утечка информации при коррекции ошибок на приемной стороне выражается через матрицу плотности Алиса–Боб $\rho_{XY}^{n\otimes}$ после измерений Боба на приемной стороне, где $\mathcal{Y} = \{0,1\}^n$ — множество битовых строк (сырой ключ Боба). В шенноновском пределе при коррекции ошибок случайными кодами минимальная утечка информации к подслушивателю дается выражением $\text{leak}_n \to nH(X|Y)$, где $H(X|Y) = H(\rho_{XY}|\rho_Y)$ — условная классическая энтропия Шеннона. Предел Шеннона является теоремой существования и конструктивно недостижим. В реальной ситуации коррекция ошибок происходит при помощи эффективно реализуемых кодов коррекции ошибок, которые дают несколько большую утечку информации к подслушивателю. LDPC-коды дают утечку, незначительно превышающую предел Шеннона (см., например, [27], где была продемонстрирована рекордная эффективность LDPC-кодов), поэтому в дальнейшем при вычислении утечки информации при коррекции ошибок будем использовать LDPC-коды.

Формула (52) имеет интуитивно понятную интерпретацию. Неформально величина $H(\rho_{XE}^{(n)}|\rho_E^{(n)})$ имеет смысл нехватки информации Евы о битовой строке $X \in \mathcal{X}$ Алисы из множества $\mathcal{X} = \{0,1\}^n$ при условии, что в ее распоряжении находится квантовая система E, коррелированная с данной строкой. Длина ключа в битах есть нехватка информации Евы минус информация, которую Ева получает через открытый классический канал связи при коррекции ошибок у Боба.

В итоге длина секретного ключа в битах, точнее, доля секретных битов в пересчете на одну зарегистрированную посылку n в совпадающих базисах Алисы и Боба — на длину сырого ключа, становится равной

$$\lim_{n\to\infty}\left(\frac{\ell_n}{n}\right) = H(\rho_{XE}|\rho_E) - \text{leak}, \qquad (53)$$

здесь leak — доля битов, расходуемых на коррекцию ошибок в пересчете на одну позицию сырого ключа.

8. СОВМЕСТНЫЕ МАТРИЦЫ ПЛОТНОСТИ АЛИСА–БОБ–ЕВА ДО ИЗМЕРЕНИЙ НА ПРИЕМНОЙ СТОРОНЕ

Важно отличать состояния, которые возникают сразу после атаки Евы, от состояний, которые получаются после измерений на приемной стороне Боба. Измерения на приемной стороне изменяют состояния Евы. Например, однофотонная компонента исходных состояний оказывается в запутанном состоянии (25) между Бобом и Евой, поэтому измерения Боба отражаются на состояниях, которые будет «видеть» Ева после измерений Боба. Сначала рассмотрим состояния, которые возникают после атаки Евы, но до измерений Боба. В следующем разделе рассмотрим модификацию состояний Боб–Ева после измерений Боба.

Согласно предыдущему разделу, для вычисления длины секретного ключа потребуются совместные матрицы плотности Алиса–Боб–Ева. Удобнее воспользоваться следующим приемом. Алиса сохраняет у себя копию посланного информационного состояния, которая никому недоступна (за это отвечает индекс X в матрицах плотности).

Важно отметить одно обстоятельство. Поскольку состояния Евы (25) ортогональны, частичная матрица плотности Боба будет иметь диагональный вид в базисе измерений, значит, можно сразу записать матрицу плотности Алиса–Боб–Ева в диагональном виде. До измерений Боба в информационных окнах в базисе L матрица плотности становится равной

$$\rho_{XBE}(0_L) = \sum_{k=0}^{\infty}\rho_{XBE}^{(k)}(0_L), \qquad (54)$$

где k — фотонная часть матрицы плотности, $k=0$ отвечает вакуумной компоненте. Далее

$$\rho^{(0)}_{XBE}(0_L) = e^{-2\mu}|0_L\rangle_{XX}\langle 0_L| \otimes (|\mathrm{vac}\rangle_{BB}\langle \mathrm{vac}|) \otimes \otimes (|\mathrm{vac}\rangle_{EE}\langle \mathrm{vac}|)\,. \quad (55)$$

Однофотонная компонента матрицы плотности записывается как

$$\rho^{(1)}_{XBE}(0_L) = e^{-2\mu}|0_L\rangle_{XX}\langle 0_L| \otimes \otimes \left\{\mu g_1 Y_1^E \left[|0_L\rangle_{BB}\langle 0_L| \otimes |\Phi_0^L\rangle_{EE}\langle \Phi_0^L| + |1_L\rangle_{BB}\langle 1_L| \otimes |\Omega_0^L\rangle_{EE}\langle \Omega_0^L| + |3c\rangle_{BB}\langle 3c| \otimes \otimes |\Lambda_0^L\rangle_{EE}\langle \Lambda_0^L|\right]\right\}, \quad (56)$$

многофотонные компоненты матрицы плотности —

$$\rho^{(k)}_{XBE}(0_L) = e^{-2\mu}\frac{\mu^k g_k}{k!} \times \times Y_k^E |0_L\rangle_{XX}\langle 0_L| \otimes |\Theta_k^L(0)\rangle_{BEBE}\langle \Theta_k^L(0)|. \quad (57)$$

Матрицы плотности, когда Алиса посылала 1_L, имеют вид

$$\rho_{XBE}(1_L) = \sum_{k=0}^{\infty} \rho^{(k)}_{XBE}(1_L). \quad (58)$$

Далее

$$\rho^{(0)}_{XBE}(1_L) = e^{-2\mu}|1_L\rangle_{XX}\langle 1_L| \otimes (|\mathrm{vac}\rangle_{BB}\langle \mathrm{vac}|) \otimes \otimes (|\mathrm{vac}\rangle_{EE}\langle \mathrm{vac}|)\,. \quad (59)$$

Однофотонная компонента матрицы плотности записывается как

$$\rho^{(1)}_{XBE}(1_L) = e^{-2\mu}|1_L\rangle_{XX}\langle 1_L| \otimes \otimes \left\{\mu g_1 Y_1^E \left[|1_L\rangle_{BB}\langle 1_L| \otimes |\Phi_1^L\rangle_{EE}\langle \Phi_1^L| + |1_L\rangle_{BB}\langle 1_L| \otimes |\Omega_1^L\rangle_{EE}\langle \Omega_1^L| + |1c\rangle_{BB}\langle 1c| \otimes |\Lambda_1^L\rangle_{EE}\langle \Lambda_1^L|\right]\right\}, \quad (60)$$

многофотонные компоненты матрицы плотности —

$$\rho^{(k)}_{XBE}(1_L) = e^{-2\mu}\frac{\mu^k g_k}{k!} Y_k^E \times \times |1_L\rangle_{XX}\langle 1_L| \otimes |\Theta_k^L(1)\rangle_{BEBE}\langle \Theta_k^L(1)|. \quad (61)$$

В итоге частичные матрицы плотности Алиса–Ева до измерений Боба имеют вид

$$\rho_{XE}(0_L) = e^{-2\mu}|0_L\rangle_{XX}\langle 0_L| \otimes \otimes \left\{|\mathrm{vac}\rangle_{EE}\langle \mathrm{vac}| + \mu g_1 Y_1^E \left[|\Phi_0^L\rangle_{EE}\langle \Phi_0^L| + |\Omega_0^L\rangle_{EE}\langle \Omega_0^L| + |\Lambda_0^L\rangle_{EE}\langle \Lambda_0^L|\right] + \sum_{k=2}^{\infty} \frac{\mu^k}{k!} g_k Y_k^E |0_L^{(k)}\rangle_{EE}\langle 0_L^{(k)}|\right\}, \quad (62)$$

где введено обозначение

$$|0_L^{(k)}\rangle_{EE}\langle 0_L^{(k)}| = \mathrm{Tr}_B\{|\Theta_k^L(0)\rangle_{BEBE}\langle \Theta_k^L(0)|\}.$$

Здесь также введено обозначение: $|0_L^{(k)}\rangle_E$ — часть многофотонного невозмущенного состояния, которое остается у Евы и при измерении которого, после раскрытия базисов Ева получит достоверную информацию о передаваемом бите ключа, в данном случае о 0_L. Аналогично для состояния 1_L

$$\rho_{XE}(1_L) = e^{-2\mu}|1_L\rangle_{XX}\langle 1_L| \otimes \otimes \left\{|\mathrm{vac}\rangle_{EE}\langle \mathrm{vac}| + \mu g_1 Y_1^E \left[|\Phi_1^L\rangle_{EE}\langle \Phi_1^L| + |\Omega_1^L\rangle_{EE}\langle \Omega_1^L| + |\Lambda_1^L\rangle_{EE}\langle \Lambda_1^L|\right] + \sum_{k=2}^{\infty} \frac{\mu^k}{k!} g_k Y_k^E |1_L^{(k)}\rangle_{EE}\langle 1_L^{(k)}|\right\}, \quad (63)$$

$$|1_L^{(k)}\rangle_{EE}\langle 1_L^{(k)}| = \mathrm{Tr}_B\{|\Theta_k^L(1)\rangle_{BEBE}\langle \Theta_k^L(1)|\},$$

где $|1_L^{(k)}\rangle_E$ — часть исходного многофотонного состояния, которое Ева оставляет у себя в квантовой памяти.

9. ИЗМЕРЕНИЯ НА ПРИЕМНОЙ СТОРОНЕ

Любое измерение в квантовой механике дается разложением единицы — формальное описание измерительного прибора. Применительно к данному протоколу такое разложение единицы выглядит следующим образом:

$$I_B = \sum_{k=1}^{\infty} I_B^{(k)}, \quad (64)$$

где разложение единичных операторов $I_B^{(k)}$ задается выбором базиса измерений. В реальной ситуации перед измерением состояний на приемной стороне происходит их преобразование на интерферометре Маха–Цандера (МЦ) и только потом происходит регистрация лавинными однофотонными детекторами. Результатом измерений является отсчет одного из двух детекторов на выходах интерферометра МЦ в информационном или контрольном временном окне.

Рассмотрим сначала преобразование состояний на интерферометре МЦ. Неидеальная балансировка интерферометра, несимметричность светоделителей также может вносить ошибки в битовую последовательность Боба. Несимметричность светоделителей не важна, поскольку самокомпенсируется при используемой реализации протокола (см. детали в [3],

а также формулы (54)–(63)). Остается только учесть неточность балансировки интерферометра МЦ.

Кроме того, лавинные детекторы имеют неидеальную (не равную единице) квантовую эффективность η, а также ненулевые темновые шумы, которые приводят к ошибочным отсчетам.

Рассмотрим преобразование и детектирование однофотонной компоненты состояний на стороне Боба, поскольку только из нее формируется секретный ключ. Явный вид преобразования многофотонных компонент состояний, в отличие от однофотонной компоненты состояний, для анализа не потребуется.

Рассмотрим преобразование информационных и контрольных состояний, фигурирующих в матрице плотности Алиса–Боб–Ева до измерений (46)–(51) на примере $|0_L\rangle_B$ и $|3\rangle_B$. Удобнее использовать преобразование соответствующих операторов, а не самих состояний. Входному состоянию, например, для 0_L отвечают операторы $-\frac{a_1^\dagger+a_2^\dagger}{\sqrt{2}}$, где $a_{1,2}^\dagger$ — операторы рождения фоковских состояний во временны́х окнах *1* и *2*. Преобразование операторов на прямом проходе на светоделителе имеет вид

$$\frac{1}{\sqrt{2}}\begin{pmatrix} \dfrac{a_1^\dagger+a_2^\dagger}{\sqrt{2}} \\ -\dfrac{a_1^\dagger+a_2^\dagger}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} \dfrac{a_1^\dagger+a_2^\dagger}{\sqrt{2}} \\ 0 \end{pmatrix}, \quad (65)$$

где операторы рождения в вектор-столбце отвечают операторам рождения на верхнем и нижнем путях интерферомтера МЦ.

Светоделители считаем идеально симметричными, поскольку несимметричность светоделителей компенсируется на обратном проходе после отражения состояний от фарадеевских зеркал. После отражения от зеркал и задержки состояний в одном из плеч интерферометра состояния принимают вид

$$\frac{1}{\sqrt{2}}\begin{pmatrix} \dfrac{a_1^\dagger+a_2^\dagger}{\sqrt{2}} \\ e^{i\varphi}\left(\dfrac{a_2^\dagger+a_3^\dagger}{\sqrt{2}}\right) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi}\delta_{\rightarrow} \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} \dfrac{a_1^\dagger+a_2^\dagger}{\sqrt{2}} \\ \dfrac{a_1^\dagger+a_2^\dagger}{\sqrt{2}} \end{pmatrix}, \quad (66)$$

где φ — фазовый сдвиг, который получают состояния при прохождении по верхнему и нижнему путям интерферометра МЦ за счет неточной балансировки и который будет вносить вклад в ошибку при детектировании состояний. Символ $\delta_{\rightarrow}$ обозначает изменение индекса на единицу для состояний, распространяющихся по длинному пути интерферометра. На обратном проходе преобразование операторов на светоделителе принимает вид

$$\frac{1}{\sqrt{2}}\begin{pmatrix} \dfrac{1}{2}a_1^\dagger + \left(\dfrac{1-e^{i\varphi}}{2}\right)a_2^\dagger - \dfrac{e^{i\varphi}}{2}a_3^\dagger \\ \dfrac{1}{2}a_1^\dagger + \left(\dfrac{1+e^{i\varphi}}{2}\right)a_2^\dagger + \dfrac{e^{i\varphi}}{2}a_3^\dagger \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} \dfrac{a_1^\dagger+a_2^\dagger}{\sqrt{2}} \\ e^{i\varphi}\left(\dfrac{a_2^\dagger+a_3^\dagger}{\sqrt{2}}\right) \end{pmatrix}. \quad (67)$$

Рассмотрим вероятность детектирования в информационном временном окне. Далее от операторов, отвечающих состояниям во временных окнах, можно уже перейти к вероятности фотоотсчета в соответствующем временном окне. Отсчеты в информационном временном окне интерпретируются как отсчеты от информационных состояний. С учетом (65)–(67) для вероятности детектирования состояний на двух выходах интерферометра находим

$$\begin{aligned} |0_L\rangle_B \to \frac{1}{2}\eta_1\frac{|1-e^{i\varphi}|^2}{4} + p_{d1} = \\ = \frac{\eta_1}{2}\sin^2\left(\frac{\varphi}{2}\right) + p_{d1} = \frac{\eta_1}{2}(1-Q_B) + p_{d1}, \\ |1_L\rangle_B \to \frac{1}{2}\eta_2\frac{|1+e^{i\varphi}|^2}{4} + p_{d2} = \\ = \frac{\eta_2}{2}\cos^2\left(\frac{\varphi}{2}\right) + p_{d2} = \frac{\eta_2}{2}Q_B + p_{d2}. \end{aligned} \quad (68)$$

Интерпретация формул (68) достаточно прозрачна. Если из канала поступило состояние $|0_L\rangle_B$, то отсчет в информационном окне *2* является правильным, и если возник отсчет в первом лавинном детекторе, то результат интерпретируется как 0. Вероятность отсчета есть $\frac{1}{2}\eta_1(1-Q_B)+p_{d1}$; первое слагаемое — отсчет от однофотонного состояния на детекторе с квантовой эффективностью η_1. Сомножитель $1-Q_B$ отвечает за неидеальность балансировки плеч интерферометра. Второе слагаемое — темновой отсчет детектора с вероятностью p_{d1}. Темновой отсчет в детекторе *1* воспринимается как правильный отсчет от состояния 0_L.

Ошибочные отсчеты — это отсчеты, возникающие на детекторе *2*. Отсчет от реального фотона

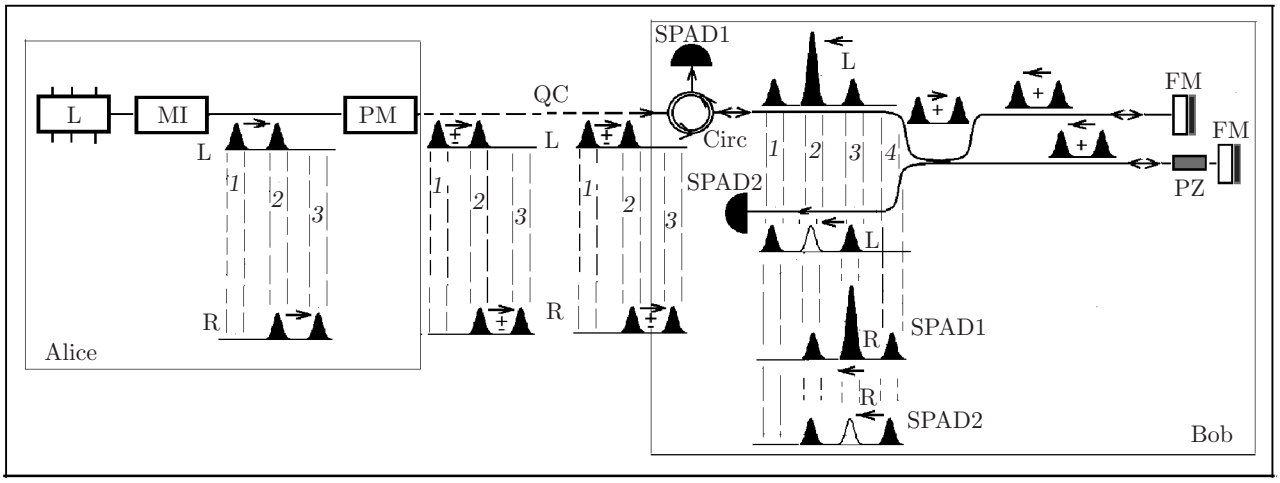

Рис. 1. Передающая сторона (Alice): L — лазер, работающий в CW-моде, MI — модулятор интенсивности, PM — фазовый модулятор. Весь оптический тракт на передающей станции выполнен на волокне, сохраняющем поляризацию. Приемная часть (Bob): весь оптический тракт выполнен на стандартном одномодовом SM-волокне. Circ — волоконный поляризационно независимый циркулятор. SPAD1,2 — однофотонные лавинные детекторы. FM — фарадеевское зеркало. PZ — управляемый пьезоэлемент для выравнивания разности хода в верхнем и нижнем плечах интерферометра. QC — линия связи на основе SM-волокна. Стрелками показана эволюция состояний

имеет место из-за неидеальной балансировки интерферометра и происходит с вероятностью $\frac{1}{2}\eta_2 Q_B + p_{d1}$. При идеальной балансировке ($Q_B = 0$) ошибочный отсчет в детекторе *2* от реального фотона отсутствует. Ошибочный отсчет возникает только из-за темновых шумов детектора *2* и имеет место с вероятностью p_{d2}.

Рассмотрим теперь преобразование состояния $|3\rangle_B$. Находим для преобразования контрольного состояния $|3\rangle_B$

$$\begin{pmatrix} \frac{1}{2}a_4^\dagger \\ \frac{1}{2}a_4^\dagger \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi}\delta_\rightarrow \end{pmatrix} \times \\ \times \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} a_3^\dagger \\ 0 \end{pmatrix}. \quad (69)$$

Вероятность детектирования контрольного состояния во временном окне *4* (см. рис. 1) на обоих детекторах имеет вид

$$|3_u\rangle_B \to \frac{1}{4}\eta_1 + p_{d1}, \\ |3_d\rangle_B \to \frac{1}{4}\eta_2 + p_{d2}, \quad (70)$$

где индексы u, d относятся к верхнему (up) и нижнему (down) детекторам. Выражения (68), (70) будут использованы ниже для вывода матриц плотности Алиса–Ева и Алиса–Боб, которые фигурируют в условной энтропии фон Неймана Алиса–Ева, входящей в формулы (52), (53) для длины секретного ключа.

10. СОВМЕСТНЫЕ МАТРИЦЫ ПЛОТНОСТИ АЛИСА–БОБ–ЕВА ПОСЛЕ ИЗМЕРЕНИЙ НА ПРИЕМНОЙ СТОРОНЕ

Найдем матрицы Алиса–Ева–Боб плотности после измерений Боба. Матрицы плотности после измерений отличаются от матриц плотности до измерений тем, что остаются только те посылки, где были отсчеты у Боба. Прежде чем выписать матрицы плотности, во избежание недоразумений необходимо сделать комментарий по поводу обозначений, используемых ниже.

Правильный отсчет, если было послано состояние $|0_L\rangle_B$, происходит с вероятностью (68). После акта регистрации формально это означает, что матрица плотности становится равной

$$|0_L\rangle_B \to |0\rangle\langle 0| \left[\frac{\eta_1}{2}(1 - Q_B) + p_{d1}\right] + \\ + |1\rangle\langle 1| \left[\frac{\eta_2}{2}Q_B + p_{d2}\right], \quad (71)$$

где $|0\rangle$ и $|1\rangle$ — состояние в информационном временном окне, которое получается после преобразований на интерферометре МЦ и которое отличается от исходного $|0_L\rangle_B$. Чтобы не вводить новых избыточных обозначений, ниже сохраним за обозначением состояния $|0\rangle$ старое обозначение $|0_L\rangle_B$, что не должно привести к путанице. Аналогично для других состояний. Формула (71) имеет простой смысл. Состояние $|0\rangle_B$ после преобразования на интерферометре и последующего детектирования лавинными детекторами с вероятностью $\frac{\eta_1}{2}(1-Q_B)+p_{d1}$ даст отсчет в детекторе *1*, который будет интерпретирован как правильный отсчет 0 — состояние $|0\rangle\langle 0|$. Состояние с вероятностью $\frac{\eta_2}{2}Q_B+p_{d2}$ даст отсчет в детекторе *2*, который будет интерпретирован как 1 из-за неидеальной балансировки интерферометра (слагаемое с Q_B) и темновых шумов (слагаемое p_{d2}).

Фактически формула (71) — это запись постулата фон Неймана–Людерса, которая дает матрицу плотности после измерений, при условии, что получен данный исход измерений — отсчет конкретного детектора. В нашем случае данная запись является скорее формальным техническим приемом, который нужен для подсчета условных энтропий фон Неймана. Тот факт, что фотон после отсчета детектора фактически пропадает, здесь не важен.

Заметим, что из-за малости $p_{d1,2}$ и $\eta_{1,2}$ слагаемыми $p_{d1,2}\eta_{1,2}$, отвечающими за парные отсчеты, при вычислении вероятностей (68) можно пренебречь.

Отметим, что следующие ниже матрицы плотности являются ненормированными, что для дальнейшего неважно, поскольку длина секретного ключа вычисляется в пересчете на зарегистрированные посылки.

Полная матрица плотности может быть записана как сумма компонент с разным числом фотонов:

$$\overline{\rho}_{XBE}(0_L)=\sum_{k=0}^{\infty}\overline{\rho}^{(k)}_{XBE}(0_L), \tag{72}$$

где k — фотонная часть матрицы плотности, $k=0$ отвечает вакуумной компоненте. Далее матрица плотности, отвечающая вакуумной компоненте состояний, имеет вид

$$\overline{\rho}^{(0)}_{XBE}(0_L)=e^{-2\mu}|0_L\rangle_{XX}\langle 0_L|\otimes\{p_{d1}|0_L\rangle_{BB}\langle 0_L|+$$
$$+\,p_{d2}|1_L\rangle_{BB}\langle 1_L|+p_{d1}|3u\rangle_{BB}\langle 3u|+p_{d2}|3d\rangle_{BB}\langle 3d|)\otimes$$
$$\otimes\,(|\mathrm{vac}\rangle_{EE}\langle\mathrm{vac}|\}\,. \tag{73}$$

Интерпретация достаточно проста. У Боба от вакуумной компоненты могут возникнуть отсчеты в информационном временном окне и контрольном окне только из-за темновых отсчетов в обоих детекторах. Однофотонная компонента матрицы плотности после измерений, если Алиса посылала 0_L, имеет вид

$$\overline{\rho}^{(1)}_{XBE}(0_L)=e^{-2\mu}\mu g_1 Y_1^E|0_L\rangle_{XX}\langle 0_L|\otimes$$
$$\otimes\left\{\left\{\left[\frac{\eta_1}{2}(1-Q_B)+p_{d1}\right]|0_L\rangle_{BB}\langle 0_L|\;+\;\left[\frac{\eta_2}{2}Q_B+p_{d2}\right]|1_L\rangle_{BB}\langle 1_L|\right\}\otimes|\Phi_0^L\rangle_{EE}\langle\Phi_0^L|+\right.$$
$$+\left\{\left[\frac{\eta_2}{2}(1-Q_B)+p_{d2}\right]|1_L\rangle_{BB}\langle 1_L|\;+\;\left[\frac{\eta_1}{2}Q_B+p_{d1}\right]|0_L\rangle_{BB}\langle 0_L|\right\}\otimes|\Omega_0^L\rangle_{EE}\langle\Omega_0^L|+$$
$$\left.+\left\{\left[\frac{\eta_1}{4}+p_{d1}\right]|3_c^u\rangle_{BB}\langle 3_c^u|+\left[\frac{\eta_2}{4}+p_{d2}\right]|3_c^d\rangle_{BB}\langle 3_c^d|\right\}\otimes|\Lambda_0^L\rangle_{EE}\langle\Lambda_0^L|\right\}. \tag{74}$$

Интерпретируем данную компоненту. Рассмотрим вторую строку формулы (74). До измерений Боба из линии связи поступало состояние $|0_L\rangle_{BB}\langle 0_L|$, в распоряжении Евы было состояние $|\Phi_0^L\rangle_{EE}\langle\Phi_0^L|$. После измерений этой компоненты поля у Боба с вероятностью $\frac{\eta_1}{2}(1-Q_B)+p_{d1}$ будет зарегистрирован правильный отсчет детектором *1*, т. е. будет зарегистрирован 0. Ошибочный отсчет будет зарегистрирован детектором *2* с вероятностью $\frac{\eta_2}{2}Q_B+p_{d2}$.

Аналогичным образом интерпретируется третья строка формулы (74). До измерений Боба на приемную станцию поступало состояние $|1_L\rangle_{BB}\langle 1_L|$ вместо неискаженного состояния Алисы $|0_L\rangle_{BB}\langle 0_L|$. Ева при этом «видит» состояние $|\Omega_0^L\rangle_{EE}\langle\Omega_0^L|$. Неправильное состояние $|1_L\rangle_{BB}\langle 1_L|$ может дать как правильный отсчет в детекторе *1* с вероятностью $\frac{\eta_1}{2}Q_B+p_{d1}$ из-за неидеальной балансировки интерферометра и темновых шумов детектора *1*. При идеальной балансировке интерферометра ($Q_B=0$) случайные, но правильные отсчеты детектора *1* могут быть в окне строба с вероятностью p_{d1} из-за темновых шумов. Ева при этом все равно «видит» состояние $|\Omega_0^L\rangle_{EE}\langle\Omega_0^L|$.

Четвертая строка формулы (74) относится к следующей ситуации. В результате унитарной атаки (см. формулы (25)) на состояние 0_L возникает ис-

каженное состояние, которое содержит компоненту $|3\rangle_B$ — однофотонное состояние, локализованное в окне *3*. Данное состояние после преобразований на интерферометре (см. формулы (65)–(70)) приводит к отсчетам во временном окне *4* (см. рис. 1). Отсчет во временно́м окне *4* на детекторе *1* и детекторе *2* происходит с вероятностями $\eta_1/4+p_{d1}$ и $\eta_2/4+p_{d2}$. В распоряжении Евы при этом будет состояние $|\Lambda_0^L\rangle_{EE}\langle\Lambda_0^L|$.

При обнаружении многофотонной компоненты Ева посылает к Бобу часть неискаженного многофотонного квантового состояния. Для многофотонной компоненты матрицы плотности, если Алисой был послан 0_L, матрица плотности имеет вид

$$\rho^{(k)}_{XBE}(1_L)=e^{-2\mu}\frac{g_k}{k!}Y_k^E|0_L\rangle_{XX}\langle 0_L|\otimes \\ \otimes\left\{\left[\eta_1^{(k)}(1-Q_B^{(k)})+p_{d1}\right]|0_L\rangle_{BB}\langle 0_L|+\left[\eta_2^{(k)}Q_B^{(k)}+p_{d2}\right]|1_L\rangle_{BB}\langle 1_L|+\right. \\ \left.+\left[\eta_1^{(k)}(c)+p_{d1}\right]|3^u\rangle_{BB}\langle 3^u|+\left[\eta_2^{(k)}(c)+p_{d2}\right]|3^d\rangle_{BB}\langle 3^d|\right\}\otimes|0_L^{(k)}\rangle_{EE}\langle 0_L^{(k)}|. \quad (75)$$

Интерпретация формулы (75) следующая. Вторая строка (75) показывает, что неискаженное многофотонное состояние, которое поступает на приемную станцию, может дать ошибочные отсчеты из-за неидеальной балансировки интерферометра и темновых шумов. Например, с вероятностью $\eta_1^{(k)}(1-Q_B^{(k)})+p_{d1}$ будет правильный отсчет в детекторе *1*, где, в отличие от однофотонной компоненты, множители включены в $\eta_i^{(k)}$, $i=1,2$. Здесь $\eta_1^{(k)}$ — квантовая эффективность детектора для детектирования многофотонной компоненты, которая, вообще говоря, отличается от квантовой эффективности для детектирования однофотонной компоненты η_1. Явный вид $\eta_1^{(k)}$ не потребуется. Далее $Q_B^{(k)}$ — ошибка детектирования многофотонной компоненты за счет неидеальной балансировки интерферометра, ее явный вид также не потребуется.

Многофотонная неискаженная компонента не имеет составляющих в контрольном временном окне (см. формулы (73), (78)), поскольку, в отличие от однофотонной компоненты, Ева не производит искажения многофотонных компонент состояния, а просто уменьшает число фотонов в этих компонентах за счет отвода части фотонов к себе в квантовую память после неразрушающих измерений числа фотонов. Отсчеты в контрольном окне имеют место из-за темновых шумов и других неидеальностей аппаратуры Боба с вероятностью $\eta_1^{(k)}(c)+p_{d1}$ в детекторе *1*, и с вероятностью $\eta_2^{(k)}(c)+p_{d2}$ в детекторе *2*. Явный вид квантовых эффективностей (отметим, что они могут отличаться от рассмотренных выше) не потребуется (см. ниже).

Выражения для остальных компонент матриц плотности, когда посылалось состояние 1_L, имеют следующий вид (интерпретация аналогична приведенной выше). Для вакуумной компоненты находим

$$\overline{\rho}^{(1)}_{XBE}(1_L)=e^{-2\mu}|1_L\rangle_{XX}\langle 1_L|\otimes(p_{d2}|1_L\rangle_{BB}\langle 1_L|+ \\ +p_d|0_L\rangle_{BB}\langle 0_L|+p_{d1}|3u\rangle_{BB}\langle 3u|+p_{d2}|3d\rangle_{BB}\langle 3d|)\otimes \\ \otimes(|\mathrm{vac}\rangle_{EE}\langle\mathrm{vac}|). \quad (76)$$

Для однофотонной компоненты состояний получаем

$$\overline{\rho}^{(1)}_{XBE}(1_L)=e^{-2\mu}\mu g_1 Y_1^E|1_L\rangle_{XX}\langle 1_L|\otimes \\ \otimes\left\{\left\{\left[\frac{\eta_2}{2}(1-Q_B)+p_{d2}\right]|1_L\rangle_{BB}\langle 1_L|+\right.\right. \\ \left.\left.+\left[\frac{\eta_1}{2}Q_B+p_{d1}\right]|0_L\rangle_{BB}\langle 0_L|\right\}\otimes|\Phi_1^L\rangle_{EE}\langle\Phi_1^L|+\right. \\ +\left\{\left[\frac{\eta_1}{2}(1-Q_B)+p_{d1}\right]|0_L\rangle_{BB}\langle 0_L|+\right. \\ \left.\left.+\left[\frac{\eta_2}{2}Q_B+p_{d2}\right]|1_L\rangle_{BB}\langle 1_L|\right\}\otimes|\Omega_0^L\rangle_{EE}\langle\Omega_0^L|+\right. \\ \left.+\left\{\left[\frac{\eta_1}{4}+p_{d1}\right]|3_c^u\rangle_{BB}\langle 3_c^u|+\left[\frac{\eta_2}{4}+p_{d2}\right]|3_c^d\rangle_{BB}\langle 3_c^d|\right\}\otimes\right. \\ \left.\otimes|\Lambda_1^L\rangle_{EE}\langle\Lambda_1^L|\right\}. \quad (77)$$

Соответственно, для многофотонных компонент состояний имеем

$$\overline{\rho}^{(k)}_{XBE}(1_L)=e^{-2\mu}\frac{g_k}{k!}Y_k^E|1_L\rangle_{XX}\langle 1_L|\otimes \\ \otimes\left\{\left[\eta_2^{(k)}(1-Q_B^{(k)})+p_{d2}\right]|1_L\rangle_{BB}\langle 1_L|+\right. \\ \left.+\left[\eta_1^{(k)}Q_B^{(k)}+p_{d1}\right]|0_L\rangle_{BB}\langle 0_L|+\right. \\ \left.+\left[\eta_1^{(k)}(c)+p_{d1}\right]|3^u\rangle_{BB}\langle 3^u|+\left[\eta_2^{(k)}(c)+p_{d2}\right]\times\right. \\ \left.\times|3^d\rangle_{BB}\langle 3^d|\right\}\otimes|1_L^{(k)}\rangle_{EE}\langle 1_L^{(k)}|. \quad (78)$$

Как видно из приведенного выше рассмотрения, матрицы плотности после атаки Евы до и после измерений у Боба существенно различаются.

10.1. Частичные матрицы плотности Евы после измерений на приемной стороне

Используем результаты предыдущего раздела для вычисления матриц плотности Алиса–Ева, через которые вычисляется утечка информации к подслушивателю. Вычисляя частичный след в (73), (74), получаем

$$\overline{\rho}_{XE}^{(0)}(0_L) = e^{-2\mu}|0_L\rangle_{X\,X}\langle 0_L| \otimes \{2p_{d1}+2p_{d2}\} \otimes \otimes |\mathrm{vac}\rangle_{E\,E}\langle \mathrm{vac}|. \quad (79)$$

Соответствующая однофотонная компонента для состояния 0_L имеет вид

$$\begin{aligned}\overline{\rho}_{XE}^{(1)}(0_L) = e^{-2\mu}\mu g_1 Y_1^E|0_L\rangle_{X\,X}\langle 0_L| \otimes \\ \otimes \left\{ \left[Y_1^L(0,0)+Y_1^L(0,1)\right]|\Phi_0^L\rangle_{E\,E}\langle\Phi_0^L| + \right. \\ + \left[Y_1^L(1,1)+Y_1^L(1,0)\right]|\Omega_0^L\rangle_{E\,E}\langle\Omega_0^L| + \\ \left. + \left[Y_1^L(3,u)+Y_1^L(3,d)\right]|\Lambda_0^L\rangle_{E\,E}\langle\Lambda_0^L|\right\}, \quad (80)\end{aligned}$$

где для краткости введены обозначения

$$\begin{aligned} Y_1^L(0,0) &= \left[\frac{\eta_1}{2}(1-Q_B)+p_{d1}\right], \\ Y_L^1(0,1) &= \left[\frac{\eta_2}{2}Q_B+p_{d2}\right], \end{aligned} \quad (81)$$

$$\begin{aligned} Y_1^L(1,1) &= \left[\frac{\eta_2}{2}(1-Q_B)+p_{d2}\right], \\ Y_L^1(1,0) &= \left[\frac{\eta_1}{2}Q_B+p_{d1}\right], \end{aligned} \quad (82)$$

$$Y_1^L(3,u) = \left[\frac{\eta_1}{4}+p_{d1}\right], \quad Y_1^L(3,d) = \left[\frac{\eta_2}{4}+p_{d2}\right]. \quad (83)$$

Для многофотонных компонент частичная матрица плотности Алиса–Ева имеет вид

$$\begin{aligned}\overline{\rho}_{XE}^{(k)}(0_L) = e^{-2\mu}\frac{g_k}{k!}Y_k^E|0_L\rangle_{X\,X}\langle 0_L| \otimes \\ \otimes \left\{Y_k^L(0,0)+Y_k^L(1,0)+Y_k^L(3,u)+Y_k^L(3,d)\right\} \otimes \\ \otimes |0_L^{(k)}\rangle_{E\,E}\langle 0_L^{(k)}|, \quad (84)\end{aligned}$$

$$\begin{aligned} Y_k^L(0,0) &= \eta_1^{(k)}(1-Q_B^{(k)})+p_{d1}, \\ Y_k^L(0,1) &= \eta_2^{(k)}Q_B^{(k)}+p_{d2}, \end{aligned} \quad (85)$$

$$\begin{aligned} Y_k^L(1,1) &= \eta_2^{(k)}(1-Q_B^{(k)})+p_{d2}, \\ Y_k^L(1,0) &= \eta_1^{(k)}Q_B^{(k)}+p_{d1}, \end{aligned} \quad (86)$$

$$\begin{aligned} Y_k^L(3,u) &= \eta_1^{(k)}(c)+p_{d1}, \\ Y_k^L(3,d) &= \eta_2^{(k)}(c)+p_{d2}. \end{aligned} \quad (87)$$

Частичные матрицы плотности для состояния 1_L записываются как

$$\overline{\rho}_{XE}^{(1)}(0_L) = e^{-2\mu}|1_L\rangle_{X\,X}\langle 1_L| \otimes \{2p_{d1}+2p_{d2}\} \otimes \otimes |\mathrm{vac}\rangle_{E\,E}\langle \mathrm{vac}|, \quad (88)$$

однофотонная компонента —

$$\begin{aligned}\overline{\rho}_{XE}^{(1)}(1_L) = e^{-2\mu}\mu g_1 Y_1^E|1_L\rangle_{X\,X}\langle 1_L| \otimes \\ \otimes \left\{ \left[Y_1^L(1,1)+Y_1^L(1,0)\right]|\Phi_1^L\rangle_{E\,E}\langle\Phi_1^L| + \right. \\ + \left[Y_1^L(0,0)+Y_1^L(0,1)\right]|\Omega_1^L\rangle_{E\,E}\langle\Omega_1^L| + \\ \left. + \left[Y_1^L(3,u)+Y_1^L(3,d)\right]|\Lambda_1^L\rangle_{E\,E}\langle\Lambda_1^L|\right\}, \quad (89)\end{aligned}$$

и многофотонные компоненты —

$$\begin{aligned}\rho_{XBE}^{(k)}(1_L) = e^{-2\mu}\frac{g_k}{k!}Y_k^E|1_L\rangle_{X\,X}\langle 1_L| \otimes \\ \otimes \left\{Y_k^L(1,1)+Y_k^L(0,1)+Y_k^L(3,u)+Y_k^L(3,d)\right\} \otimes \\ \otimes |1_L^{(k)}\rangle_{E\,E}\langle 1_L^{(k)}|. \quad (90)\end{aligned}$$

10.2. Частичные матрицы плотности Боба после измерений

Найдем частичные матрицы плотности Боба после измерений на приемной стороне. Вычисляя частичный след по пространству состояний Евы в (73), (74) для состояний 0_L, получаем

$$\overline{\rho}_{X\,B}(0_L) = \sum_{k=0}^{\infty}\overline{\rho}_{X\,B}^{(k)}(0_L), \quad (91)$$

где k — фотонная часть матрицы плотности, $k=0$ отвечает вакуумной компоненте. Далее для вакуумной компоненты получаем

$$\begin{aligned}\overline{\rho}_{X\,B}^{(0)}(0_L) = e^{-2\mu}|0_L\rangle_{X\,X}\langle 0_L| \otimes \{p_{d1}|0_L\rangle_{B\,B}\langle 0_L| + \\ + p_{d2}|1_L\rangle_{B\,B}\langle 1_L| + p_{d1}|3u\rangle_{B\,B}\langle 3u| + \\ + p_{d2}|3d\rangle_{B\,B}\langle 3d|\}, \quad (92)\end{aligned}$$

соответственно, однофотонная компонента для состояния 0_L имеет вид

$$\begin{aligned}\overline{\rho}_{X\,B}^{(1)}(0_L) = e^{-2\mu}\mu g_1 Y_1^E|0_L\rangle_{X\,X}\langle 0_L| \otimes \\ \otimes \left\{ [Y_1^L(0,0)_E\langle\Phi_0^L|\Phi_0^L\rangle_E + \right. \\ + Y_1^L(1,0)_E\langle\Omega_0^L|\Omega_0^L\rangle_E]|0_L\rangle_{B\,B}\langle 0_L| + \\ + [Y_1^L(0,1)_E\langle\Phi_0^L|\Phi_0^L\rangle_E + \\ + Y_1^L(1,1)_E\langle\Omega_0^L|\Omega_0^L\rangle_E]|1_L\rangle_{B\,B}\langle 1_L| + \\ + [Y_1^L(3,u)|3_c^u\rangle_{B\,B}\langle 3_c^u| + \\ \left. + Y_1^L(3,d)|3_c^d\rangle_{B\,B}\langle 3_c^d|]_E\langle\Lambda_0^L|\Lambda_0^L\rangle_E\right\}. \quad (93)\end{aligned}$$

Многофотонные компоненты матрицы плотности для состояния 0_L записываются как

$$\begin{aligned}\rho_{X\,B}^{(k)}(0_L) = e^{-2\mu}g_k Y_k^E|0_L\rangle_{X\,X}\langle 0_L| \otimes \\ \otimes \left\{Y_k^L(0,0)|0_L\rangle_{B\,B}\langle 0_L| + Y_k^L(0,1)|1_L\rangle_{B\,B}\langle 1_L| + \right. \\ \left. + Y_k^L(3u)|3^u\rangle_{B\,B}\langle 3^u| + Y_k^L(3d)|3^d\rangle_{B\,B}\langle 3^d|\right\}. \quad (94)\end{aligned}$$

Аналогичные выражения получаются для состояния 1_L:

$$\overline{\rho}_{XB}(1_L) = \sum_{k=0}^{\infty} \overline{\rho}_{XB}^{(k)}(1_L), \tag{95}$$

где k — фотонная часть матрицы плотности, $k = 0$ отвечает вакуумной компоненте. Далее

$$\begin{aligned}\overline{\rho}_{XB}^{(0)}(1_L) = e^{-2\mu}|1_L\rangle_{X\,X}\langle 1_L| \otimes \\ \otimes \{p_{d1}|0_L\rangle_{B\,B}\langle 0_L| + p_{d2}|1_L\rangle_{B\,B}\langle 1_L| + \\ + p_{d1}|3u\rangle_{B\,B}\langle 3u| + p_{d2}|3d\rangle_{B\,B}\langle 3d|\}\,.\end{aligned} \tag{96}$$

Матрица плотности однофотонной компоненты для состояния 1_L имеет вид

$$\begin{aligned}\overline{\rho}_{XB}^{(1)}(1_L) = e^{-2\mu}\mu g_1 Y_1^E|1_L\rangle_{X\,X}\langle 1_L| \otimes \\ \otimes \big\{[Y_1^L(1,1)_E\langle\Phi_1^L|\Phi_1^L\rangle_E + \\ + Y_1^L(0,1)_E\langle\Omega_1^L|\Omega_1^L\rangle_E]|1_L\rangle_{B\,B}\langle 1_L| + \\ + [Y_1^L(1,0)_E\langle\Phi_1^L|\Phi_1^L\rangle_E + \\ + Y_1^L(0,0)_E\langle\Omega_1^L|\Omega_1^L\rangle_E]|0_L\rangle_{B\,B}\langle 0_L| + \\ + [Y_1^L(3,u)|3_c^u\rangle_{B\,B}\langle 3_c^u| + \\ + Y_1^L(3,d)|3_c^d\rangle_{B\,B}\langle 3_c^d|]_E\langle\Lambda_1^L|\Lambda_1^L\rangle_E\big\}\,.\end{aligned} \tag{97}$$

Наконец, для многофотонных компонент для состояния 1_L имеем

$$\begin{aligned}\rho_{XB}^{(k)}(1_L) = e^{-2\mu}g_k Y_k^E|1_L\rangle_{X\,X}\langle 1_L| \otimes \\ \otimes \big\{Y_k^L(1,1)|1_L\rangle_{B\,B}\langle 1_L| + Y_k^L(1,0)|0_L\rangle_{B\,B}\langle 0_L| + \\ + Y_k^L(3u)|3^u\rangle_{B\,B}\langle 3^u| + Y_k^L(3d)|3^d\rangle_{B\,B}\langle 3^d|\big\}\,.\end{aligned} \tag{98}$$

11. DECOY STATE-МЕТОД ДЛЯ ФАЗОВО-ВРЕМЕННОГО КОДИРОВАНИЯ, ОДИНАКОВЫЕ ДЕТЕКТОРЫ

В этом разделе вычислим вероятности отсчетов в информационных временных окнах, а также вероятность отсчетов в контрольных окнах, используя матрицы плотности, рассмотренные в предыдущих разделах. Затем получим выражения для утечки информации к подслушивателю и количество информации, расходуемое на коррекцию ошибок в первичных ключах.

11.1. Оценка параметров

Число отсчетов в информационных временны́х окнах определяется следом матрицы плотности Боба после измерений. Полная доля как отношение посланных посылок в совпадающих базисах к числу зарегистрированных отсчетов на приемной стороне на обоих детекторах есть

$$Q_\mu = \frac{1}{2}\mathrm{Tr}_{X\,B}\left\{\overline{\rho}_{X\,B}(0_L) + \overline{\rho}_{X\,B}(1_L)\right\}. \tag{99}$$

Более детально полная доля отсчетов в базисе L (99) в информационном временном окне с учетом (91)–(98) равна

$$\begin{aligned}Q_\mu = \\ = e^{-2\mu}\left\{2(p_{d1}+p_{d2}) + \mu g_1 Y_1^E\left(\frac{\eta_1+\eta_2}{4} + p_{d1} + p_{d2}\right)\times\right. \\ \left.\times\,(1-q_1) + \sum_{k=2}^{\infty}\frac{\mu^k}{k!}g_k\overline{Y}_k^E\right\},\end{aligned} \tag{100}$$

$$\overline{Y}_k^E = \sum_{i,j=0,1} Y_k^E(i,j). \tag{101}$$

Чтобы не загромождать дальнейшие выкладки, считаем, что балансировка интерферометра на приемной стороне идеальна, т. е. в формулах (68), (70) положено $Q_B = 0$. Далее, используя формулы (91)–(98), находим долю отсчетов в контрольном временно́м окне:

$$\begin{aligned}\Delta_\mu = e^{-2\mu}\left\{2(p_{d1}+p_{d2}) + \right. \\ + \mu g_1 Y_1^E\left(\frac{\eta_1+\eta_2}{4} + p_{d1} + p_{d2}\right)q_1 + \\ \left. + \sum_{k=2}^{\infty}\frac{\mu^k}{k!}\overline{Y}_k(3)\right\},\end{aligned} \tag{102}$$

$$\overline{Y}_k(3) = Y_k^L(3u) + Y_k^L(3d). \tag{103}$$

Для дальнейшего найдем вероятность ошибки. Полная доля ошибочных отсчетов с учетом (91)–(98) имеет вид

$$\begin{aligned}\mathrm{Err}_\mu = e^{-2\mu}\left\{\frac{p_{d1}+p_{d2}}{2} + \frac{1}{2}\mu g_1 Y_1^E(1-q_1)\times\right. \\ \times\left[\left(\frac{\eta_1+\eta_2}{2}Q_B^1 + p_{d1} + p_{d2}\right)(1-Q_1) + \right. \\ \left.\left. + \left(\frac{\eta_1+\eta_2}{2}(1-Q_B^1) + p_{d1} + p_{d2}\right)Q_1\right] + \right. \\ \left. + \sum_{k=2}^{\infty}\frac{\mu^k}{k!}\overline{Y}_k Q_k\right\}.\end{aligned} \tag{104}$$

Далее введем для удобства обозначения

$$\begin{gathered}\overline{Q}_\mu = e^{2\mu}Q_\mu, \quad \overline{\Delta}_\mu = e^{2\mu}\Delta_\mu, \\ \overline{\mathrm{Err}}_\mu = e^{2\mu}\mathrm{Err}_\mu.\end{gathered} \tag{105}$$

Decoy state-метод состоит в том, что посылаются состояния с разным средним числом фотонов. Возможны различные варианты данного метода, точнее, разное число состояний ловушек — когерентных состояний с разным средним числом фотонов. Будем использовать три типа состояний: состояния со средним числом μ, ν и $\nu = 0$. В асимптотическом пределе длинных последовательностей можно найти вероятности отсчетов в информационных окнах (100) и в контрольных временны́х окнах (104), вероятность ошибки (102). Группировка посылок с разным средним числом фотонов в состоянии позволяет оценить долю однофотонной компоненты в посылках со средним числом фотонов μ, а также параметры q_1 и Q_1, через которые выражается длина секретного ключа. Использование посылок с тремя разными значениями среднего числа фотонов μ, $\nu < \mu$ и $\nu = 0$ позволяют оценить параметры атаки Евы. Имеют место следующие неравенства, которые следуют непосредственно из формул (100), (102), (104):

$$(1-q_1)\overline{Y}_1 \geq \frac{\overline{Q}_\nu - \overline{Q}_{\nu=0} - \dfrac{\nu^2}{\mu^2}\left(\overline{Q}_\mu - \overline{p}_d\right)}{\nu - \dfrac{\nu^2}{\mu}}, \qquad q_1\overline{Y}_1 \leq \frac{2(\overline{\Delta}_\nu - \overline{\Delta}_{\nu=0})}{\nu}, \tag{106}$$

где $\overline{Q}_\nu$ и $\overline{Q}_{\nu=0}$ — вероятности отсчетов в информационном временно́м окне, когда посылались состояния «ловушки» со средним числом фотонов ν и $\nu = 0$; $\overline{\Delta}_\nu$ и $\overline{\Delta}_{\nu=0}$ — вероятности отсчетов в контрольном временно́м окне. Здесь введены обозначения

$$\overline{Y}_1 = 2g_1 Y_1^E\left(\frac{\eta_1+\eta_2}{4} + p_{d1} + p_{d2}\right), \qquad \overline{p}_d = p_{d1} + p_{d2}, \tag{107}$$

где (107) есть наблюдаемая доля однофотонных посылок, и

$$\chi = \frac{q_1}{1-q_1} \leq \frac{2(\overline{\Delta}_\nu - \overline{\Delta}_{\nu=0})}{\nu} \times \left(\frac{\overline{Q}_\nu - \overline{Q}_{\nu=0} - \dfrac{\nu^2}{\mu^2}(\overline{Q}_\nu - \overline{p}_d)}{\nu - \dfrac{\nu^2}{\mu}}\right)^{-1}. \tag{108}$$

Вероятность наблюдаемой ошибки в информационном временном окне определяется по посылкам, в которых посылались информационные состояния со средним числом фотонов μ. Ошибка (102) определяет утечку информации к подслушивателю при коррекции ошибок в сырых ключах, находим

$$Q_{err}(\mu) = \frac{\overline{\mathrm{Err}}_\mu}{\overline{Q}_\mu}. \tag{109}$$

Decoy state-метод позволяет получить точные значения параметров, имеем

$$\left.\frac{d\overline{Q}_\mu}{d\mu}\right|_{\mu=0} = \overline{Y}_1(1-q_1), \quad 2\left.\frac{d\overline{\Delta}_\mu}{d\mu}\right|_{\mu=0} = \overline{Y}_1 q_1, \qquad \left(2\left.\frac{d\overline{\Delta}_\mu}{d\mu}\right|_{\mu=0}\right)\left(\left.\frac{d\overline{Q}_\mu}{d\mu}\right|_{\mu=0}\right)^{-1} = \chi = \frac{q_1}{1-q_1}. \tag{110}$$

Однако такое определение требует посылки состояний «ловушек» с очень малым средним числом фотонов, в пределе стремящемся к нулю, что в реальной ситуации требует длинных последовательностей, поэтому практически неприменимо, и приходится использовать формулы (100)–(108).

11.2. Условная энтропия подслушивателя

В этом разделе вычислим условные энтропии фон Неймана, которые дают величину утечки информации к подслушивателю. Рассмотрим сначала ситуацию, когда параметры лавинных однофотонных детекторов — квантовая эффективность и вероятность темновых шумов — являются одинаковыми, $\eta_1 = \eta_2 = \eta$, $p_{d1} = p_{d2} = p_d$. Эта ситуация имеет место при полной симметрии по индексам детекторов, что заметно упрощает последующие выкладки при вычислении условной энтропии фон Неймана.

Отметим, что вероятность регистрации 0 и 1 по всем базисам в этом случае также оказывается одинаковой. Если детекторы различны, то число зарегистрированных 0 и 1 внутри одного базиса будет разным. Результат интерпретируется как 0 при отсчете детектора *1* и как 1 при отсчете детектора *2*.

В другом базисе, наоборот, значению бита 0 отвечает отсчет детектора *2*, а отсчет детектора *1* отвечает значению бита 1 у Боба. Суммарное число 0 и 1 у Боба в обоих базисах будет одинаковым даже при разных квантовых эффективностях и вероятностях темновых шумов обоих детекторов. С учетом (79)–(90) получаем

$$H\left(\overline{\rho}_{XE}|\overline{\rho}_E\right) = H\left(\overline{\rho}^L_{XE}|\overline{\rho}^L_E\right) + H\left(\overline{\rho}^R_{XE}|\overline{\rho}^R_E\right), \qquad H\left(\overline{\rho}^{L,R}_{XE}|\overline{\rho}^{L,R}_E\right) = H\left(\overline{\rho}^{L,R}_{XE}\right) - H\left(\overline{\rho}^{L,R}_E\right), \tag{111}$$

где

$$\overline{\rho}_{XE}^{L,R} = \frac{1}{2}\left(\overline{\rho}_{XE}^{L,R}(0_{L,R}) + \overline{\rho}_{XE}^{L,R}(1_{L,R})\right). \qquad (112)$$

Находим для условной энтропии фон Неймана

$$\begin{aligned} H(\overline{\rho}_{XE}) &= e^{-2\mu}\mu\overline{Y}_1(1-q_1)\,(1+h(Q_1))\,, \\ H(\overline{\rho}_{E}) &= e^{-2\mu}\mu\overline{Y}_1(1-q_1)\,(h(Q_1)+h(\chi))\,, \end{aligned} \qquad (113)$$

$$H(\overline{\rho}_{XE}|\overline{\rho}_{E}) = e^{-2\mu}\mu\overline{Y}_1(1-q_1)\,(1-h(\chi))\,, \qquad (114)$$

$$\begin{aligned} h(Q_1) &= -Q_1\log_2(Q_1) - (1-Q_1)\log_2(1-Q_1), \\ \chi &= \frac{q_1}{1-q_1}. \end{aligned} \qquad (115)$$

Неформально условная энтропия фон Неймана равна нехватке информации Евы о передаваемом бите ключа в пересчете на одну зарегистрированную посылку на приемной стороне. Поскольку многофотонные компоненты состояний после раскрытия базисов дают Еве достоверную информацию о передаваемом бите ключа (см. формулы (75), (78)), нехватка информации Евы определяется только долей однофотонной компоненты.

Отметим, что в формулах (113)–(115) для условной энтропии фон Неймана опущен вклад от темновых шумов, который имеет следующий порядок малости по сравнению с остальными членами.

11.3. Длина секретного ключа, оценка предельной длины линии связи, одинаковые детекторы

Для длины секретного ключа в пересчете на одну позицию с учетом (111)–(115) получаем

$$\lim_{n\to\infty}\frac{\ell}{n} = \frac{e^{-2\mu}\mu\overline{Y}_1(1-q_1)}{\overline{Q}_\mu}(1-h(\chi)) - \\ - \operatorname{leak}\left(\frac{\mathrm{Err}_\mu}{Q_\mu}\right). \qquad (116)$$

Оценим длину линии связи, до которой можно передавать секретные ключи. В отсутствие подслушивателя ошибки в информационных и контрольных временных окнах связаны только с темновыми шумами. Для оценки предельной длины линии считаем балансировку интерферометра идеальной, тогда $Q_B = 0$ (см. формулы (68), (70)). Без подслушивателя однофотонные посылки не блокируются, т. е. $Y_1^E = 1$. Другие параметры атаки, которые задаются Евой, равны $Q_1 = 0$ и $q_1 = 0$, соответственно в (115) $\chi = 0$. Вероятность регистрации в информационных временных окнах становится равной

$$Q_\mu \approx 2e^{-2\mu}\left\{p_d + \eta\mu\right\}. \qquad (117)$$

Вероятность (ненормированная) ошибочных отсчетов при идеальной балансировке интерферометра $Q_B = 0$ и параметрах $Q_1 = 0$ и $q_1 = 0$ принимает вид

$$\mathrm{Err}_\mu \approx e^{-2\mu}p_d, \qquad (118)$$

где учтено, что $\mu p_d \ll 1$. Для нормированной вероятности ошибки с учетом (117) и (118) получаем

$$Q_{err}(\mu) \approx \frac{1}{2}\frac{p_d}{p_d+\mu\eta}. \qquad (119)$$

Принимая во внимание (117)–(119), окончательно для длины секретного ключа имеем

$$\lim_{n\to\infty}\frac{\ell}{n} = \\ = 2e^{-2\mu}\mu\frac{p_d+\eta}{\mu\eta+2p_d} - \operatorname{leak}\left(\frac{1}{2}\,\frac{p_d}{p_d+\mu\eta}\right). \qquad (120)$$

В шенноновском пределе информация leak, расходуемая на коррекцию ошибок, равна

$$\operatorname{leak}\left(\frac{1}{2}\,\frac{p_d}{p_d+\mu\eta}\right) = h\left(\frac{1}{2}\,\frac{p_d}{p_d+\mu\eta}\right). \qquad (121)$$

При использовании реальных кодов коррекции ошибок, например, наиболее эффективных LDPC-кодов, расход информации в битах на коррекцию ошибок оказывается несколько больше минимального теоретического предела (см. ниже).

Предельная длина линии для секретного распределения ключей получается следующим образом. Во всех формулах нужно заменить параметр μ (среднее число фотонов): $\mu \to \mu(L) = \mu 10^{-\xi L/10}$, где $\xi = 0.2$ дБ/км — коэффициент потерь в одномодовом волокне, L — длина линии связи. Критическая длина линии связи L_c определяется из условия обращения в нуль длины секретного ключа, с учетом (116) находим

$$\frac{2e^{-2\mu}\mu(\eta+p_d)}{\mu(L_c)\eta+p_d} = h\left(\frac{1}{2}\frac{p_d}{p_d+\mu(L_c)\eta}\right). \qquad (122)$$

Зависимости критической длины линии связи как функции параметров η, μ и p_d приведены на рис. 6, 7 (см. ниже).

12. DECOY STATE-МЕТОД ДЛЯ ФАЗОВО-ВРЕМЕННОГО КОДИРОВАНИЯ, РАЗНЫЕ ДЕТЕКТОРЫ

В этом разделе вычислим длину секретного ключа для случая различных параметров лавинных детекторов. Вклад в условную энтропию, которая есть

нехватка информации Евы о передаваемом ключе, дает только однофотонная компонента матриц плотности. Нормированные матрицы плотности для однофотонной компоненты в базисе L могут быть представлены в виде

$$\widehat{\rho}^{(1)}_{XE}(0_L) = |0_L\rangle_{EE}\langle 0_L| \otimes \\ \otimes \left(\kappa|\Phi^L_0\rangle_{EE}\langle\Phi^L_0| + (1-\kappa)|\Omega^L_0\rangle_{EE}\langle\Omega^L_0|\right), \quad (123)$$

$$\widehat{\rho}^{(1)}_{XE}(1_L) = |1_L\rangle_{EE}\langle 1_L| \otimes \\ \otimes \left((1-\kappa)|\Phi^L_1\rangle_{EE}\langle\Phi^L_1| + \kappa|\Omega^L_1\rangle_{EE}\langle\Omega^L_1|\right), \quad (124)$$

где введено обозначение

$$\kappa = \frac{Y^L_1(0,0) + Y^L_1(1,0)}{Y^L_1(0,0)+Y^L_1(1,0)+Y^L_1(1,1)+Y^L_1(0,1)}. \quad (125)$$

Аналогичные выражения получаются для матриц плотности в базисе R:

$$\widehat{\rho}^{(1)}_{XE}(0_R) = |0_R\rangle_{EE}\langle 0_R| \otimes \\ \otimes \left((1-\kappa)|\Phi^R_0\rangle_{EE}\langle\Phi^R_0| + \kappa|\Omega^R_0\rangle_{EE}\langle\Omega^R_0|\right), \quad (126)$$

$$\widehat{\rho}^{(1)}_{XE}(1_R) = |1_R\rangle_{EE}\langle 1_R| \otimes \\ \otimes \left(\kappa|\Phi^R_1\rangle_{EE}\langle\Phi^R_1| + (1-\kappa)|\Omega^R_1\rangle_{EE}\langle\Omega^R_1|\right). \quad (127)$$

Обратим внимание, что суммарная матрица плотности по всем базисам симметрична по 0 и 1 и не зависит от различных параметров детекторов, что принципиально для сохранения одинаковых суммарных вероятностей регистрации 0 и 1 в обоих базисах. Для матриц плотности в базисе L находим

$$\widehat{\rho}^{(1)}_{XE} = \frac{1}{2}\left(\widehat{\rho}^{(1)}_{XE}(0_L) + \widehat{\rho}^{(1)}_{XE}(1_L)\right), \quad (128)$$

$$\widehat{\rho}^{(1)}_{E} = \frac{1}{2}\left(\kappa|\Phi^L_0\rangle_{EE}\langle\Phi^L_0| + (1-\kappa)|\Phi^L_1\rangle_{EE}\langle\Phi^L_1| + \right. \\ \left. + (1-\kappa)|\Omega^L_0\rangle_{EE}\langle\Omega^L_0| + \kappa|\Omega^L_1\rangle_{EE}\langle\Omega^L_1|\right). \quad (129)$$

12.1. Условная энтропия подслушивателя

Воспользуемся полученными в предыдущем разделе матрицами плотности для вычисления условной энтропии фон Неймана. По определению для условной энтропии находим

$$H\left(\widehat{\rho}^{(1)}_{XE}|\widehat{\rho}^{(1)}_{E},\kappa\right) = H\left(\widehat{\rho}^{(1)}_{XE},\kappa\right) - H\left(\widehat{\rho}^{(1)}_{E},\kappa\right), \quad (130)$$

$$H(\widehat{\rho}^{(1)}_{XE},\kappa) = h(Q) + h(\kappa). \quad (131)$$

Прямое вычисление энтропии требует знания параметра неидеальности балансировки интерферометра, который может быть получен из измерения величины ошибки. Поэтому при вычислении энтропии удобно воспользоваться неравенствами, которые следуют из того факта, что максимум энтропии достигается на равновероятном распределении. Получаем

$$H\left(\widehat{\rho}^{(1)}_{XE},\kappa\right) \geq H\left(\widehat{\rho}^{(1)}_{XE},\min\{\kappa\}\right) = \\ = h(Q) + h(\min\{\kappa\}), \quad (132)$$

$$\min\{\kappa\} = \frac{\min\{\eta_{1,2}\} + \min\{p_{d1,2}\}}{\eta_1+\eta_2+p_{d1}+p_{d2}}. \quad (133)$$

Далее, с учетом сказанного имеем

$$H\left(\widehat{\rho}^{(1)}_{E},\kappa\right) \leq H\left(\widehat{\rho}^{(1)}_{XE},\kappa=\frac{1}{2}\right) = h(Q)+h(\chi). \quad (134)$$

В итоге для условной энтропии фон Неймана находим

$$H\left(\widehat{\rho}^{(1)}_{XE}|\widehat{\rho}^{(1)}_{E},\kappa\right) \leq H\left(\widehat{\rho}^{(1)}_{XE},\min\{\kappa\}\right) - \\ - H\left(\widehat{\rho}^{(1)}_{XE},\kappa=\frac{1}{2}\right) = h(\min\{\kappa\}) - h(\chi). \quad (135)$$

12.2. Длина секретного ключа, оценка предельной длины линии связи, разные детекторы

Для длины секретного ключа с учетом (130)–(135) получаем

$$\lim_{n\to\infty}\frac{\ell}{n} = \frac{e^{-2\mu}\mu\overline{Y}_1(1-q_1)}{\overline{Q}_\mu} \times \\ \times \left(h(\min\{\kappa\}) - h(\chi)\right) - \mathrm{leak}\left(\frac{\mathrm{Err}_\mu}{Q_\mu}\right), \quad (136)$$

где для вычисления q_1 и χ нужно воспользоваться формулами (100)–(108).

Для оценки критической длины линии, до которой гарантируется секретное распределение ключей, вместо (122) в шенноновском пределе получаем

$$\frac{2e^{-2\mu}\mu(\overline{\eta}+\overline{p}_d)}{\mu(L_c)\overline{\eta}+\overline{p}_d}h(\min\{\kappa\}) = \\ = h\left(\frac{1}{2}\frac{\overline{p}_d}{\overline{p}_d+\mu(L_c)\overline{\eta}}\right), \quad (137)$$

$$\overline{\eta} = \frac{\eta_1+\eta_2}{2}, \quad \overline{p}_d = \frac{p_{d1}+p_{d2}}{2}.$$

Пусть квантовая эффективность одного из детекторов отличается в три раза, т. е. $\eta_1/\eta_2 = 1/3$, при этом

$\kappa = 1/4$ и, как обычно, $p_{d1,2} \ll \eta_{1,2}$. В этом случае длина секретного ключа при нулевой длине линии связи оказывается приблизительно равной (см. формулы (136), (137)) $h(1/4) \approx 0.8$ бит в пересчете на посылку. Если бы квантовая эффективность детекторов была одинаковой, то длина секретного ключа была бы равна ≈ 1 бит. Как видно из данного примера, подсчет длины секретного ключа в условиях разных детекторов оказывается на 20 % меньше. Зависимости критической длины линии связи как функции параметров $\eta_{1,2}$, μ и $p_{d1,2}$ приведены на рис. 7 (см. ниже).

13. КОРРЕКЦИЯ ОШИБОК В ПЕРВИЧНЫХ КЛЮЧАХ

После передачи серии квантовых состояний, измерений на приемной стороне, Алиса и Боб имеют битовые строки длины n. Строка Алисы $x \in \mathcal{X} = \{0,1\}^n$, строка Боба $y \in \mathcal{Y} = \{0,1\}^n$, строка Боба содержит ошибки. Следующая стадия протокола — коррекция ошибок посредством обмена информацией между Алисой и Бобом через классический аутентичный канал связи. На данной стадии протокола Алиса и Боб находятся в ситуации бинарного классического канала связи с некоторой вероятностью ошибки. В асимптотическом пределе длинных последовательностей вероятность ошибки на стороне Боба равна $\varepsilon = \mathrm{Err}_\mu / Q_\mu$.

Для исправления ошибок обычно используются линейные коды коррекции ошибок. В асимптотическом пределе длинных последовательностей количество информации в битах в пересчете на одну посылку, которое требуется для исправления ошибок и которое выдается через открытый канал связи и доступно Еве, есть $\mathrm{leak}(\varepsilon)$. Финальная длина секретного ключа зависит от эффективности корректирующего кода. Чем меньшее количество информации через открытый классический канал связи, тем большая длина финального секретного ключа может быть получена. Минимально необходимое количество информации в пересчете на одну позицию, которое требуется для исправления ошибок в пределе длинных последовательностей, с вероятностью исправления сколь угодно близкой к единице, дается условной шенноновской энтропией $H(X|Y) = h(Q)$, которая зависит от вероятности ошибки в канале связи. Неформально говоря, шенноновский предел дает минимальную избыточность кода, при которой можно исправить ошибки. Однако шенноновская процедура коррекции ошибок является, скорее, теоремой существования, чем конструктивной процедурой, в том смысле, что является экспоненциально сложной по длине последовательности. Конструктивные коды коррекции ошибок имеют большую избыточность и требует раскрытия большего количества битов информации для исправления ошибок. На сегодняшний день наиболее эффективными в этом смысле являются коды коррекции ошибок с низкой плотностью проверок на четность (LDPC-коды), которые впервые были предложены Галлагером в 1962 г. [23, 24]. Данные коды, в отличие от ряда других кодов, требуют определенного объема компьютерных вычислений, поэтому более 30 лет после их открытия не были широко востребованы. Прогресс в использовании LDPC-кодов возник после работ [28, 29] (см. также [30]), где был предложен итерационный алгоритм с так называемым мягким декодированием.

Использование линейных кодов при передаче информации отличается от использования линейных кодов в квантовой криптографии при коррекции ошибок. При передаче информации через канал с шумом исходная информационная битовая строка длины $k = n - m$ дополняется контрольными символами — битовой строкой длины m. Для каждого линейного кода существует матрица — генератор кода G размером $(n-m) \times n$, такая что кодовые слова длиной n задаются умножением исходной битовой информационной строки на эту матрицу: $C = \{G\mathbf{a} \in \{0,1\}^{n-m}\}$. Альтернативным описанием линейного кода является описание при помощи проверочной матрицы H размером $m \times n$, такой что $GH^T = 0$. Из этого определения следует, что неискаженные кодовые слова — битовые строки $\mathbf{y}$ длиной n удовлетворяют проверкам на четность:

$$\mathbf{y} \in C \Leftrightarrow \mathbf{y}H^T = 0. \tag{138}$$

Поскольку H — битовая матрица, данное условие можно трактовать как то, что m различных комбинаций битов из $\mathbf{x}$ должны удовлетворять проверкам на четность. Величина $\mathbf{z} = \mathbf{y}H^T \neq 0$ называется синдромом, синдром на всех кодовых словах равен нулю, $\mathbf{z} \neq 0$. При передаче информации на приемной стороне декодер проверяет условие — вычисляет синдром, если синдром отличен от нуля, то декодер по тому или иному алгоритму исправляет ошибки в кодовом слове. Ошибки могут быть как в информационных, так и контрольных символах.

В квантовой криптографии коррекция ошибок происходит несколько иначе. Формирования кодовых слов из исходной битовой строки Алисы не происходит. Пусть Алиса и Боб имеют битовые строки

длиной n, строка Боба с ошибками. Алиса вычисляет синдром для своей случайной битовой строки длиной n посредством умножения своей битовой строки на проверочную матрицу H, получает новую битовую строку — синдром, и направляет его к Бобу. Боб аналогичным образом по своей битовой строке вычисляет свой синдром. Далее декодер исправляет ошибки у Боба, добиваясь совпадения синдромов Алисы и Боба.

Ниже термины «исправление (коррекция) ошибок» и «декодирование» будем использовать как эквивалентные.

13.1. LDPC-коды

Проверочную матрицу можно представить в виде двудольного графа (см. ниже рис. 3). Одни вершины отвечают значениям битов исходной битовой последовательности (s — symbol nodes, далее символьные биты), а другие — значениям битов синдрома (c — check nodes, далее проверочные символы). Эти группы вершин соединены между собой в соответствии с положениями единиц в проверочной матрице: единица на позиции $\{ij\}$ — ребро между i-м символьным битом и j-м проверочным. Для LDPC-кодов проверочная матрица является сильно разреженной и соответствующий граф получается далеко не полносвязным. Задача алгоритма декодирования состоит в вычислении истинных значений битов (символьных и проверочных) при данном входном искаженном битовом векторе $\mathbf{y}$ и соответствующем искаженном синдроме Боба $\mathbf{z}$, который задается проверочной матрицей H. Декодирование для LDPC-кодов является итерационным — мягким декодированием, и работа состоит в пересылке некоторых «сообщений», фактически вероятностей, по ребрам графа между его вершинами $\mathbf{s}$ и $\mathbf{c}$, с обновлением значений битов в символьных вершинах на каждой итерации. Алгоритм применим, пока не будут удовлетворены проверочные условия или не будет достигнуто максимальное число итераций, после которых работа алгоритма прерывается. Если работа алгоритма прервана по числу итераций, а при этом проверочные условия еще не были выполнены, то последнее будет означать ошибку декодирования. Отметим, что сходимость данных алгоритмов и декодирование — исправление ошибок — строго доказаны только для деревьев, т. е. графов без циклов [30]. Если граф, порожденный проверочной матрицей, имеет циклы, то сходимость уже не всегда имеет место. По этой причине, проверочные матрицы специально подбирают таким образом, чтобы увеличить длину наименьшего цикла в соответствующем графе.

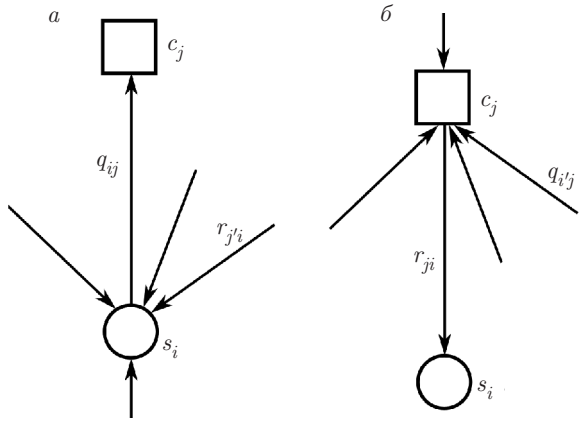

Рис. 2. Схемы создания сообщения от проверочного бита к символьному ($а$), от символьного к проверочному ($б$)

13.2. Алгоритм распространения доверия — вероятностей (belief-propagation)

Данный итерационный алгоритм был предложен в работах [28, 29]. Суть данного алгоритма сводится к следующему. Вершинам графа и ребрам (сообщениям) присваиваются не значения 0 или 1, а вероятности иметь соответствующие значения 0 или 1. Алгоритм получает на вход априорные вероятности, которые задаются вероятностью ошибки в канале связи. На выходе алгоритм выдает вероятность ошибки в каждом бите, которая далее преобразуется в само бинарное значение по порогу 0.5. Символически алгоритм может быть представлен как

$$P_{prior}(s_i|y_i) \to P_{post}(s_i|H, \mathbf{z}, \mathbf{y}). \qquad (139)$$

При представлении $s_i = y_i \oplus \tau_i$, где вероятность ошибки $\Pr(\tau_i = 1) = \varepsilon$, для канала без памяти априорная вероятность i-го бита будет зависеть только от вероятности ошибки ε в канале связи. Применительно к задаче исправления ошибок в квантовой криптографии, ошибка в канале связи Алиса–Боб есть $\varepsilon = \mathrm{Err}_\mu/Q_\mu$ (см. выше). Сообщения — условные вероятности бита — имеют значения 0 или 1. Для дальнейшего удобно ввести более краткие обозначения для вероятности ошибки, $q_{ij}(0) = 1 - q_{ij}(1)$, поэтому ниже будем считать, что $q_{ij} \equiv q_{ij}(0)$ и $r_{ij} \equiv r_{ij}(0)$. Алгоритм состоит из последовательности шагов [28–31] (см. также рис. 2).

• На нулевом шаге, $l = 0$, символьные биты сообщают свою априорную оценку из уровня ошибки

($\epsilon = E_\mu/Q_\mu$) в канале связи. Пока считаем, что оценка вероятности ошибки известна, тогда

$$q_{ij}^{(0)} = P_i = P(s_i = 0|y_i) = \\ = \begin{cases} \epsilon, & \text{если } y_i = 1, \\ 1-\epsilon, & \text{если } y_i \neq 1. \end{cases} \quad (140)$$

• На данном шаге l фиксированы значения не самих битов, кроме i-го бита, а их вероятности, т. е. $q_{i'j}$. Требуется рассчитать вероятность того, что при этих условиях значение i-го бита $s_i = 0$. В этом случае сумма остальных s_i' равна c_j (при $s_i = 0$),

$$r_{ji}^{(l)} = P\left(s_i = 0 | \bigoplus_{i' \in \mathcal{N}(j)} s_{i'} = c_j\right) = \\ = P\left(\bigoplus_{i' \in \mathcal{N}(j)/\{i'\}} = c_j\right) = \\ = \frac{1}{2} + \frac{1}{2} \prod_{i' \in \mathcal{N}(j)/\{i'\}} \left(1 - 2q_{i'j}^{(l-1)}\right) \quad (141)$$

и (при $s_i = 1$)

$$r_{ji}^{(l)} = P\left(s_i = 1 | \bigoplus_{i' \in \mathcal{N}(j)} s_{i'} = c_j\right) = \\ = P\left(\bigoplus_{i' \in \mathcal{N}(j)/\{i'\}} = c_j\right) = \\ = \frac{1}{2} - \frac{1}{2} \prod_{i' \in \mathcal{N}(j)/\{i'\}} \left(1 - 2q_{i'j}^{(l-1)}\right),$$

где при вычислении за вероятности символьных битов берутся сообщения, полученные на предыдущем шаге: $P(s_{i'} = 0) = q_{i'j}^{(l-1)}$.

• Получив новые сообщения от проверочных битов, символьные узлы обновляют свои вероятности. Для этого берется среднее геометрическое априорной и всех пришедших от проверочных битов вероятностей:

$$Q_i^{(l)} = k_i\, P_i \prod_{j' \in \mathcal{N}(i)} r_{j'i}^{(l)}. \quad (142)$$

Множитель k_i нужен для сохранения нормировки: $Q_i^{(l)}(0) + Q_i^{(l)}(1) = 1$.

• Сообщения от символьных битов к проверочным — текущие оценки вероятности данного символьного бита, т. е. $Q_i^{(l)}$. Как упоминалось ранее в разд. 13.1, алгоритм строго доказан только для графов без циклов, из-за этого для сообщения берется несколько другая оценка вероятности, не содержащая в себе только что полученное обратное сообщение $r_{ji}^{(l)}$:

$$q_{ij}^{(l)} = k_{ij} P_i \prod_{j' \mathcal{N}(i)/\{j\}} r_{j'i}^{(l)}. \quad (143)$$

Здесь множитель k_{ij} зависит также и от j.

• Чтобы проверить, удовлетворяет ли текущий вектор синдрому, вычисляют решение по полученным вероятностям: $\hat{\mathbf{y}}_i^{(l)} = 1$ при $Q_i^{(l)} \leq 0.5$, соответственно, $\hat{\mathbf{y}}_0^{(l)} = 0$ при $Q_i^{(l)} > 0.5$.

13.3. Алгоритм сложения–умножения вероятностей (sum-product)

Технически удобнее работать не с самими вероятностями, а с логарифмическими отношениями вероятностей (Logarithmic Likelihood Ratio, LLR) [28–31]. В этом случае алгоритм переформулируется в следующем виде:

$$\mathrm{LLR}(x) = \ln\left(\frac{P(x=0)}{P(x=1)}\right). \quad (144)$$

Учитывая данное соотношение, можно получить все величины из предыдущего раздела на языке логарифмических отношений вероятностей. Для краткости введем обозначение

$$\prod \equiv \prod_{i' \in \mathcal{N}(j)/\{i\}}. \quad (145)$$

Далее

$$q_{ij}^{LLR} = \ln\left(\frac{q_{ij}(0)}{q_{ij}(1)}\right) = \\ = \ln\left(\frac{k_{ij}\, P_i \prod r_{j'i}(0)}{k_{ij}\,(1-P_i) \prod r_{j'i}(1)}\right) = \\ = p_i + \sum_{j' \in \mathcal{N}(i)/\{j\}} r_{j'i}^{LLR}, \quad (146)$$

$$r_{ji}^{LLR} = \ln\left(\frac{r_{ji}(0)}{r_{ji}(1)}\right) = \ln\left(\frac{\frac{1}{2} + \frac{1}{2}\prod(1-2q_{i'j})}{\frac{1}{2} - \frac{1}{2}\prod(1-2q_{i'j})}\right) = \\ = \ln\left(\frac{1 + \prod \mathrm{th}(q_{i'j}^{LLR}/2)}{1 - \prod \mathrm{th}(q_{i'j}^{LLR}/2)}\right) = \\ = 2\,\mathrm{th}^{-1}\left(\prod \mathrm{th}\left(\frac{q_{i'j}^{LLR}}{2}\right)\right). \quad (147)$$

Эти формулы и дают название алгоритму. Конечный битовый вектор задается знаком LLR:

$$\hat{\mathbf{y}}_i = \begin{cases} 1 \text{ при } \mathrm{LLR} \le 0, \\ 0 \text{ при } \mathrm{LLR} > 0. \end{cases}$$

Для более эффективных и быстрых вычислений данные выражения можно упростить [31]. Для этого рассмотрим функцию

$$\phi(x) = -\ln \mathrm{th}\left(\frac{x}{2}\right) = \ln \frac{e^x + 1}{e^x - 1}. \qquad (148)$$

Имеем

$$\phi(\phi(x)) = \ln \frac{e^{\phi(x)} + 1}{e^{\phi(x)} - 1} = x \Rightarrow \phi^{-1} = \phi. \qquad (149)$$

Гиперболический тангенс является четной функцией, $\mathrm{th}(-x) = -\mathrm{th}(x)$, тогда

$$r_{ji}^{LLR} = \prod (\mathrm{sign}(q_{i'j}))\, \phi\Big(\sum \phi(|q_{i'j}|)\Big). \qquad (150)$$

Многократное вычисление ϕ становится самой трудоемкой операцией во всем алгоритме. Поэтому обычно ϕ заменяют различными приближениями, например, кусочно-линейной табличной аппроксимацией.

13.4. Модуляция скорости кода

Под скоростью кода (R) стандартно понимается отношение числа информационных символов (k) в кодовом слове к полной длине кодового слова (n), $R = k/n$ [32], соответственно, избыточность кода $R_r = m/n = (n-k)/n$ — отношение числа контрольных символов $m = n - k$ к длине кодового слова n, индекс r — сокращение от redundancy. Корректирующая способность кода зависит от его скорости. Неформально говоря, чем выше скорость кода, тем меньше его корректирующая способность и тем меньше вероятность ошибки в канале связи, до которой код может исправить ошибки. Применительно к квантовой криптографии это означает, что потребуется хранить несколько матриц, отвечающих кодам с разной скоростью, что крайне неудобно и затратно. Поэтому был предложен способ модуляции скорости кода (см. детали в [33–35], а также ссылки там), который вкратце сводится к тому, что используется одна матрица, отвечающая коду, например, со скоростью 1/2, но при этом меняется лишь доля (соотношение) между информационными и контрольными символами [33–35].

При заданной скорости кода всегда существует вероятность того, что ошибки не будут исправлены — это отказ декодирования. Обычно при заданной вероятности ошибки в канале Алиса–Боб выбирают такую скорость кода, чтобы вероятность отказа декодирования FER (Frame Error Rate) была на уровне 10^{-3}.

Скорость LDPC-кода при его использовании описанным выше способом постоянна и не зависит от наблюдаемой ошибки в канале между Алисой и Бобом (далее BER — Bit Error Rate). При другой вероятности ошибки в канале связи Алиса и Боб должны выбрать другую скорость кода, которая дает вероятность отказа декодирования вблизи порогового значения FER $\approx 10^{-3}$ и, соответственно, эффективность декодирования $1 - \mathrm{FER} \approx 1$. Существуют модификации процедуры исправления ошибок, которые позволяют изменять скорость кода, сохраняя тем самым эффективность, близкую к предельной в более широком диапазоне значений BER [33–35].

13.5. Уменьшение избыточности LDPC-кода «выкалыванием» (puncturing)

Идея «выкалывания» битов в кодах коррекции ошибок возникла достаточно давно (см., например, монографию Галлагера [32]) (см. также [36]). Применительно к исправлению ошибок в квантовой криптографии идея состоит в следующем. Например, пусть выбран код со скоростью 1/2. При малых значениях BER избыточность LDPC-кода слишком велика, соответственно, скорость кода слишком низка при данной BER. Избыточность кода можно эффективно понизить, заменив часть символьных битов p (p — число заменяемых, «выколотых», битов) на случайные биты, при этом значение LLR для этих битов равно $\mathrm{LLR} = 0$. Замена части битов на случайные приводит к тому, что длина синдрома — избыточность кода — уменьшается, соответственно, скорость кода возрастает. Это происходит потому, что при сложении произвольного числа битов с абсолютно случайным, сумма также будет случайной. Действительно, пусть s_0 — значение выколотого бита, который принимает равновероятно значение 0 и 1, причем независимо от других битов s_{i_k}, входящих в контрольную сумму $c_i = s_0 \oplus s_{i_1} \oplus s_{i_2} \oplus \ldots$ При этом вероятность значения контрольного символа c_i равна $P(c_i = 1) = P(c_i = 0) = P(s_0 = 0) = P(s_0 = 1) = 0.5$.

Все проверочные биты, связанные со случайными выколотыми, тоже становятся случайными, и их можно удалить из рассмотрения (как бесполезные), что эффективно уменьшает длину синдрома и увеличивает скорость кода.

Применительно к коррекции ошибок в квантовой криптографии, «выкалывание» происходит кон-

катенированием — добавлением (независимо Алисой и Бобом) строки случайных битов длиной p к сырому ключу длиной $n-p$. При этом полная длина битовой строки есть n.

Передача значений проверочных битов c_i, в которые входят случайные выколотые биты, не раскрывает никакой информации подслушивателю. В этом случае для избыточности кода имеем

$$C(n,k) \to C(n-p,k),$$
$$R_{0r} \to R_r = \frac{m-p}{n-p} = \frac{R_{0r}-\pi}{1-\pi}, \qquad (151)$$
$$R_{0r} = \frac{m}{n}, \quad \pi = \frac{p}{n}.$$

Здесь $C(n,k)$ обозначает код с длиной обрабатываемой битовой строки (кодового слова) n и скоростью k/n, $m = n-k$ — число проверочных символов в кодовом слове — длина синдрома, соответственно, $n-m$ — число информационных символов, p — начальное число случайных битов. Выкалывание p битов отвечает уменьшению длины кодового слова. Уменьшение длины синдрома приводит к увеличению скорости кода:

$$R = 1 - R_r = \frac{k}{n-p} = \frac{R_0}{1-\pi}, \quad R_0 = \frac{k}{n}.$$

Позиции выколотых битов влияют на эффективность работы декодера, поэтому выбираются не случайным образом, а специальным алгоритмом — untainted puncturing [34,35]. Алгоритм работает так, чтобы в проверочные соотношения входил ровно через один выколотый бит (множество $\mathcal{N}^2(s_i) = \{\cup_{j'\in\mathcal{N}(s_i)}\mathcal{N}(c'_j)\}$, см. рис. 3). Иными словами, при выборе позиций с помощью этого алгоритма ни один проверочный бит не будет соединен более чем с одним выколотым битом.

Выколотые биты выкидываются после декодирования, не попадая в окончательный ключ. Также, что очень важно, они не передаются между Алисой и Бобом по классическому каналу связи — на позиции выколотых битов Алиса и Боб подставляют случайные, независимые друг от друга, значения. Хотя генерация таких битов и использует генератор случайных чисел, но не требует обмена по классическому каналу связи.

13.6. Увеличение избыточности LDPC-кода «укорачиванием» (shortening)

Процедура укорачивания применяется в ситуации, когда ошибка BER в канале Алиса–Боб велика для данного кода — синдром короче, чем требуется для коррекции ошибок. Иначе говоря, при данной BER избыточность кода уже недостаточна для исправления данного уровня BER. Соответственно, скорость кода велика. Увеличить избыточность кода, соответственно, увеличить длину синдрома невозможно из-за фиксированных размеров проверочных матриц кода, поэтому применяется другой подход. Перед декодированием раскрываются значения определенных битов из битовой последовательности. Данные биты для краткости называют укороченными, а сама процедура — укорачиванием (shortening). В этом случае избыточность кода возрастает:

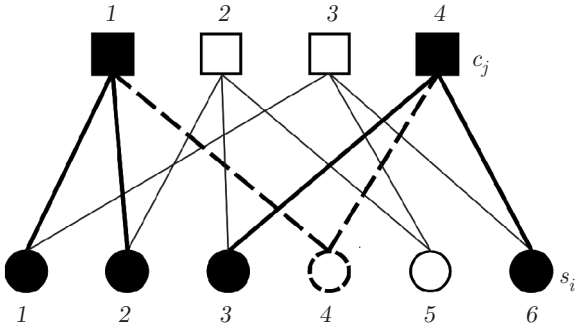

Рис. 3. Пример: четырехсимвольный бит является выколотым и отмечен штрихами (штриховая окружность), его соседи $\mathcal{N}^2(s_i) = \{\cup_{j'\in\mathcal{N}(s_i)}\mathcal{N}(c'_j)\}$ отмечены темными кружками

$$C(n,k) \to C(n-s,k-s),$$
$$R_{0r} \to R_r = \frac{m}{n-s} = \frac{R_{0r}}{1-\sigma}, \quad \sigma = \frac{s}{n}, \qquad (152)$$

а скорость кода уменьшается:

$$R = 1 - R_r = \frac{R_0-\sigma}{1-\sigma}.$$

Позиции укороченных битов могут выбираться как случайно, так и по определенному правилу. В интерактивных схемах коррекции ошибок для увеличения эффективности декодирования удобнее раскрывать значения битов не в случайных, а в определенных позициях (см. ниже, а также [37]).

13.7. Адаптивное по скорости однократное декодирование

Каждый из описанных выше методов позволяет улучшить эффективность в одну или другую сторону от предельного значения BER, при котором код еще исправляет ошибки с сохранением эффективности, в смысле сохранения заданного уровня успешного декодирования $1-\mathrm{FER}$. В кодовом слове фик-

сированной длины n можно заранее зарезервировать общую долю битов $\delta = d/n = \sigma + \pi$, которые в дальнейшем будут использоваться при выкалывании или укорачивании. При этом соотношение между долями выколотых и укороченных битов в множестве зарезервированных битов можно изменять в зависимости от текущей оценки BER, сохраняя при этом общее число выколотых и укороченных битов. При фиксированном d можно записать

$$C(n,k) \to C(n-s,k-s), \quad R_0 \to R_{min} = \\ = \frac{R_0 - \delta}{1-\delta} \le R = \frac{k-p}{n-p-s} \le \frac{R_0}{1-\delta} = R_{max}. \quad (153)$$

Заметим, что при увеличении δ, с одной стороны, расширяется диапазон ошибок BER, которые код способен исправить с высокой эффективностью — малой вероятностью отказа декодирования FER. С другой стороны, минимально достижимая эффективность становится больше, чем при использовании немодифицированного кода. Это связано с тем, что значение δ фиксировано, и даже при пороговом значении BER, при котором немодифицированный код работает оптимальнее всего, требуется модифицировать все те же d символов. Эта проблема присуща всем алгоритмам, предложенным в [33].

На рис. 4 приведены вероятности отказа декодирования FER в зависимости от вероятности ошибки BER при разных долях δ выколотых и укороченных битов.

13.8. Интерактивное декодирование

Описанные в предыдущем разделе методы предполагали только один акт обмена информацией между Алисой и Бобом. А именно, Алиса посылала Бобу только синдром своей битовой последовательности, после этого Боб проводил декодирование — исправление ошибок в своей последовательности. При этом в случае неудачного декодирования выбрасывалась вся посылка. Интерактивное декодирование подразумевает неоднократный обмен информацией между Алисой и Бобом. Например, если произошел отказ декодирования (декодер не может исправить ошибки при данной длине синдрома), то Алиса может сообщить дополнительную информацию Бобу для следующей попытки декодирования с кодом с большей избыточностью.

Собственно, в этом и состоит идея интерактивного декодирования.

13.9. Протокол «слепого» исправления ошибок (blind)

Идея «слепого» декодирования состоит в следующем (см. детали в [33–35]). Зафиксируем число модифицируемых битов d и делаем их сначала выколотыми. В случае неудачного декодирования Алиса дополнительно раскрывает Δ битов из выколотых битов и декодирование повторяется. Так продолжается до тех пор, пока не будет получена избыточность кода, при которой либо все ошибки исправлены, либо все выколотые биты будут раскрыты. Чем меньше берется шаг по Δ, тем лучше эффективность, но требуется большее число итераций. При фиксированной скорости кода время обработки, количество итераций и шаг связаны однозначно и подбираются исходя из дополнительных требований к системе. Такой алгоритм не требует априорного точного знания вероятности ошибки (BER), поэтому его называют «слепым».

Несмотря на сравнительную простоту метода, анализ эффективности требует отдельного рассмотрения. Если успешное декодирование произошло через i итераций, то окончательная скорость кода для данного блока будет равна

$$R_i = \frac{k - p_0 + i\Delta}{n - p_0}, \quad (154)$$

где p_0 — начальное число выколотых битов.

В принципе, зная зависимость FER(BER) как функцию вероятности ошибки BER в канале связи для данной проверочной матрицы, можно рассчитать вероятность того, что декодирование на i-м шаге будет успешным с вероятностью $1-\mathrm{FER}$, а отсюда получить и зависимость средней скорости кода от BER. Однако на практике это проще сделать с использованием компьютерной симуляции, результаты которой представлены в следующем разделе.

13.10. Интерактивный «слепой» протокол коррекции ошибок

Данный протокол является дальнейшим развитием «слепого» алгоритма [33–35]. Здесь общее число вспомогательных битов заранее не фиксировано, как раньше, а меняется как при инициализации, так и во время работы алгоритма. Более точно, изначально фиксируется только число выколотых битов. Если в слепом протоколе заканчивались выколотые биты, а успешного декодирования так и не произошло, то вычисления заканчивались и данный блок выбрасывался. В данном модифицированном протоколе, если все выколотые биты уже исчерпаны,

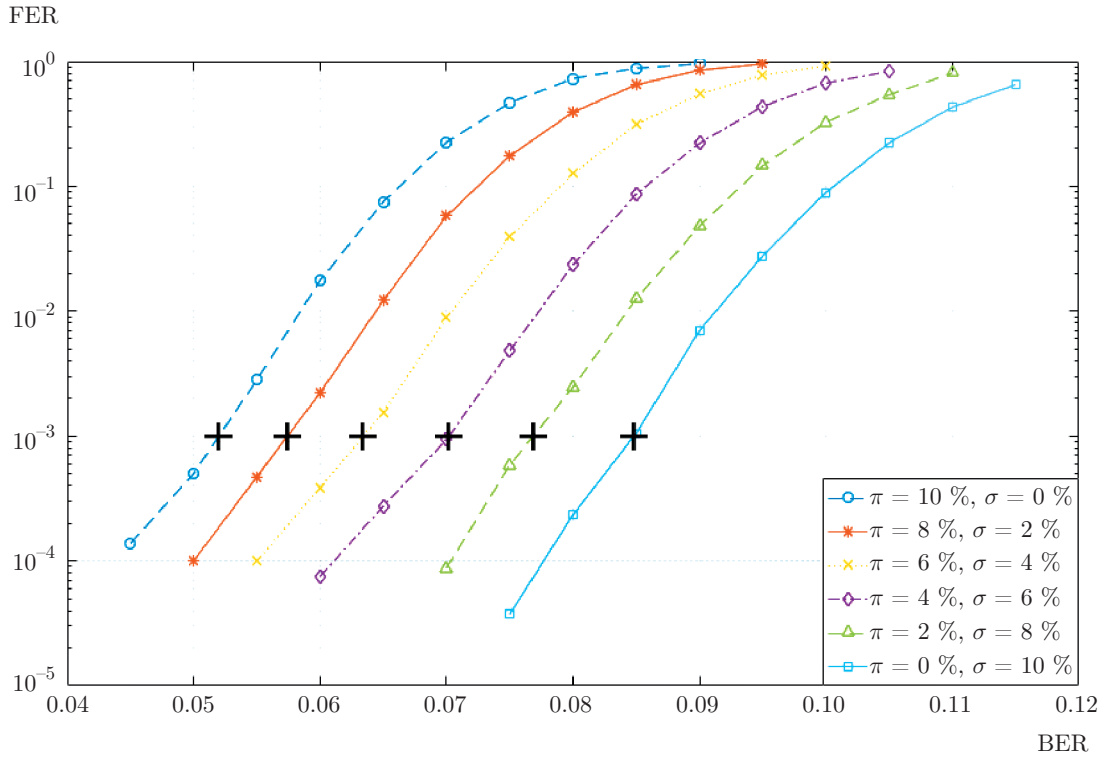

Рис. 4. (В цвете онлайн) Вероятности отказа декодирования FER как функции ошибки в канале между Алисой и Бобом BER при разных долях выколотых и укороченных битов для кода со скоростью $R = 1/2$. Черными крестиками обозначен рабочий уровень вероятности отказа FER $= 10^{-3}$

то Боб начинает раскрывать информационные биты с наименьшим LLR, т. е. биты с наиболее неопределенным значением — наиболее трудно декодируемые биты. Так происходит до тех пор, пока либо все ошибки не будут исправлены, либо все биты в кодовом слове не будут раскрыты. Таким образом, каждая строка гарантированно будет декодирована — ошибки исправлены, пусть даже ценой раскрытия всех битов в строке. Естественно, что в этом случае секретный ключ уже невозможно будет получить.

• Если в слепом протоколе все вспомогательные биты изначально брались выколотыми, то начальное количество и тип вспомогательных битов зависят от оценки вероятности ошибки BER $= \epsilon_{est}$. Если избыточность исходного кода в шенноновском пределе $f_0 = m/nh(\epsilon) > 1$, то избыточность можно уменьшить, выбрав число выколотых битов p равным

$$p = \lfloor \frac{m - nh(\epsilon_{est})}{1 - h(\epsilon_{est})} \rfloor.$$

Если избыточность кода в шенноновском пределе $f_0 = m/nh(\epsilon) < 1$ и недостаточна для исправления ошибок, то избыточность кода может быть увеличена путем выбора числа укороченных битов s, равного

$$s = \lceil n - \frac{m}{h(\epsilon_{est})} \rceil.$$

С одной стороны, это незначительно ухудшает среднюю эффективность алгоритма, но с другой уменьшает число итераций, необходимых для декодирования. Это особенно важно при больших уровнях BER.

• В «слепом» алгоритме раскрывались только выколотые биты, причем позиции среди выколотых битов выбирались случайным образом. В интерактивном «слепом» алгоритме после каждой итерации “sum-product” алгоритма декодирования (см. разд. 13.3) раскрываются Δ битов, у которых абсолютное значение LLR оказалось наименьшим. Это могут быть как выколотые биты, так и информационные биты. Именно в этих позициях значения битов являются наиболее не неопределенными — наиболее сложно декодируемыми “sum-product” алгоритмом. Скорее всего, при раскрытии именно данных позиций декодер получает наибольшую вспомогательную информацию, что ускоряет декодирование. Однако это является лишь эвристическим со-

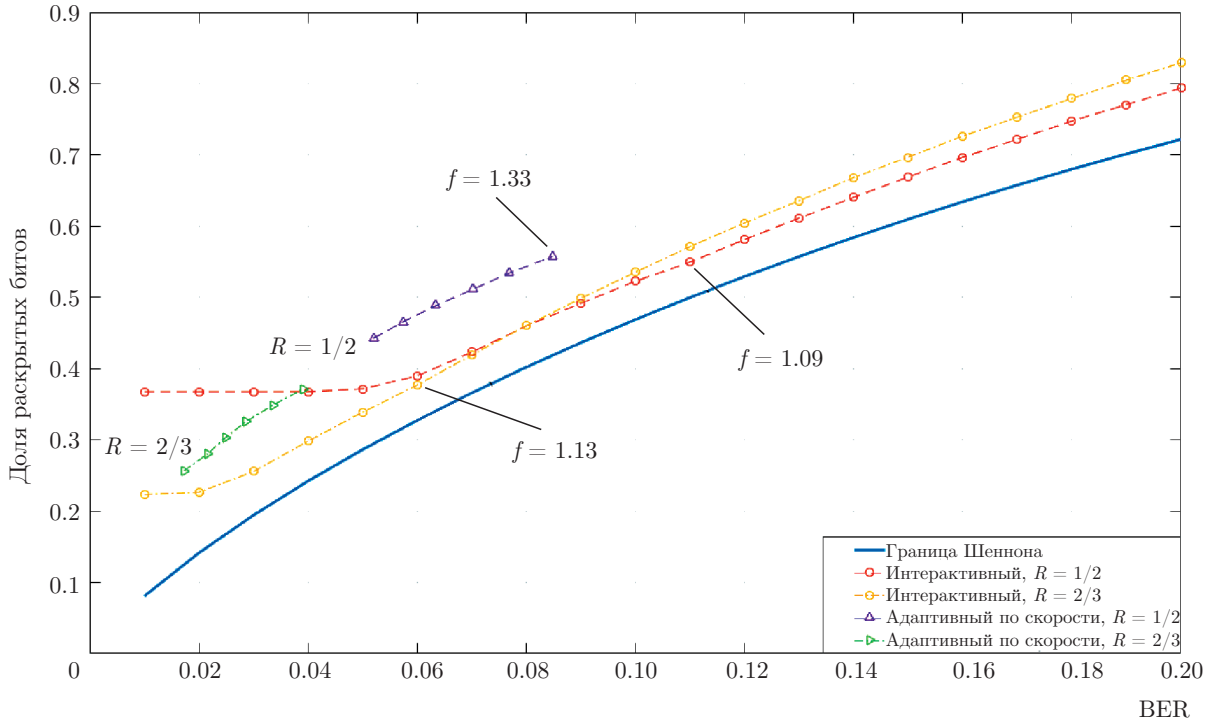

Рис. 5. (В цвете онлайн) Графики зависимости доли раскрытых битов от вероятности ошибки BER в канале связи. Представлены все протоколы очистки, описанные в тексте. Приведена также доля раскрытых битов в шенноновском пределе. Сплошной прямой линией показана эффективность простого LDPC-декодирования. Показаны эффективности декодирования для адаптивного по скорости протокола при уровне ошибки 10^{-3} для двух разных скоростей кодов. Эффективности декодирования f по отношению к шенноновскому пределу показаны стрелками

ображением, какие-либо доказательства этого факта в литературе отсутствуют. Таким образом, больше нет ограничения на максимальное число битов, которое можно раскрыть, и в предельном случае алгоритм завершит работу, когда раскроет все биты.

В завершение приведем график эффективности работы различных протоколов (рис. 5), описанных в данной работе при коррекции ошибок в первичных ключах. Из рис. 5 видно, что зависимость от скорости кода R (от размера проверочной матрицы) в многопроходном случае проявляется слабее, и при различных скоростях кода коррекция ошибок происходит практически с одинаковой и высокой эффективностью по отношению к шенноновскому пределу. Разница же при использовании кодов различных скоростей заключается в числе итераций, которое требуется для декодирования. В качестве проверочных матриц кода использовались матрицы стандарта IEEE [36]. Размеры проверочных матриц выбирались из следующих соображений. При передаче информационных состояний пакетами длиной 10^8 бит за серию, при длине линии в 100 км, после согласования базисов остается длина сырого ключа $1 \div 2 \cdot 10^3$ бит, поэтому для коррекции ошибок достаточно проверочной матрицы размером 1944×972.

14. ПРЕДЕЛЬНАЯ ДЛИНА ЛИНИИ ДЛЯ СЕКРЕТНОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

14.1. Одинаковые детекторы

Приведем зависимости длины секретного ключа при разных параметрах системы как функции длины линии связи. На рис. 6 представлены зависимости длины секретного ключа от длины линии связи при коррекции ошибок случайными шенноновскими кодами и LDPC-кодами. Параметры системы указаны на рис. 6 для случая одинаковых детекторов. Длина секретного ключа вычислялась по формуле (120). Как видно из рис. 5, LDPC-коды близки к шенноновскому пределу до вероятности наблюдаемой ошибки в 14 % — горизонтальная штриховая линия на рис. 6. При данной ошибке длина секретного ключа обращается в нуль. Как видно из рис. 6, предельная длина линии, при которой гарантируется секретное распределение ключей по Decoy state-методу, не превышает 165–175 км.

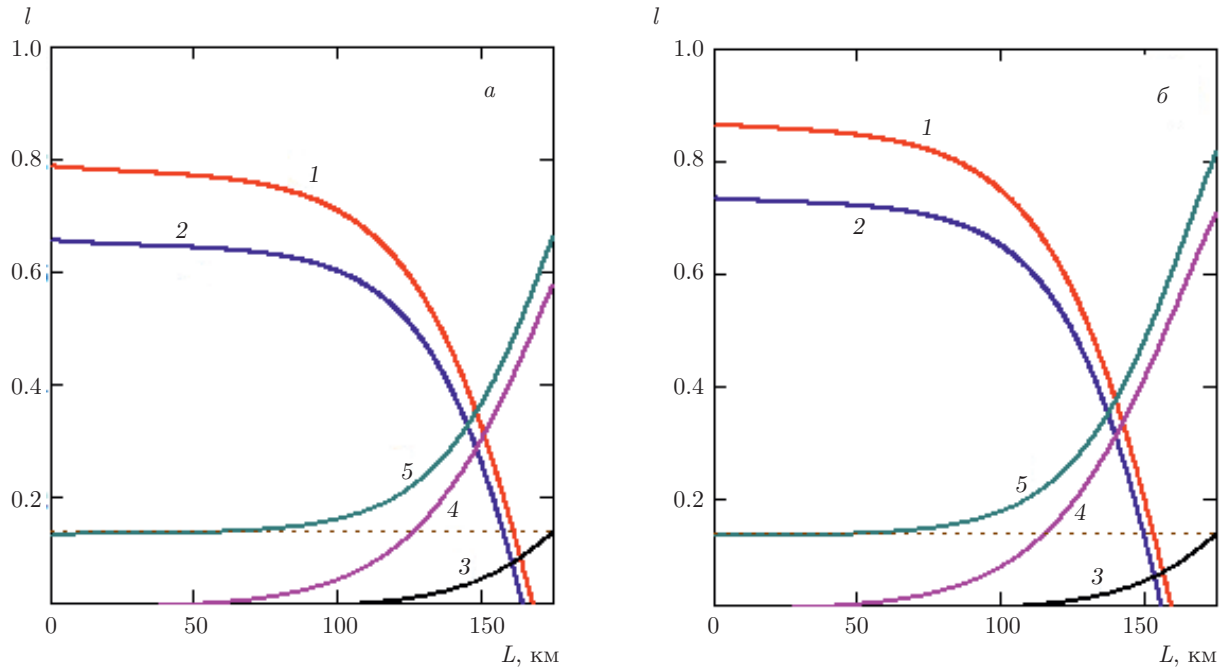

Рис. 6. Зависимости длины для секретного ключа в пересчете на одну посылку от длины линии связи. Кривые 1 отвечают коррекции ошибок случайными шенноновскими кодами. Кривые 2 отвечают коррекции ошибок LDPC-кодами. Кривые 3 — зависимости наблюдаемой ошибки на приемной стороне от длины линии связи. Кривые 4 — число раскрытых битов в пересчете на посылку при коррекции ошибок шенноновскими случайными кодами. Кривые 5 — число раскрытых битов в пересчете на посылку при коррекции ошибок LDPC-кодами. Среднее число фотонов в информационном состоянии $\mu = 0.25$ ($а$), 0.15 ($б$). Остальные параметры: $\eta = 0.1$ — квантовая эффективность лавинных детекторов, $p_d = 3 \cdot 10^{-6}$ отсчет./окно — вероятность темновых шумов на строб. Потери в линии связи 0.2 дБ/км

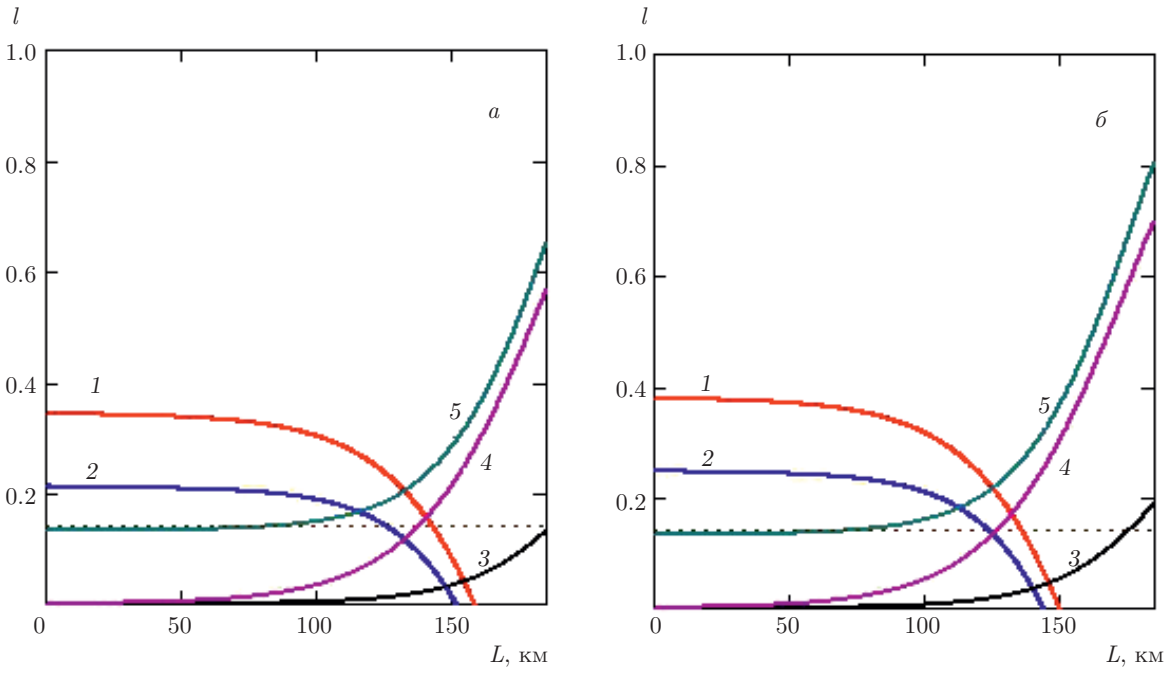

Рис. 7. Зависимости длины для секретного ключа в пересчете на одну посылку от длины линии связи. Квантовая эффективность лавинных детекторов $\eta_1 = 0.01$ ($а$) и $\eta_2 = 0.1$ ($б$). Остальные параметры такие же, как для рис. 6

14.2. Разные детекторы

В предыдущем разделе были приведены зависимости длины секретного ключа от длины линии в случае одинаковых параметров лавинных однофотонных детекторов. В реальной ситуации параметры лавинных детекторов всегда различаются. На рис. 7 приведены зависимости длины секретного ключа от длины линии связи. Оценочная длина секретного ключа в этом случае оказывается меньше, чем в случае одинаковых параметров детекторов. Данный факт можно увидеть из формулы (136). Однофотонная компонента состояний в случае разных детекторов содержит множитель $h(\min\{\kappa\})$ (формулы (133), (136)). Функция $h(x)$ является растущей функцией в интервале $(0, 1/2)$. При одинаковых детекторах $\min\{\kappa\} = 1/2$, соответственно, $h(1/2) = 1$. В этом случае максимальна условная энтропия фон Неймана в формуле (135) $H\left(\widehat{\rho}_{XE}^{(1)}|\widehat{\rho}_{E}^{(1)}, \kappa\right)$, которая имеет смысл нехватки информации подслушивателя о ключе Алисы, при условии, что подслушиватель имеет в своем распоряжении квантовую систему, коррелированную с ключом. По этой причине оценка длины секретного ключа также максимальна. Например, при равной вероятности темновых шумов длина секретного ключа обращается в нуль практически при длине линии связи в несколько километров, при отношении квантовых эффективностей детекторов, равной $\eta_1/\eta_2 = 1\,\%$. Гораздо более критической является сама величина секретного ключа.

На рис. 6, 7 видно, что максимум нижней оценки длины секретного ключа достигается при одинаковой квантовой эффективности лавинных детекторов.

15. ЗАКЛЮЧЕНИЕ

Выше была исследована криптостойкость квантового распределения ключей с фазово-временны́м кодированием в асимптотическом пределе длинных последовательностей. Учет конечной длины передаваемых последовательностей требует отдельного рассмотрения. Вычисление длины секретного ключа для однофотонной компоненты в случае конечной длины последовательности приведено в работе [38], аналогичным образом могут быть учтены флуктуации параметров для многофотонных компонент информационных состояний.

Благодарности. Один из авторов (С. Н. М.) выражает благодарность коллегам из Академии криптографии Российской Федерации за обсуждения. Авторы благодарят И. М. Арбекова, К. А. Балыгина, А. Н. Климова, К. С. Кравцова, С. П. Кулика за многочисленные и интенсивные обсуждения, а также И. М. Арбекова и С. П. Кулика за прочтение рукописи и ряд замечаний, способствующих улучшению текста.

Финансирование. Работа поддержана проектом Российского научного фонда 16-12-00015 (Продолжение).

ЛИТЕРАТУРА

1. C. H. Bennett and G. Brassard, in *Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process.*, pp. 175–179, Bangalore, India (1984).

2. M. Tomamichel, Ch. Ci Wen Lim, N. Gisin, and R. Renner, Nature Commun. **3**, 1 (2012).

3. A. N. Klimov, K. A. Balygin, and S. N. Molotkov, Laser Phys. Lett. **15**, 075207 (2018).

4. K. A. Balygin, A. N. Klimov, I. B. Bobrov, K. S. Kravtsov, S. P. Kulik, and S. N. Molotkov, Laser Phys. Lett. **15**, 095203 (2018).

5. L. Lydersen, C. Wiechers, Ch. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photon. **4**, 686 (2010).

6. G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

7. Won-Young Hwang, arXiv[quant-ph]:0211153.

8. Xiang-Bin Wang, Phys. Rev. Lett. **94**, 230503 (2005).

9. Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, Phys. Rev. Lett. **94**, 230504 (2005).

10. Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo, arXiv[quant-ph]:0503005.

11. Yi Zhao, Bing Qi, Xiongfeng Ma, Hoi-Kwong Lo, and Li Qian, arXiv[quant-ph]:0503192.

12. D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, Sae Woo Nam, and J. E. Nordholt, Phys. Rev. Lett. **98**, 010503 (2007).

13. B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Zh. Yuan, and A. J. Shields, Nature **501**, 69 (2013).

14. M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, Opt. Express **21**, 24550 (2013).

15. Sellami Ali, Shuhairi Saharudin, and MR. B. Wahiddin, Amer. J. Engin. Appl. Sci. **2**, 694 (2009).

16. Ch. Ci Wen Lim, M. Curty, N. Walenta, Feihu Xu, and H. Zbinden, Phys. Rev. A **89**, 022307 (2014); arXiv[quant-ph]:1311.7129.

17. Feihu Xu, Shihan Sajeed, Sarah Kaiser, Zhiyuan Tang, V. Makarov, and Hoi-Kwong Lo, Phys. Rev. A **92**, 032305 (2014).

18. Zhen Zhang, Qi Zhao, Mohsen Razavi, and Xiongfeng Ma, Phys. Rev. A **95**, 012333 (2017).

19. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comp. **4**, 325 (2004).

20. С. Н. Молотков, ЖЭТФ **133**, 5 (2008) [S. N. Molotkov, JETP **106**, 1 (2008)].

21. S. N. Molotkov, JETP Lett. **102**, 473 (2015).

22. С. Н. Молотков, К. С. Кравцов, М. И. Рыжкин, ЖЭТФ **155**, 636 (2019).

23. R. Gallager, IRE Trans. Inf. Theory **8**, 21 (1962).

24. R. G. Gallager, *Low-Density Parity-Check Codes*, MIT Press, Cambridge (1963).

25. R. Renner, PhD thesis, ETH Zürich, arXiv/quant-ph:0512258 (2005).

26. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, Cambridge (2010).

27. T. J. Richardson and R. L. Urbanke, IEEE Trans. Inf. Theory **47**, 599 (2001).

28. D. J. MacKay and R. Neal, Electron. Lett. **32**, 1645 (1996).

29. D. J. MacKay, IEEE Trans. Inf. Theory **45**, 399 (1999).

30. D. J. MacKay, *Information Theory, Inference, and Learning Algorithms*, Cambridge Univ. Press, Cambridge (2003).

31. Sarah J. Johnson, *Introducing Low-Density Parity-Check Codes*, School of Electrical Engineering and Computer Science, Univ. of Newcastle, Australia (2006).

32. R. G. Gallager, *Information Theory and Reliable Communication*, J. Wiley & Sons, New York, London, Sydney, Toronto (1968).

33. J. Martinez Mateo, Ph. D. Thesis, Univ. Politécnica de Madrid, Facultad de Informática, Madrid (2011).

34. D. Elkouss Coronas, PhD Dissertation, Univ. Politécnica de Madrid, Facultad de Informática, Madrid (2011).

35. D. Elkouss, J. Martinez-Mateo, and V. Martin, arXiv: 1103.6149 [cs.IT].

36. IEEE Standard for Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std.802.11n$^{\text{TM}}$ (2009).

37. E. O. Kiktenko, A. S. Trushechkin, C. W. Lim, Y. V. Kurochkin, and A. K. Fedorov, Phys. Rev. Appl. **8**, 044017 (2017).

38. S. N. Molotkov, Laser Phys. Lett. **16**, 035203 (2019).