ЖЭТФ, 2009, том 136, вып. 4 (10), стр. 650–683

ДВУХПАРАМЕТРИЧЕСКАЯ КВАНТОВАЯ КРИПТОГРАФИЯ НА ВРЕМЕННЫ́Х СДВИГАХ, УСТОЙЧИВАЯ К АТАКЕ С РАСЩЕПЛЕНИЕМ ПО ЧИСЛУ ФОТОНОВ

Д. А. Кронберг [c], ***С. Н. Молотков*** [a,b,c*]

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

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

Поступила в редакцию 27 апреля 2009 г.

Рассмотрено новое семейство двухпараметрических протоколов квантового распределения ключей. В этом семействе детектирование попыток подслушивания происходит по двум параметрам — вероятности ошибки в информационной последовательности Q и вероятности отсчетов в контрольных временных окнах q. Для однофотонного источника и ортогональных состояний внутри базиса данный протокол обеспечивает самую большую критическую ошибку, до которой гарантируется секретность распределения ключей. Для данного протокола достигается теоретический предел в 50 %. В случае неоднофотонных информационных состояний, когда источником является ослабленное лазерное излучение (когерентное состояние), данный протокол также обеспечивает наибольшую длину линии связи по сравнению с другими известными системами квантовой криптографии. Секретность ключей обеспечивается вплоть до длины линии связи, когда потери в линии связи таковы, что подслушиватель может блокировать все посылки, содержащие пять фотонов.

PACS: 03.67.Dd

1. ВВЕДЕНИЕ

Квантовая информатика лежит на пересечении двух наиболее значительных теорий прошлого века — квантовой механики и теории информации. Квантовая криптография, или более точно квантовое распределение криптографических ключей, является примером того, как достаточно абстрактные идеи за достаточно короткое время были доведены до практических технологий [1, 2].

Целью квантовой криптографии является передача криптографических ключей по открытым, доступным для прослушивания и любой модификации каналам связи при помощи специальных протоколов, использующих квантовые состояния, таким образом, чтобы на приемной (обычно называемой Бобом) и передающей стороне (обычно Алиса) возник идентичный и известный только им секретный ключ — случайная строка битов. На практике такими каналами являются либо оптоволоконные линии связи, либо открытое пространство [1, 2].

Протокол квантового распределения ключей позволяет детектировать любые попытки подслушивания, которые неизбежно приводят к появлению ошибок на приемной стороне [3]. При этом секретность ключей гарантируется на уровне фундаментальных законов природы лишь при условии, что наблюдаемая ошибка на приемной стороне не превышает некоторой критической величины, которая зависит от протокола квантового распределения ключей [1, 2]. Если наблюдаемая ошибка на приемной стороне достигает критической величины, то длина секретного ключа в битах стремится к нулю, и передача ключей становится невозможной.

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

Поэтому, чем больше допустимая критическая ошибка протокола, тем более устойчивой является система квантовой криптографии по отношению к собственным шумам и попыткам подслушивания. Ошибки, вносимые подслушивателем, и ошибки за счет собственных шумов принципиально неразличимы, и все ошибки приходится относить на счет действий подслушивателя. Из-за фундаментальных ограничений квантовой механики на измеримость квантовых состояний любое измерение, вообще говоря, приводит к возмущению состояний и соответственно к ошибкам на приемной стороне. Величина возмущения (ошибки) связана с утечкой информации к подслушивателю, поэтому, чем больше критическая ошибка, тем допустимы бóльшие собственные шумы и более интенсивные вторжения в канал связи, при которых все еще гарантируется секретность передаваемых ключей.

Таким образом, одно из главных требований, предъявляемых к квантовым протоколам распределения ключей, сводится к тому, чтобы допустимая критическая ошибка имела максимально возможное значение.

Были затрачены значительные усилия по модификации протоколов квантового распределения ключей для того, чтобы увеличить допустимую критическую ошибку [1, 2, 4–11]. На сегодняшний день наибольшая критическая ошибка, до которой можно передавать ключи, составляет $Q_c \approx 30\,\%$ [4–11].

С другой стороны, известно, что безошибочная передача информации через бинарный классический канал связи возможна вплоть до вероятности ошибки $Q < 50\,\%$ [12, 13], что согласно теореме кодирования для канала с шумом является теоретическим пределом [12, 13]. В связи с этим возникает принципиальный вопрос о том, можно ли предъявить технически реализуемый квантовый протокол распределения ключей, который обеспечивает не только передачу ключей, но и гарантирует их секретность вплоть до теоретического предела по вероятности ошибки в $50\,\%$. Ниже будет приведен подробный анализ такого протокола для строго однофотонного источника.

Однако тот факт, что протокол распределения ключей обеспечивает большую критическую ошибку в случае однофотонного источника, еще не гарантирует стойкость протокола, если источник не является строго однофотонным. Хотя нет принципиальных запретов на создание однофотонного источника и существует ряд успешных экспериментов по таким источникам [14–18], в существующих системах квантовой криптографии в качестве квантовых состояний используется ослабленное лазерное излучение, которое описывается когерентным состоянием. Лазерное излучение имеет пуассоновское распределение по числу фотонов, поэтому с определенной вероятностью, которая зависит от среднего числа фотонов (интенсивности), в когерентном состоянии могут встретиться посылки, где присутствуют два, три и более фотонов с убывающими вероятностями.

Кроме того, реальные каналы связи имеют потери. Было осознано [19, 20], что неоднофотонность источника и потери в канале связи могут приводить к невозможности передачи секретных ключей при длинах линии связи, большей некоторой критической. Это связано с так называемой PNS-атакой (Photon Number Splitting Attack — атака с расщеплением по числу фотонов). Такая атака была открыта в работе [19] и сводится к следующему. В квантовой механике нет принципиальных запретов на неразрушающее (без возмущения) измерение числа фотонов, но не их состояния. При наличии потерь в канале связи число посылок на передающей и приемной сторонах не совпадает. При длине линии связи, известной заранее, на приемной стороне можно лишь следить за средним числом посылок, достигающих приемной стороны, поэтому подслушивателю достаточно лишь сохранить среднее число посылок на приемной стороне. При неоднофотонном источнике, подслушиватель может определить число фотонов в каждой посылке[1)]. Если в посылке обнаружен один фотон, то посылка блокируется. Поскольку сама линия связи в квантовой криптографии не контролируется легитимными пользователями, подслушиватель может любым образом модифицировать линию связи, заменив ее, например, на линию с меньшим затуханием (в пределе вообще без потерь), и перепосылать свои состояния по этой линии. При длине линии связи, большей некоторой критической, такое блокирование остается недетектируемым и списывается на приемной стороне на потери в канале связи.

Если обнаружено два и более фотонов, то часть фотонов подслушиватель сохраняет у себя в квантовой памяти[2)], а часть через канал связи с меньшими потерями посылает на приемную сторону. Если используется протокол, в котором состояния в разных

[1)] В квантовой криптографии при анализе стойкости протоколов консервативно считается, что легитимные пользователи ограничены существующим уровнем технологий, а действия подслушивателя не лимитируются никакими техническими ограничениями кроме запретов, диктуемых фундаментальными законами природы.

[2)] В реальной ситуации достаточно использовать оптоволоконную линию задержки.

базисах ортогональны, например, как в наиболее известном и наиболее подробно изученном протоколе BB84 [21–23], то подслушиватель может задерживать свои измерения до стадии разглашения базисов, а затем измерять свои состояния в уже известном базисе и иметь полную информацию о ключе, не внося при этом ошибок на приемной стороне. Начиная с некоторой критической длины линии связи подслушиватель может блокировать все однофотонные посылки, а из многофотонных посылок иметь полную информацию о ключе. Таким образом, для протоколов с ортогональными состояниями внутри базиса распределение ключей при не строго однофотонном источнике и потерях в канале связи невозможно при длине линии связи, большей критической.

Усовершенствование протокола сводится к тому, чтобы сделать состояния достоверно неразличимыми внутри базиса, что может быть достигнуто, если сделать состояния неортогональными. Один из таких модифицированных протоколов был назван SARG04 [24]. Исследование стойкости показало [25], что протокол теряет секретность начиная с длины линии связи, при которой подслушиватель может блокировать все трехфотонные посылки, не меняя общего среднего числа посылок, достигающих приемной стороны. Посылок с тремя фотонами уже достаточно для того, чтобы подслушиватель мог иметь полную информацию о ключе, не внося ошибок на приемной стороне. Протокол SARG04 [24] гарантирует секретность ключей при бóльших длинах, чем BB84 [3], однако этого не всегда достаточно.

Ниже будет предложен и исследован протокол квантового распределения ключей, который имеет максимальную из всех известных протоколов критическую ошибку при строго однофотонном источнике и гарантирует секретность при неоднофотонном источнике при большем, по сравнению с другими протоколами, затухании (соответственно длине линии связи). Протокол теряет секретность лишь при длине линии связи, начиная с которой подслушиватель может блокировать все посылки, в которых присутствуют пять фотонов.

Структура работы следующая. В разд. 2 получена связь между различными формулировками критерия секретности ключей, которые используются в дальнейшем. Раздел 3 посвящен анализу стойкости комбинированного протокола распределения ключей в однофотонном режиме с ортогональными и неортогональными состояниями внутри базисов. В разд. 4 приведены результаты по исследованию стойкости квантовой криптографии при неоднофотонном источнике, потерях в канале связи и неидеальных фотодетекторах для комбинированного протокола с неортогональными состояниями внутри базисов.

2. КРИТЕРИЙ СЕКРЕТНОСТИ КЛЮЧЕЙ

2.1. Критерий секретности ключей в классическом случае

Ключ представляет собой случайную битовую строку. Пусть длина ключа r бит. В конце протокола легитимные пользователи должны иметь одинаковый и случайный ключ $x \in X = \{0,1\}^r$ $(x = (x_1, x_2, \ldots, x_r))$, подчиняющийся равномерному распределению $P_U(x)$ на X — $P_U(x) = 1/2^r$. Пусть соответствующий ключ подслушивателя $x_E \in X_E = \{0,1\}^r$, который каким-то образом коррелирован с ключом легитимных пользователей x. Неформально ключ x секретен, если он неизвестен подслушивателю. Более формально ключ x секретен, если условная вероятность $P_{X|X_E}(x|x_E)$, описывающая степень корреляции ключей, равна

$$P_{X|X_E}(x|x_E) = \frac{1}{2^r}, \tag{1}$$

т. е. вероятность того, что подслушиватель знает ключ, равна вероятности простого угадывания случайной строки x. Это идеальная ситуация для легитимных пользователей и наихудшая для подслушивателя.

Пусть $P_{XX_E}(x, x_E)$ — совместное распределение вероятностей, которое описывает корреляцию ключей легитимных пользователей и подслушивателя, и

$$P_{X_E}(x_E) = \sum_x P_{XX_E}(x, x_E)$$

— соответствующее маргинальное распределение. Близость к идеальной ситуации может быть выражена при помощи расстояния

$$d = \| P_{XX_E} - P_U P_{X_E} \|_1 = \sum_{x,x_E} |P_{XX_E}(x, x_E) - P_U(x) P_{X_E}(x_E)|. \tag{2}$$

Если данное расстояние равно нулю, то реализуется идеальная ситуация.

2.2. Критерий секретности ключей в квантовой криптографии

Любой протокол квантового распределения ключей состоит из следующих шагов. Далее будем рассматривать протоколы с несколькими базисами.

1. Используется несколько равноправных базисов, в каждом из которых имеется алфавит классических символов X, как правило бинарный: $X = \{0,1\}$. В каждой посылке Алиса случайно в соответствии с равномерным распределением выбирает сначала базис, а затем символ классического алфавита в этом базисе, приготавливает отвечающее этому символу квантовое состояние и направляет в канал связи, причем возможны два эквивалентных способа действий. В первом Алиса готовит квантовое состояние ρ_A и напрямую посылает к Бобу. Во втором Алиса готовит запутанное состояние ρ_{AB}, подсистема B направляется к Бобу, а подсистема A остается у Алисы. В дальнейшем Алиса делает измерения над своей подсистемой A. Поскольку состояние ρ_{AB} запутанное, измерение над подсистемой A фиксирует состояние подсистемы B.

2. После достаточно большого числа посылок N ситуация для всех участников протокола описывается совместной матрицей плотности $\rho_{A^N B^N E^N}$. Далее через открытый классический канал связи Алиса и Боб осуществляют согласованные случайные перестановки состояний своих подсистем в разных посылках. Это приводит к тому, что частичная матрица плотности $\rho_{A^N B^N}$ становится инвариантной относительно перестановок и согласно квантовому аналогу классической теоремы де Финетти (de Finetti, см. детали в работе [26]) может быть сколь угодно точно представлена в виде тензорного произведения матриц плотности, относящихся к отдельным посылкам[3]: $\rho_{A^N B^N} \approx \sigma_{AB}^{\otimes N}$.

3. Затем Алиса и Боб через открытый канал связи выбирают базис, в котором они будут проводить измерения. Как правило, измерения на стороне Алисы описываются ортогональными проекторами $\{\mathcal{M}_x\}$ ($x \in X$). Измерения на стороне Боба, если состояния внутри базиса неортогональны, могут описываться неортогональными разложениями единицы. Пусть набор измеряющих операторов на приемной стороне есть $\{\mathcal{M}_y\}$ ($y \in Y$, Y — множество результатов измерений[4]). Совместная матрица плотности Алисы и Боба после измерений становится равной σ_{XY}, соответственно совместная матрица плотности всех участников протокола есть σ_{XYE}. В результате измерений возникает совместное распределение вероятностей

$$P_{XY}(x,y) = \mathrm{Tr}\{\mathcal{M}_x \mathcal{M}_y \sigma_{AB}\},$$

такое что вероятность ошибки Q на приемной стороне равна $Q = \sum_{x \neq y} P_{XY}(x,y)$.

4. Следующий шаг состоит в оценке степени искажения подслушивателем переданных состояний. После измерений и отбрасывания исходов с неопределенным результатом Алиса и Боб имеют битовые строки длины n — первичный ключ, но строка Боба еще содержит ошибки. Часть последовательности раскрывается и оценивается вероятность ошибки, раскрытая часть в дальнейшем отбрасывается. При большой длине исходной последовательности в оставшейся нераскрытой части вероятность ошибки такая же, как в раскрытой.

5. Следующий шаг состоит в коррекции ошибок на приемной стороне посредством обмена классической информацией через открытый аутентичный канал связи. Далее будем иметь в виду односторонние обмены. Алиса открыто выбирает код корректирующей ошибки, зависящий от величины ошибки Q, и сообщает Бобу корректирующую информацию. Теоретически минимальная информация в битах, которую необходимо сообщить Алисе через открытый канал Бобу для исправления ошибок при больших n, составляет $nH(X|Y)$ ($nH(X|Y)$ — условная энтропия Шеннона[5]). После исправления ошибок Алиса и Боб имеют идентичные битовые строки длины n — очищенный ключ, о котором Ева при наблюдаемой ошибке $Q < Q_c$ меньше критической имеет частичную информацию. При ошибке $Q > Q_c$ Ева имеет полную информацию об очищенном ключе.

6. «Удаление» информации подслушивателя (усиление секретности — privacy amplification [27]), которую Ева получила из квантового канала связи и из классического при коррекции ошибок, происходит посредством хэширования (сжатия) очищенного ключа при помощи универсальных хэш-функций второго порядка [28], сжимающих битовую строку длины n до строки длиной r. Хэш-функция

$$f(x) \in \mathcal{F} = \{f : \{\{0,1\}^n \to \{0,1\}^r\}$$

сама является случайной величиной, которую легитимные пользователи выбирают открыто и случайно в соответствии с равномерным распределением на множестве таких функций $\mathcal{F}$ (см. детали

[3] Из этого факта следует, что когерентная атака (coherent) Евы не является более эффективной, чем коллективная атака, т. е. достаточно ограничиться только коллективной атакой.

[4] При неортогональных состояниях внутри базиса множество исходов имеет вид $Y = \{0,1,?\}$, где исходы ? отвечают исходам измерений с неопределенным результатом, которые в дальнейшем отбрасываются.

[5] После измерений и отбрасывания исходов с неопределенным результатом условная энтропия Шеннона $H(X|Y)$ совпадает с условной энтропией фон Неймана $S(\sigma_{XY}|\sigma_Y)$.

в работе [27]). Данные функции обладают следующим свойством: для любой случайно выбранной функции и любых двух случайных значений аргумента вероятность совпадения значений функции $\Pr\{f(x_1) = f(x_2)\} \leq 1/2^r$. Строка длины r представляет собой финальный секретный ключ.

В квантовой криптографии используется аналогичный (2) критерий секретности ключей, введенный и подробно исследованный в работе [26]. В квантовой криптографии на конечной стадии протокола совместное состояние Евы и легитимных пользователей описываются матрицей плотности σ_{XE}. В качестве критерия секретности ключей [26] используется расстояние

$$d = \| \sigma_{XE} - \sigma_U \otimes \sigma_E \|_1 = \mathrm{Tr}|\sigma_{XE} - \sigma_U \otimes \sigma_E|, \quad (3)$$

где модуль оператора $|A| = \sqrt{A^+ A}$,

$$\begin{aligned} \sigma_{XE} &= \sum_{x\in X} P_X(x) |x\rangle_X \langle x| \otimes \sigma_E^x, \\ \sigma_U &= \frac{1}{2^r} \sum_{x\in X} |x\rangle_X \langle x| \end{aligned} \quad (4)$$

— матрица плотности, отвечающая однородному распределению, $|x\rangle_X = |x_1, x_2, \ldots, x_r\rangle_X$ — ортонормированный набор базисных векторов, отвечающий ключу x.

Квантовая криптография гарантирует, что если ошибка меньше критической величины, то расстояние (3) может быть сделано экспоненциально близким к идеальной ситуации по длине исходной переданной последовательности $N - d \sim 2^{-\gamma N}$ [26]. При этом длина секретного ключа (доля секретных битов на посылку), которую можно получить в результате шагов протокола, описанных выше, в асимптотическом пределе больших N стремится к значению

$$\begin{aligned} r &= \lim_{N\to\infty} \frac{r(N)}{N} = \\ &= \min_{\sigma_{AB}\in\Gamma(\mathcal{M}_x,\mathcal{M}_y,Q)} (S(\sigma_{XE}|\sigma_E) - S(\sigma_{XY}|\sigma_Y)), \end{aligned} \quad (5)$$

$$\sigma_{XYE} = \mathcal{T}_{XYE\leftarrow ABE}(\sigma_{ABE}). \quad (6)$$

Здесь $\mathcal{T}_{XYE\leftarrow ABE}(\ldots)$ — вполне положительное отображение[6)], описывающее изменение совместной матрицы плотности всех участников при измерениях Алисы и Боба, σ_{ABE} — «очищенная» матрица плотности σ_{AB}, $\Gamma(\mathcal{M}, Q)$ — множество матриц плотности σ_{AB}, на которых измерения $\mathcal{M}_x, \mathcal{M}_y$ дают наблюдаемую ошибку Q. Условная энтропия фон Неймана по определению равна

$$\begin{aligned} S(\sigma_{XY}|\sigma_Y) &= S(\sigma_{XY}) - S(\sigma_Y), \\ S(\sigma_{XE}|\sigma_E) &= S(\sigma_{XE}) - S(\sigma_E), \end{aligned} \quad (7)$$

где $S(\sigma) = -\mathrm{Tr}\{\sigma \log_2 \sigma\} = -\sum_i \lambda_i \log_2 \lambda_i$ — энтропия фон Неймана, λ_i — собственные числа матрицы плотности σ.

Формула (5) имеет простую качественную интерпретацию. До исправления ошибок Алиса имеет битовую строку x, а Боб — строку y длины n, которая содержит ошибки. Бобу, чтобы исправить ошибки и сделать свою строку идентичной строке Алисы, не хватает $nS(\sigma_{XY}|\sigma_Y)$ битов информации. Ева имеет в своем распоряжении квантовые состояния, описывающиеся матрицей плотности σ_E, которые коррелированы с битовой строкой Алисы. Количество битов информации, которых не хватает Еве для того, чтобы узнать строку Алисы, есть $nS(\sigma_{XE}|\sigma_E)$. Разница двух информаций в битах в формуле (5), собственно, и является той секретной информацией о строке битов Алисы, которой обладает Боб по сравнению с Евой.

Важно отметить, что все матрицы плотности относятся к отдельной посылке. Однако формула (5) подразумевает, что измерения Евы являются коллективными (см. ниже).

2.3. Связь между различными критериями секретности ключей в квантовой криптографии

Ниже мы обсудим другие критерии секретности ключей в квантовой криптографии, которые оказываются эквивалентными между собой. Для экономии вычислений в разных случаях удобно пользоваться критерием в той или иной форме.

Существует два вида эквивалентных формулировок протоколов квантового распределения ключей. Первый способ состоит в том, что в каждой посылке Алиса готовит квантовое состояние и напрямую посылает его в канал связи. Второй способ использует запутанные состояния двух подсистем A и B, так называемый entanglement based version [29]. Подсистема A остается на передающей стороне, а подсистема B посылается на приемную сторону.

Прежде всего найдем связь между двумя формулировками. Начнем со второго способа. Алиса при-

[6)] Если состояния внутри базисов ортогональны и нет отбрасывания исходов с неопределенным результатом, отображение имеет простой вид $\mathcal{T}_{XYE\leftarrow ABE}(\ldots) = \sum_{x,y} \mathcal{P}_{xy}(\ldots)\mathcal{P}_{xy} \otimes I_E$, $\mathcal{P}_{xy} = |x,y\rangle_{AB\,AB}\langle x,y|$ — ортогональные проекторы в $\mathcal{H}_A \otimes \mathcal{H}_B$, I_E — единичный оператор в пространстве $\mathcal{H}_E$, отражающий то обстоятельство, что Ева на данном этапе не делает никаких измерений.

готавливает запутанное состояние в пространстве состояний $\mathcal{H}_A \otimes \mathcal{H}_B$:

$$|\Phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |\phi^0\rangle_B + |1\rangle_A \otimes |\phi^1\rangle_B). \qquad (8)$$

Здесь состояния $|\phi^0\rangle_B$ и $|\phi^1\rangle_B$ относятся к некоторой группе состояний (базису). Базисы считаются равноправными и их выбор осуществляется равновероятно. Состояния $|\Phi\rangle_{AB}$ внутри каждого базиса также выбираются равновероятно. Индекс базиса, чтобы не загромождать выкладки, опускаем.

В дальнейшем состояние на приемной стороне фиксируется случайным образом в результате измерения на передающей стороне над подсистемой A. Измерение дается ортогональным разложением единицы в пространстве $\mathcal{H}_A$:

$$I_A = \sum_{x=0,1} \mathcal{M}_x, \quad \mathcal{M}_x = |x\rangle_A \, {}_A\langle x|. \qquad (9)$$

Измерение Алисы случайно и равновероятно дает два исхода: $x = 0$ или $x = 1$, каждый исход у Алисы фиксирует состояние у Боба: соответственно $|\phi^0\rangle_B$ или $|\phi^1\rangle_B$.

Ева имеет доступ только к подсистеме B. Тот факт, что совместная матрица плотности Алисы и Боба $\rho_{A^N B^N}$ после случайных перестановок может быть представлена в виде тензорного произведения $\sigma_{AB}^{\otimes N}$ — матриц плотности, относящихся к отдельным посылкам, — означает, что наиболее общая стратегия Евы сводится к приготовлению в каждой посылке некоторого вспомогательного квантового состояния $|E\rangle_E$ в пространстве $\mathcal{H}_E$, которое приводится во взаимодействие с состоянием подсистемы B. Совместная эволюция описывается унитарным оператором U_{BE}, действующим в пространстве $\mathcal{H}_B \otimes \mathcal{H}_E$, имеем

$$|\Phi\rangle_{AB} \otimes |E\rangle_E \to U_{BE}(|\Phi\rangle_{AB} \otimes |E\rangle_E). \qquad (10)$$

Измерение (9) Алисы переводит состояние (10) в следующее:

$$\sqrt{\mathcal{M}_x}(U_{BE}(|\Phi\rangle_{AB} \otimes |E\rangle_E)) \to \\ \to |x\rangle_A \otimes (U_{BE}(|\phi^x\rangle_B \otimes |E\rangle_E)). \qquad (11)$$

Измерения на приемной стороне проводятся над возмущенной подслушивателем подсистемой B. Состояния $|\phi^0\rangle_B$, $|\phi^1\rangle_B$ внутри одного базиса в общем случае могут быть неортогональными (см. ниже), т. е. достоверно неразличимыми. Измерения на приемной стороне даются разложениями единицы:

$$I_B = \sum_{y=1,1_?} \mathcal{M}_y, \quad \mathcal{M}_1 = I_B - |\phi^0\rangle_B \, {}_B\langle\phi^0|, \\ \mathcal{M}_{1_?} = |\phi^0\rangle_B \, {}_B\langle\phi^0|, \qquad (12)$$

$$I_B = \sum_{y=0,0_?} \mathcal{M}_y, \quad \mathcal{M}_0 = I_B - |\phi^1\rangle_B \, {}_B\langle\phi^1|, \\ \mathcal{M}_{0_?} = |\phi^1\rangle_B \, {}_B\langle\phi^1|. \qquad (13)$$

Измерения (12) и (13) имеют следующий смысл. Первое измерение (12) дает два исхода, причем исход с индексом «1» никогда не возникнет от состояния $|\phi^0\rangle_B$, а исход «0» — от состояния $|\phi^1\rangle_B$. Исход «$1_?$» может иметь место как от состояния $|\phi^0\rangle_B$, так и от состояния $|\phi^1\rangle_B$, т. е. является неопределенным (inconclusive). Аналогично для другого измерения (13). Исходы «$0_?$» и «$1_?$» отбрасываются. Если состояния внутри базиса ортогональны, то два различных измерения (12) и (13) вырождаются в одно измерение с двумя определенными исходами.

После измерений на приемной стороне Боба состояние (11) переходит в новое:

$$|x\rangle_A \otimes |y\rangle_B \otimes {}_B\langle y|\Psi^x\rangle_{BE}, \\ |\Psi^x\rangle_{BE} = U_{BE}(|\phi^x\rangle_B \otimes |E\rangle_E). \qquad (14)$$

Совместная матрица плотности Алисы, Боба и Евы в каждой посылке имеет вид

$$\sigma_E^{xy} = |x\rangle_A \, {}_A\langle x| \otimes |y\rangle_B \, {}_B\langle y| \otimes \\ \otimes \, {}_B\langle y|\Psi^x\rangle_{BE} \, {}_{BE}\langle\Psi^x|y\rangle_B. \qquad (15)$$

Соответствующая частичная матрица плотности Алисы и Боба в каждой посылке имеет вид

$$\sigma^{xy} = \lambda_{xy}|x\rangle_A \, {}_A\langle x| \otimes |y\rangle_B \, {}_B\langle y|, \\ \lambda_{xy} = \mathrm{Tr}_E\{{}_B\langle y|\Psi^x\rangle_{BE} \, {}_{BE}\langle\Psi^x|y\rangle_B\}. \qquad (16)$$

Полная совместная матрица плотности Алисы и Боба, описывающая корреляцию их результатов измерений, равна

$$\sigma_{XY} = \sum_{x,y} \lambda_{xy}|x\rangle_A \, {}_A\langle x| \otimes |y\rangle_B \, {}_B\langle y|, \qquad (17)$$

где λ_{xy} — собственные числа матрицы плотности (17).

Если бы не было подслушивателя, матрица плотности Алисы и Боба (17) описывала бы идеальные корреляции исходов измерений (т. е. битовая строка x Алисы равна битовой строке y Боба). Из-за действий подслушивателя строка Боба содержит ошибки. Матрица плотности (17) возникла в результате игнорирования степеней свободы Евы (взятия частичного следа по пространству $\mathcal{H}_E$), к которым Алиса и Боб не имеют доступа.

Матрицу плотности для дальнейшего рассмотрения удобно представить в диагональном виде, после случайных перестановок имеем

$$\sigma_{XY} = \sum_{i=0}^{3} \lambda_i |\Phi_i\rangle_{XY\ XY}\langle\Phi_i|, \tag{18}$$

где $|\Phi_i\rangle_{XY}$ — белловские состояния. Согласно теореме Наймарка [30], любой симметричный оператор может быть расширен до проектора в более широком пространстве. Применительно к нашей ситуации, любой статистический квантовый ансамбль в пространстве $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ может быть представлен как чистое состояние в более широком пространстве $\mathcal{H}_{ABE} = \mathcal{H}_{AB} \otimes \mathcal{H}_E$:

$$\begin{gathered}\sigma_{XYE} = |\Psi\rangle_{XYE\ XYE}\langle\Psi|, \\ |\Psi\rangle_{XYE} = \sum_{i=0}^{3} \sqrt{\lambda_i}|\Phi_i\rangle_{XY} \otimes |e_i\rangle_E,\end{gathered} \tag{19}$$

причем $|e_i\rangle_E$ — нормированные ортогональные состояния в пространстве $\mathcal{H}_E$. Ортогональность следует из того факта, что состояния $|\Phi_i\rangle_{XY}$ являются собственными состояниями матрицы плотности σ_{XY}, в этом случае разложение Шмидта гарантирует (см., например, [31]), что состояния $|e_i\rangle_E$ автоматически будут собственными состояниями матрицы плотности Евы $\sigma_E = \mathrm{Tr}_{XY}\{|\Psi\rangle_{XYE\ XYE}\langle\Psi|\}$. При этом ненулевые собственные числа матрицы плотности Евы совпадают с ненулевыми собственными числами совместной матрицы плотности Алиса–Боб (18). В представлении базисных векторов $|x\rangle_A \otimes |y\rangle_E$ с учетом (18) имеем

$$|\Psi\rangle_{XYE} = \sum_{x,y} |x\rangle_A \otimes |y\rangle_B \otimes |f^{xy}\rangle_E. \tag{20}$$

Здесь состояния $|f^{xy}\rangle_E$ уже не обязаны быть ортогональными, кроме того они ненормированы. Частичная матрица плотности Евы имеет вид

$$\sigma_E = \sum_{x,y} |f^{xy}\rangle_{EE}\langle f^{xy}|, \tag{21}$$

но с другой стороны, та же самая матрица плотности согласно (19), (20) имеет вид

$$\sigma_E = \sum_{x,y} {}_B\langle y|\Psi^x\rangle_{BEBE}\langle\Psi^x|y\rangle_B. \tag{22}$$

Соотношения (21) и (22) дают связь между функциями:

$${}_B\langle y|\Psi^x\rangle_{BE} = |f^{xy}\rangle_E. \tag{23}$$

Отсюда же может быть найдена совместная матрица плотности Алисы и Евы, которая фигурирует в критерии (5). С учетом (20) имеем

$$\sigma_{XE} = \sum_{x,y} |x\rangle_{AA}\langle x| \otimes |f^{xy}\rangle_{EB}\langle f^{xy}|. \tag{24}$$

Длина финального секретного ключа записывается в следующем эквивалентном (5) виде:

$$\begin{aligned}\frac{r}{n} = \min_{\sigma_{AB}\in\Gamma(\mathcal{M}_y,Q)} [(S(\sigma_{XE}) - S(\sigma_E)) - \\ - (S(\sigma_{XY}) - S(\sigma_Y))],\end{aligned} \tag{25}$$

где минимум находится по матрицам плотности Боба, измерения над которыми дают наблюдаемую ошибку Q. Таким образом, длина ключа выражается только через матрицы плотности Боба и подслушивателя, когда Алиса посылает выбранные состояния $|\phi^x\rangle_B$ непосредственно к Бобу.

2.3.1. Критерий секретности, основанный на границе Холево

В этом разделе найдем связь критерия секретности ключей с фундаментальной границей Холево [32]. Данная граница тесно связана со способностью безошибочной передачи классической информации при помощи квантовых состояний.

Количество классической информации в битах, которое может быть получено из ансамбля квантовых состояний $\{p_X(x), \sigma_B^x\}$ Бобом и из ансамбля $\{p_X(x), \sigma_E^x\}$ Евой, дается фундаментальной величиной (информацией) Холево $\chi(\sigma)$ [32][7]. Для Боба и Евы имеем соответственно

$$\begin{aligned}\chi(\sigma_B) = S(\sigma_B) - \sum_x p_X(x) S(\sigma_B^x), \\ \chi(\sigma_E) = S(\sigma_E) - \sum_x p_X(x) S(\sigma_E^x),\end{aligned} \tag{26}$$

где

$$\sigma_B = \sum_x p_X(x)\sigma_B^x, \quad \sigma_E = \sum_x p_X(x)\sigma_E^x.$$

Найдем связь величины Холево с критерием секретности. Матрица плотности Алисы, Боба и Евы после фиксации состояний Алисой имеет вид

$$\begin{gathered}\sigma_{ABE} = \sum_x p_X(x)|x\rangle_{A\,A}\langle x| \otimes \sigma_{BE}^x, \\ \sigma_{BE}^x = |\Psi^x\rangle_{BEBE}\langle\Psi^x|, \\ |\Psi^x\rangle_{BE} = U_{BE}(|\phi^x\rangle_B \otimes |E\rangle_E).\end{gathered} \tag{27}$$

Поскольку состояние (27) чистое, разложение Шмидта гарантирует, что собственные числа частичных матриц плотности

$$\sigma_B^x = \mathrm{Tr}_E\{\sigma_{BE}^x\}, \quad \sigma_E^x = \mathrm{Tr}_B\{\sigma_{BE}^x\} \tag{28}$$

[7] Здесь введены априорные вероятности $p_X(x)$, с которыми выбираются квантовые состояния. В протоколах квантового распределения ключей априорное распределение вероятностей отвечает равномерному распределению.

совпадают, т. е. имеют место спектральные разложения

$$\sigma_B^x = \sum_i d_i^x |d_i^x\rangle_{BB}\langle d_i^x|,$$
$$\sigma_E^x = \sum_i d_i^x |d_i^x\rangle_{EE}\langle d_i^x|, \tag{29}$$

где $|d_i^x\rangle_B$ и $|d_i^x\rangle_E$ — собственные векторы соответственно в пространствах $\mathcal{H}_B$ и $\mathcal{H}_E$, ненулевые собственные числа d_i^x совпадают, поэтому совпадают энтропии фон Неймана частичных матриц плотности, которые зависят только от собственных чисел. Имеем

$$S(\sigma_B^x) = S(\sigma_E^x). \tag{30}$$

Для длины ключа с учетом (5), (26) находим

$$\frac{r}{n} = \min_{\sigma_{AB}\in\Gamma(Q)} (S(\sigma_B) - S(\sigma_E)) = \min_{\sigma_{AB}\in\Gamma(Q)} (\chi(\sigma_B) - \chi(\sigma_E)), \tag{31}$$

где последнее равенство написано с учетом совпадения энтропий фон Неймана для частичных матриц плотности (28)–(30).

Граница Холево является достижимой и достигается на коллективных измерениях [32]. На сегодняшний день не предъявлено ни одного протокола квантового распределения ключей, для которого достигалась бы такая длина ключа. Это связано с тем, что на приемной стороне Боб обычно использует не коллективные, а индивидуальные измерения в некотором базисе $I_B = \sum_y |y\rangle_{BB}\langle y|$ (см. также формулы (12), (13)). Покажем теперь, что при индивидуальных измерениях на приемной стороне критерий (25) сводится к (31).

После измерений можно переписать матрицу плотности (17) в виде

$$\sigma_{XY} = \sum_{x,y} p_{XY}(x,y)|x\rangle\langle x| \otimes |y\rangle\langle y|,$$
$$p_{XY}(x,y) = p_X(x)\mathrm{Tr}_E\{{}_B\langle y|\Psi^x\rangle_{BE}\ {}_{BE}\langle\Psi^x|\rangle_B\}. \tag{32}$$

Соответственно частичная матрица плотности Боба после измерений равна

$$\sigma_Y = \mathrm{Tr}_X\{\sigma_{XY}\} = \sum_{x,y} p_{XY}(x,y)|y\rangle\langle y|. \tag{33}$$

Для энтропии фон Неймана с учетом соотношения (32) находим

$$S(\sigma_{XY}) = -\sum_{x,y} p_{XY}(x,y)\log_2 p_{XY}(x,y) = H(X,Y), \tag{34}$$

где $H(X,Y)$ — классическая энтропия Шеннона для совместного распределения Алисы и Боба. Далее с учетом формулы (33) получаем

$$S(\sigma_Y) = -\sum_y p_Y(y)\log_2 p_Y(y) = H(Y), \tag{35}$$

где $H(Y)$ — энтропия Шеннона для распределения на приемной стороне Боба. Энтропия фон Неймана для совместной матрицы плотности Алиса–Ева

$$\sigma_{XE} = \sum_{x,y} p_{XY}(x,y)|x\rangle\langle x| \otimes \sigma_E^{xy} = \sum_x p_X(x)|x\rangle\langle x| \otimes \sigma_E^x, \tag{36}$$

где

$$\sigma_E^{xy} = {}_B\langle y|\Psi^x\rangle_{BE}\ {}_{BE}\langle\Psi^x|\rangle_B,$$
$$\sigma_E^x = \sum_y p_{X|Y}(x|y)\sigma_E^{xy}, \tag{37}$$

имеет вид

$$S(\sigma_{XE}) = H(X) + \sum_x p_X(x)S(\sigma_E^x),$$
$$H(X) = -\sum_x p_X(x)\log_2 p_X(x). \tag{38}$$

Здесь $H(X)$ — классическая энтропия Шеннона от распределения на стороне Алисы. И наконец, запишем частичную матрицу плотности Евы

$$\sigma_E = \sum_x p_X(x)\sigma_E^x \tag{39}$$

и соответствующую энтропию фон Неймана

$$S(\sigma_E) = S\left(\sum_x p_X(x)\sigma_E^x\right). \tag{40}$$

Критерий (25) с учетом формул (34), (35), (38) теперь может быть записан в следующем виде:

$$\frac{r}{n} = \min_{\sigma_X\in\Gamma(Q)} (I(X;Y) - \chi(\sigma_E)), \tag{41}$$

$$I(X;Y) = H(X) + H(Y) - H(X,Y),$$
$$\chi(\sigma_E) = S\left(\sum_x p_X(x)\sigma_E^x\right) - \sum_x p_X(x)S(\sigma_E^x).$$

Здесь $I(X;Y)$ — взаимная информация Алиса–Боб.

Таким образом, критерий секретности, основанный на фундаментальной границе Холево [32], при индивидуальных измерениях на приемной стороне и коллективных измерениях Евы совпадает с (25) и (31).

2.3.2. Связь критерия секретности с классическими пропускными способностями квантового канала связи

Ситуация между участниками протокола может быть переведена на язык классических пропускных способностей квантового канала связи. Кодирование на передающей стороне происходит индивидуально в каждой посылке. Квантовый канал связи между передающей и приемной сторонами описывается вполне положительным отображением (инструментом) [31, 33, 34] как

$$\{p_X(x), \sigma_A^x = |\phi^x\rangle_{A\,A}\langle\phi^x|\} \to \{p_X(x), \sigma_B^x\}, \quad \sigma_B^x = \mathcal{T}_{B\leftarrow A}(\sigma_A^x), \tag{42}$$

где квантовый канал связи Алиса–Боб ($\mathcal{T}_{B\leftarrow A}$) определяется соотношением

$$\mathcal{T}_{B\leftarrow A}(|\phi^x\rangle_{A\,A}\langle\phi^x|) = \mathrm{Tr}_E\{|\Psi^x\rangle_{BE\;\;BE}\langle\Psi^x|\}. \tag{43}$$

Аналогично квантовый канал Алиса–Ева

$$\{p_X(x), |\phi^x\rangle_{A\,A}\langle\phi^x|\} \to \{p_X(x), \sigma_E^x\}, \quad \sigma_E^x = \mathcal{T}_{E\leftarrow A}(\sigma_A^x), \tag{44}$$

задается инструментом $\mathcal{T}_{E\leftarrow A}$:

$$\mathcal{T}_{E\leftarrow A}(|\phi^x\rangle_{A\,A}\langle\phi^x|) = \mathrm{Tr}_B\{|\Psi^x\rangle_{BE\;\;BE}\langle\Psi^x|\}. \tag{45}$$

Оба квантовых канала связи связаны унитарным оператором Евы:

$$|\Psi^x\rangle_{BE} = U_{BE}(|\phi^x\rangle_B \otimes |E\rangle_E). \tag{46}$$

Согласно работам [35, 36] существует целое многообразие классических пропускных способностей квантового канала связи, которые обозначаются как $C_{k,m}(\mathcal{T})$, где $k, m = 1, \ldots, \infty$. Индекс «k» отвечает за способ кодирования на передающей стороне, индекс «m» — за способ декодирования на принимающей стороне.

Пропускная способность $C_{1,1}(\mathcal{T})$ «за один шаг» отвечает ситуации, когда классическая информация кодируется в индивидуальные квантовые состояния в каждой посылке и декодируется при помощи оптимальных индивидуальных квантовомеханических измерений в каждой посылке. Под оптимальными индивидуальными измерениями понимаются измерения, которые минимизируют ошибку различения квантовых состояний. Пропускная способность $C_{1,\infty}(\mathcal{T})$ отвечает за индивидуальное кодирование на передающей стороне в каждой посылке и декодирование всей переданной последовательности квантовых состояний как целого (коллективные измерения). Такие оптимальные измерения минимизируют ошибку различения всей кодовой последовательности квантовых состояний. Данные коллективные измерения требуют использования запутанных состояний.

Имеют место следующие соотношения между различными классическими пропускными способностями квантовых каналов связи [37]:

$$\begin{array}{ccc} C_{\infty,1}(\mathcal{T}) & \overset{<}{\neq} & C_{\infty,\infty}(\mathcal{T}) \\ \| & & ? \\ C_{1,1}(\mathcal{T}) & \overset{<}{\neq} & C_{1,\infty}(\mathcal{T}). \end{array} \tag{47}$$

Одношаговая пропускная способность $C_{1,1}(\mathcal{T})$ меньше, чем величина $C_{1,\infty}(\mathcal{T})$ (обозначаемая чаще как $\overline{C}(\mathcal{T})$). Неформально говоря, это означает, что оптимальные коллективные измерения, минимизирующие ошибку различения целых переданных последовательностей длины n (при $n \to \infty$), оказываются более выгодными, поскольку позволяют извлечь большее количество информации, чем индивидуальные измерения над отдельными квантовыми состояниями. Кроме того, $C_{1,1}(\mathcal{T}) \leq C_{1,m}(\mathcal{T})$ ($m = 2, 3, \ldots, \infty$), т. е. оптимальное различение кодовых блоков из m состояний на принимающей стороне также позволяет извлечь большее количество информации, чем оптимальные индивидуальные измерения.

Известно также, что $C_{1,1}(\mathcal{T}) = C_{\infty,1}(\mathcal{T})$ [32], т. е. кодирование информации в целые последовательности, а затем оптимальные индивидуальные измерения на принимающей стороне не увеличивают количество извлекаемой классической информации из ансамбля квантовых состояний. И наконец, соотношение $C_{\infty,1}(\mathcal{T}) \leq C_{\infty,\infty}(\mathcal{T})$ означает, что имеет место кодирование при помощи запутанных состояний целой передаваемой последовательности квантовых состояний, и коллективные измерения для различения всей последовательности состояний как кодового слова позволяют передать максимум классической информации при помощи квантового ансамбля [32, 37].

Классическая пропускная способность квантового канала связи для оптимальных коллективных измерений на выходе совпадает с информацией Холево [32]:

$$\overline{C}(\mathcal{T}) = C_{1,\infty}(\mathcal{T}) = \chi(\sigma) = \\ = \max_{p_X(x)} \left(S(\mathcal{T}(\sigma)) - \sum_x p_X(x) S(\mathcal{T}(\sigma^x)) \right), \quad (48) \\ \sigma = \sum_x p_X(x)\sigma^x,$$

где максимум берется по всевозможным входным распределениям априорных вероятностей.

Вернемся к квантовой криптографии. Все известные практически реализуемые квантовые протоколы распределения ключей используют индивидуальное кодирование на передающей стороне и индивидуальные измерения Бобом на приемной стороне. Ева может использовать любые, в том числе и коллективные, измерения; в этом случае с учетом формул (42)–(45) и (5) критерий секретности принимает вид

$$\frac{r}{n} = \min_{\sigma_{AB} \in \Gamma(\mathcal{M}_y, Q)} (C_{1,1}(\mathcal{T}_{B\leftarrow A}(\sigma_A)) - \\ - C_{1,\infty}(\mathcal{T}_{E\leftarrow A}(\sigma_A))). \quad (49)$$

Часто также используется критерий секретности ключей, введенный в работе [38] еще до появления квантовой криптографии. Данный критерий применительно к протоколу квантового распределения ключей, записывается как

$$\frac{r}{n} = \min_{\text{all attack} \to \Gamma(Q)} (I(X;Y) - I(X;Y_E)), \quad (50)$$

где $I(X;Y_E)$ — взаимная информация Алиса–Ева, Y_E — битовая строка Евы. Минимизация происходит по всем атакам Евы, которые дают наблюдаемую ошибку Q на приемной стороне Боба.

Взаимная информация $I(X;Y)$ ограничена величиной Холево для ансамбля, который после индивидуальных измерений описывается матрицей плотности (32) и (33). После измерений на стороне Боба канал Алиса–Боб становится классическим каналом без памяти. Для такого канала связи информация Холево достигается на индивидуальных измерениях и равна пропускной способности этого канала связи, которая для бинарного алфавита равна $C(Q)$. Максимум взаимной информации для Евы в критерии (50) ограничен величиной Холево для квантового ансамбля (39), причем данный максимум достигается на коллективных измерениях Евы и является по сути классической пропускной способностью квантового канала Алиса–Ева. При этом оба канала Алиса–Боб и Алиса–Ева связаны через унитарный оператор Евы (43), (45).

Таким образом, все критерии секретности ключей (25), (39), (41) и (50) эквивалентны. В зависимости от ситуации бывает удобнее пользоваться той или иной формой критерия. Приведем содержательный пример такого использования для нового протокола распределения ключей.

Для бинарного алфавита $x = 0, 1$ одношаговая пропускная способность $C_{1,1}(\mathcal{T}_{B\leftarrow A}(\sigma_A))$ превращается в пропускную способность классического бинарного симметричного канала связи с ошибкой Q:

$$C_{1,1}(\mathcal{T}_{B\leftarrow A}(\sigma_A)) = C(Q) = 1 - h(Q), \quad (51)$$

причем максимум достигается при равномерном распределении априорных вероятностей, что окончательно, с учетом (49) и (51) дает

$$\frac{r}{n} = \min_{\sigma_{AB} \in \Gamma(Q)} \left(C(Q) - \overline{C}(\sigma_E) \right). \quad (52)$$

Минимум берется по матрицам плотности σ_{BE}, измерения над которыми дают ошибку Q на принимающей стороне.

2.3.3. Бесконечное множество атак Евы

Отметим, что из формул (47), (49) следует существование бесконечного множества атак Евы на передаваемый ключ, которые параметризуются унитарным оператором U_{BE} и отличаются только измерениями Евы на конечной стадии протокола. Длина ключа для случая оптимального различения Евой блоков из k состояний дается соотношением

$$\frac{r}{n}(k) = \min_{\sigma_{AB} \in \Gamma(\mathcal{M}_y, Q)} (C_{1,1}(\mathcal{T}_{B\leftarrow A}(\sigma_A)) - \\ - C_{1,k}(\mathcal{T}_{E\leftarrow A}(\sigma_A))), \quad k = 1, \ldots, \infty,$$

причем длина ключа является убывающей функцией k, соответственно, допустимая критическая ошибка, до которой можно передавать секретные ключи, также убывает с ростом k. Здесь k означает размер блока, над которым Ева может проводить коллективные измерения. Допустимая критическая ошибка, до которой гарантируется секретность передаваемых ключей, зависит от вида измерений Евы. Например, для протокола BB84 [39] коллективные измерения Евы дают

$$\min_{\sigma_{AB} \in \Gamma(\mathcal{M}_y, Q)} C_{1,\infty}(\mathcal{T}_{E\leftarrow A}(\sigma_A)) = h(Q),$$

где

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

— бинарная энтропийная функция.

Для индивидуальных измерений получаем

$$\min_{\sigma_{AB}\in\Gamma(\mathcal{M}_y,Q)} C_{1,1}(\mathcal{T}_{E\leftarrow A}(\sigma_A)) =$$

$$= \frac{1}{2}\left[\left(1-\sqrt{1-\varepsilon^2(Q)}\right)\log_2\left(1-\sqrt{1-\varepsilon^2(Q)}\right) + \right.$$

$$\left. + \left(1+\sqrt{1-\varepsilon^2(Q)}\right)\log_2\left(1+\sqrt{1-\varepsilon^2(Q)}\right)\right],$$

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

Критические ошибки в этих случаях приблизительно равны 11 % и 15 % соответственно. Все остальное множество атак Евы при $k \neq 1$ и $k \neq \infty$ дает критическую ошибку, находящуюся в интервале $11\,\% < Q_c < 15\,\%$.

При коллективных измерениях подслушивателя допустимая критическая ошибка, до которой можно гарантировать секретность ключей, оказывается меньше, чем при индивидуальных измерениях. Коллективные измерения Евы позволяют извлечь больше информации, чем индивидуальные при той же самой величине возмущения передаваемых состояний (наблюдаемой ошибке Q). При произвольных значениях k соответствующую классическую пропускную способность квантового канала связи Алиса–Ева

$$\min_{\sigma_{AB}\in\Gamma(\mathcal{M}_y,Q)} (C_{1,k}(\mathcal{T}_{E\leftarrow A}(\sigma_A)))$$

можно вычислить лишь численно.

3. ДВУХПАРАМЕТРИЧЕСКИЕ ПРОТОКОЛЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

В этом разделе будет исследована стойкость нового протокола квантового распределения ключей. Идея данного протокола была предложена в работе [40], где также приведена оптоволоконная реализация такой системы квантовой криптографии. Данный протокол относится к новому семейству так называемых двухпараметрических протоколов и отличается от всех предыдущих систем квантовой криптографии тем, что позволяет передавать ключи с гарантией их секретности вплоть до ошибки $Q_c \to 50\,\%$. Напомним, что ошибка 50 % является теоретическим пределом для бинарного классического симметричного канала связи, до которой вообще возможна безошибочная передача информации в пределе длинных последовательностей.

Все исследованные до настоящего времени протоколы квантового распределения ключей являются однопараметрическими. Под этим понимается то, что детектирование любых попыток подслушивания на приемной стороне происходит по одному параметру — ошибке Q, поэтому для таких систем квантовой криптографии теоретический предел по ошибке в 50 % принципиально недостижим, несмотря на любые ухищрения, предпринятые в ряде работ. Этот факт можно усмотреть из формулы (45). Действительно, пропускная способность классического симметричного бинарного канала связи $C(Q)$, как известно [12, 13], является убывающей функцией Q ($C(Q=0)=1$ и $C(Q=1/2)=0$). Поскольку Ева всегда может получить хоть какую-то информацию из квантового канала связи, классическая пропускная способность квантового канала связи Алиса–Ева $\overline{C}(\sigma_E)$ в формуле (45) строго больше нуля. Поэтому длина ключа r в (52) обращается в нуль ($C(Q_c) = \overline{C}(\sigma_E) > 0$) при ошибке $Q_c < 50\,\%$. Физическая причина этого заключается в том, что в однопараметрических протоколах информация Евы о ключе зависит от ошибки Q: чем больше ошибка на приемной стороне Боба, тем больше информации получает Ева о ключе. Функция $\min_{\sigma_{AB}\in\Gamma(Q)} \overline{C}(\sigma_E)$ в формуле (52) является растущей функцией Q, что по существу является следствием соотношений неопределенностей по «переменным» информация–ошибка.

В двухпараметрическом протоколе для детектирования возмущения передаваемых квантовых состояний используется пара переменных — ошибка Q и вероятность отсчетов в контрольных временных окнах q. При этом классические пропускные способности квантовых каналов Алиса–Боб и Алиса–Ева начинают зависеть от двух переменных Q, q, поэтому возникают не интервалы по ошибке $0 < Q < Q_c$, где возможно секретное распределение ключей, как для однопараметрических протоколов, а целые области на плоскости параметров (Q, q).

3.1. Ортогональные состояния внутри базисов

Перейдем к исследованию стойкости протокола (подробности оптоволоконной реализации см. в работе [40]).

В протоколе используются четыре базиса и восемь однофотонных информационных состояний. Каждое однофотонное состояние в «левом» базисе (рис. 1) представляет собой суперпозицию двух состояний, локализованных во временных окнах 1 и 2 (рис. 1). Квантовые состояния в базисах $+L$, $\times L$ имеют вид

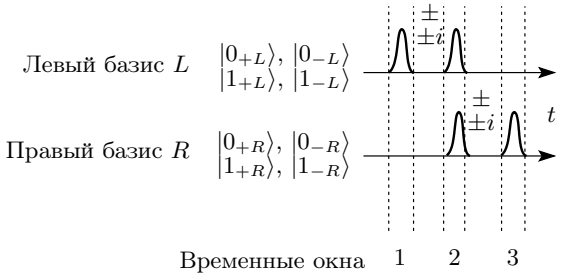

Рис. 1. Временная структура информационных состояний

$$|0^{+L}\rangle = \frac{1}{\sqrt{2}}(|1\rangle+|2\rangle), \quad |1^{+L}\rangle = \frac{1}{\sqrt{2}}(|1\rangle-|2\rangle), \quad (53)$$

$$|0^{\times L}\rangle = \frac{1}{\sqrt{2}}(|1\rangle+i|2\rangle), \quad |1^{\times L}\rangle = \frac{1}{\sqrt{2}}(|1\rangle-i|2\rangle). \quad (54)$$

Соответственно состояния в «правом» базисе (рис. 1) представляют собой суперпозицию состояний, локализованных во временных окнах 2 и 3, и устроены аналогично состояниям в «левом» базисе. Для базисов $+R$, $\times R$ имеем

$$|0^{+R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle+|3\rangle), \quad |1^{+R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle-|3\rangle), \quad (55)$$

$$|0^{\times R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle+i|3\rangle), \quad |1^{\times R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle-i|3\rangle). \quad (56)$$

Здесь $|i\rangle$ $(i = 1, 2, 3)$ — локализованные состояния во временных окнах 1, 2, 3, которые сдвинуты по времени на одинаковую величину (см. детали в работе [40])).

Состояния из различных базисов L и R попарно неортогональны. Внутри одного базиса состояния ортогональны.

Нетрудно заметить, что внутри базиса L информационные состояния устроены так же, как и в известном протоколе BB84 [3], а структура любой пары состояний из базисов L и R аналогична протоколу B92 [3], использующему пару неортогональных состояний. Такая комбинация состояний, как будет видно ниже, приводит к нетривиальным следствиям.

3.1.1. Вычисление критической ошибки с использованием запутанных состояний

Рассмотрим сначала версию протокола квантового распределения ключей, использующего запутанные состояния. Шаги протокола аналогичны описанным в разд. 2.2. Алиса случайно и равновероятно готовит одно из восьми состояний:

$$|\Phi^{+,\times L,R}\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0^{+,\times L,R}\rangle_A \otimes |0^{+,\times L,R}\rangle_B + \right.$$

$$\left. + |1^{+,\times L,R}\rangle_A \otimes |1^{+,\times L,R}\rangle_B\right), \quad (57)$$

и направляет подсистему B на приемную сторону, подсистема A остается на передающей стороне.

После передачи всей последовательности Алиса и Боб осуществляют случайную согласованную перестановку состояний в различных посылках, а затем проводят измерения над своими подсистемами в согласованных базисах. Согласование базисов происходит через открытый канал связи. Измерения на передающей и приемной сторонах описываются следующими разложениями единицы в пространстве $\mathcal{H}_A \otimes \mathcal{H}_B$. В левых базисах имеем

$$I_A^L \otimes I_B =$$

$$= \sum_{x=0^{+,\times},1^{+,\times};\ y=0^{+,\times},1^{+,\times},3} \mathcal{M}_x^{A\ L} \otimes \mathcal{M}_y^{B\ L}, \quad (58)$$

$$\mathcal{M}_x^{A\ L} = |x^L\rangle_{AA}\langle x^L|,$$

$$\mathcal{M}_y^{B\ L} = |y^L\rangle_{BB}\langle y^L| \quad \text{при } y = 0^{+,\times}, 1^{+,\times}, \quad (59)$$

$$\mathcal{M}_3^{B\ L} = |3\rangle_{BB}\langle 3|,$$

в правых базисах —

$$I_A^R \otimes I_B =$$

$$= \sum_{x=0^{+,\times},1^{+,\times};\ y=0^{+,\times},1^{+,\times},1} \mathcal{M}_x^{A\ R} \otimes \mathcal{M}_y^{B\ R}, \quad (60)$$

$$\mathcal{M}_x^{A\ R} = |x^R\rangle_{AA}\langle x^R|,$$

$$\mathcal{M}_y^{B\ R} = |y^R\rangle_{BB}\langle y^R| \quad \text{при } y = 0^{+,\times}, 1^{+,\times}, \quad (61)$$

$$\mathcal{M}_1^{B\ R} = |1\rangle_{BB}\langle 1|.$$

В (58)–(60) единичные операторы, относящиеся к левым и правым базисам в представлении базисных векторов в трех временных окнах (рис. 1), равны в пространстве $\mathcal{H}_B$

$$I_B = |1\rangle_{BB}\langle 1| + |2\rangle_{BB}\langle 2| + |3\rangle_{BB}\langle 3|,$$

в пространстве $\mathcal{H}_A$

$$I_A^L = |1\rangle_{A\,A}\langle 1| + |2\rangle_{A\,A}\langle 2|, \quad I_A^R = |2\rangle_{A\,A}\langle 2| + |3\rangle_{A\,A}\langle 3|.$$

Данные измерения имеют простой физический смысл. Если нет подслушивателя, измерения в согласованном базисе, например в левом, дадут полностью коррелированные исходы у Алисы и Боба. При таких измерениях у Алисы и Боба случайно, равновероятно, но полностью согласованно может возникнуть либо 0, либо 1. Ева, которая не знает, в каком базисе приготовлена подсистема B (левом или правом) из-за неортогональности состояний в левом и правом базисах будет неизбежно ошибаться (путать состояния из левого и правого базисов), что приведет к появлению отсчетов во временном окне 3 (ошибка q), которых при невозмущенных состояниях в левом базисе никогда не должно быть. Кроме того, поскольку Ева также не может достоверно различить состояния внутри левого базиса для $+L$ и $\times L$, это приведет еще и к ошибкам в информационной последовательности 0 и 1 у Боба (ошибка Q). Таким образом, кроме ошибки в информационной последовательности 0 и 1 возникают отсчеты в контрольном временном окне 3 для левого базиса и соответственно во временном окне 1 для правого базиса. Вероятность таких ошибочных отсчетов в контрольных временных окнах, q, является вторым параметром протокола, по которому также детектируются попытки подслушивания.

Дальнейшей задачей будет получение критерия секретности для распределения ключей с учетом этих двух параметров. Поскольку ситуация симметрична для различных базисов, дальше можно рассматривать состояния только в одном из них. Возмущенная подслушивателем матрица плотности, например, произошедшая из состояний в левом базисе, может быть разложена по линейно независимым операторам вида $|i\rangle_{A\,A}\langle j| \otimes |k\rangle_{B\,B}\langle m|$, где $i, j = 1, 2$ и $k, m = 1, 2, 3$. Из-за того, что измерения (58)–(60) диагональны по состояниям в контрольных временных окнах ($|3\rangle_{B\,B}\langle 3|$ в левом, $|1\rangle_{B\,B}\langle 1|$ в правом базисе), матрицу плотности $\sigma_{AB}^{L,R}$ сразу можно записать в диагональном виде по состояниям в контрольных временных окнах.

Нетрудно проверить явными вычислениями, что любая матрица плотности Алисы и Боба в пространстве $\mathcal{H}_A^{L,R} \otimes \mathcal{H}_B$ после случайных перестановок принимает вид (далее индексы «+», «×» у 0 и 1 из-за симметрии относительно 0 и 1 в разных базисах для сокращения обозначений опускаем)

$$\begin{aligned}\sigma_{AB}^{L,R} = \frac{1}{4} \times \\ \times \sum_{\sigma_i^{L,R} = I^{L,R}, \sigma_x^{L,R}, \sigma_y^{L,R}, \sigma_z^{L,R}} \left(\sigma_i^{L,RA} \sigma_i^{L,RB}\right) \times \\ \times \sigma_{AB}^{L,R} \left(\sigma_i^{L,RA} \sigma_i^{L,RB}\right) = \\ = \sum_{i=0}^{3} \lambda_i^{L,R} |\Phi_i^{L,R}\rangle_{AB\ AB}\langle\Phi_i^{L,R}| + \frac{q}{2} \times \\ \times \begin{cases} (|0^L\rangle_{A\,A}\langle 0^L| + |1^L\rangle_{A\,A}\langle 1^L|) \otimes |3\rangle_{B\,B}\langle 3|, \\ (|0^R\rangle_{A\,A}\langle 0^R| + |1^R\rangle_{A\,A}\langle 1^R|) \otimes |1\rangle_{B\,B}\langle 1|. \end{cases} \end{aligned} \quad (62)$$

Здесь $\sigma_{x,y,z}^{L,R}$ — матрицы Паули, действующие на состояния $|1\rangle$, $|2\rangle$ с индексом L и на состояния $|2\rangle$, $|3\rangle$ с индексом R, $\lambda_i^{L,R}$ и q — коэффициенты разложения, которые подлежат определению. Величина q, как упоминалось выше, отвечает за вероятность появления отсчетов в контрольных временных окнах. Далее, как обычно, введены обозначения белловских состояний:

$$|\Phi_0^{L,R}\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|0^{L,R}\rangle_A \otimes |0^{L,R}\rangle_B + |1^{L,R}\rangle_A \otimes |1^{L,R}\rangle_B\right), \quad (63)$$

$$|\Phi_1^{L,R}\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|0^{L,R}\rangle_A \otimes |0^{L,R}\rangle_B - |1^{L,R}\rangle_A \otimes |1^{L,R}\rangle_B\right), \quad (64)$$

$$|\Phi_2^{L,R}\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|0^{L,R}\rangle_A \otimes |1^{L,R}\rangle_B + |1^{L,R}\rangle_A \otimes |0^{L,R}\rangle_B\right), \quad (65)$$

$$|\Phi_3^{L,R}\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|0^{L,R}\rangle_A \otimes |1^{L,R}\rangle_B - |1^{L,R}\rangle_A \otimes |0^{L,R}\rangle_B\right). \quad (66)$$

Состояние (62) произошло из-за действий Евы и получено взятием частичного следа по степеням свободы в $\mathcal{H}_E$. Из теоремы Наймарка о расширении симметричных операторов [30] следует, что любая матрица плотности, отвечающая смешанному состоянию, может быть представлена в виде чистого состояния в более широком пространстве, в нашем случае — в $\mathcal{H}_A^{L,R} \otimes \mathcal{H}_B \otimes \mathcal{H}_E$. Причем частичный след (игнорирование степеней свободы в $\mathcal{H}_E$) даст исходную матрицу плотности. Совместное запутанное чистое состояние Алиса–Боб–Ева с учетом (55) имеет вид

$$|\Psi^{L,R}\rangle_{ABE}=\sum_{i=0}^{3}\sqrt{\lambda_i^{L,R}}|\Phi_i^{L,R}\rangle_{AB}\otimes|e_i^{L,R}\rangle_E+\sqrt{\frac{q}{2}}\times$$
$$\times\begin{cases}|0\rangle_A\otimes|3\rangle_B\otimes|q_0^L\rangle_E+|1\rangle_A\otimes|3\rangle_B\otimes|q_1^L\rangle_E,\\ |0\rangle_A\otimes|1\rangle_B\otimes|q_0^R\rangle_E+|1\rangle_A\otimes|1\rangle_B\otimes|q_1^R\rangle_E.\end{cases}\quad(67)$$

Состояния Евы $|e_i^L\rangle_E$ ($|e_i^R\rangle_E$), $i=0,1,2,3$, а также состояния $|q_0^L\rangle_E$ и $|q_1^L\rangle_E$ ($|q_0^R\rangle_E$ и $|q_1^R\rangle_E$) автоматически оказываются ортогональными. Это следует из разложения Шмидта [31], поскольку матрица плотности в формуле (62) сразу записана в диагональном представлении.

Поскольку измерения Алисы и Боба описываются ортогональными разложениями единицы (58)–(60), удобно перейти к представлению чистого состояния (67) в ортогональном базисе измерений. Имеем

$$|\Psi^{L,R}\rangle_{ABE}=$$
$$=\sum_{x,y=0,1}|x^{L,R}\rangle_A\otimes|y^{L,R}\rangle_B\otimes|f_{L,R}^{xy}\rangle_E+\sqrt{\frac{q}{2}}\times$$
$$\times\begin{cases}|0^L\rangle_A\otimes|3\rangle_B\otimes|q_0^L\rangle_E+|1^L\rangle_A\otimes|3\rangle_B\otimes|q_1^L\rangle_E,\\ |0^R\rangle_A\otimes|1\rangle_B\otimes|q_0^R\rangle_E+|1^R\rangle_A\otimes|1\rangle_B\otimes|q_1^R\rangle_E,\end{cases}\quad(68)$$

где введены обозначения

$$|f_{L,R}^{00}\rangle=\sqrt{\frac{\lambda_0^{L,R}}{2}}|e_0^{L,R}\rangle_E+\sqrt{\frac{\lambda_1^{L,R}}{2}}|e_1^{L,R}\rangle_E,$$
$$|f_{L,R}^{11}\rangle=\sqrt{\frac{\lambda_0^{L,R}}{2}}|e_0^{L,R}\rangle_E-\sqrt{\frac{\lambda_1^{L,R}}{2}}|e_1^{L,R}\rangle_E,\quad(69)$$

$$|f_{L,R}^{01}\rangle=\sqrt{\frac{\lambda_1^{L,R}}{2}}|e_0^{L,R}\rangle_E+\sqrt{\frac{\lambda_2^{L,R}}{2}}|e_1^{L,R}\rangle_E,$$
$$|f_{L,R}^{10}\rangle=\sqrt{\frac{\lambda_1^{L,R}}{2}}|e_0^{L,R}\rangle_E-\sqrt{\frac{\lambda_2^{L,R}}{2}}|e_1^{L,R}\rangle_E.\quad(70)$$

Амплитуды $|f_{L,R}^{xy}\rangle_E$ в формулах (69), (70) имеют простой физический смысл. Величина $\|f_{L,R}^{xy}\rangle_E|^2$ является вероятностью того, что Алиса зарегистрирует значения бита x, а Боб зарегистрирует значение бита y. При этом вероятность ошибки подсчитывается как

$$Q=\sum_{x\neq y;x,y=0,1}\|f_{L,R}^{xy}\rangle_E|^2,$$

что позволяет связать наблюдаемую ошибку Q на приемной стороне с собственными числами $\lambda_i^{L,R}$. Кроме того, существует вероятность того, что Алиса зарегистрирует значения бита $x=0,1$, например, в базисе L, а у Боба возникнет отсчет в контрольном временном окне 3 там, где его никогда не должно было быть, если бы состояние не было возмущено Евой. Вероятность отсчета в контрольном временном окне равна $q/2$ (68). Аналогично для состояний в правом базисе — из-за подслушивания появятся отсчеты в контрольном временном окне 1. Посылки, в которых возникли отсчеты в контрольных временных окнах, затем отбрасываются и служат только для определения величины q.

Для вычисления длины финального секретного ключа по формуле (5) потребуются частичные матрицы плотности, которые могут быть получены взятием частичного следа от состояния (68). Для матрицы плотности Алисы и Боба имеем

$$\sigma_{XY}^{L,R}=\mathrm{Tr}_E\{|\Psi^{L,R}\rangle_{ABE\ ABE}\langle\Psi^{L,R}|\}=$$
$$=\sum_{x,y=0,1}|x^{L,R}\rangle_{A\,A}\langle x^{L,R}|\otimes$$
$$\otimes|y^{L,R}\rangle_{B\,B}\langle y^{L,R}|\mathrm{Tr}\{|f_{L,R}^{xy}\rangle_{E\,E}\langle f_{L,R}^{xy}|\}+$$
$$+\frac{q}{4}\begin{cases}(|0^L\rangle_{A\,A}\langle 0^L|+|1^L\rangle_{A\,A}\langle 1^L|)\otimes|3\rangle_{B\,B}\langle 3|,\\ |0^R\rangle_{A\,A}\langle 0^R|+|1^R\rangle_{A\,A}\langle 1^R|)\otimes|1\rangle_{B\,B}\langle 1|.\end{cases}\quad(71)$$

Частичная матрица плотности Алисы и Евы имеет вид

$$\sigma_{XE}^{L,R}=\mathrm{Tr}_B\{|\Psi^{L,R}\rangle_{ABE\ ABE}\langle\Psi^{L,R}|\}=$$
$$=\sum_{x,y=0,1}|x^{L,R}\rangle_{A\,A}\langle x^{L,R}|\otimes|f_{L,R}^{xy}\rangle_{E\,E}\langle f_{L,R}^{xy}|+\frac{q}{4}\times$$
$$\times\begin{cases}|0^L\rangle_{A\,A}\langle 0^L|\otimes|q_0^L\rangle_{B\,B}\langle q_0^L|+\\ \qquad+|1^L\rangle_{A\,A}\langle 1^L|\otimes|q_1^L\rangle_{B\,B}\langle q_1^L|,\\ |0^R\rangle_{A\,A}\langle 0^R|\otimes|q_0^R\rangle_{B\,B}\langle q_0^R|+\\ \qquad+|1^R\rangle_{A\,A}\langle 1^R|\otimes|q_1^R\rangle_{B\,B}\langle q_1^R|.\end{cases}\quad(72)$$

После измерений (58)–(60) и отбрасывания посылок, в которых получены отсчеты в контрольных временных окнах, редуцированная матрица плотности всех участников протокола принимает вид

$$\overline{\sigma}_{XYE}^{L,R}=\sum_{x,y=0,1}|x\rangle_{A\,A}\langle x|\otimes|y\rangle_{B\,B}\langle y|\otimes\overline{\sigma}_E^{L,Rxy},\quad(73)$$

где $\overline{\sigma}_E^{L,Rxy}$ имеет такую же структуру, как и первое слагаемое в (72), но с заменой собственных чисел

$$\lambda_i\to\overline{\lambda}_i=\frac{\lambda_i}{1-q/2}.\quad(74)$$

Поскольку ситуация симметрична по отношению к различным базисам, собственные числа не должны зависеть от выбора базисов Алисой и Бобом, поэтому индексы базисов опущены. Формула (73) отража-

ет тот факт, что после отбрасывания посылок с отсчетами в контрольных временных окнах редуцированная матрица плотности нормирована на информационные временные окна. Для энтропии фон Неймана с учетом (73) находим

$$S(\sigma_{XE}) = 1 + h(\overline{\lambda}_0 + \overline{\lambda}_1), \tag{75}$$

$$S(\sigma_E) = h(\overline{\lambda}_0 + \overline{\lambda}_1) + (\overline{\lambda}_0 + \overline{\lambda}_1)h\left(\frac{\overline{\lambda}_0}{\overline{\lambda}_0 + \overline{\lambda}_1}\right) + \\ + (\overline{\lambda}_2 + \overline{\lambda}_3)h\left(\frac{\overline{\lambda}_2}{\overline{\lambda}_2 + \overline{\lambda}_3}\right), \tag{76}$$

$$S(\sigma_{XY}|\sigma_Y) = h(\overline{\lambda}_0 + \overline{\lambda}_1). \tag{77}$$

Для длины финального секретного ключа имеем

$$\frac{r}{n} = 1 + h(\overline{\lambda}_0 + \overline{\lambda}_1) - (\overline{\lambda}_0 + \overline{\lambda}_1)h\left(\frac{\overline{\lambda}_0}{\overline{\lambda}_0 + \overline{\lambda}_1}\right) - \\ - (\overline{\lambda}_2 + \overline{\lambda}_3)h\left(\frac{\overline{\lambda}_2}{\overline{\lambda}_2 + \overline{\lambda}_3}\right). \tag{78}$$

Остается определить связь собственных чисел с наблюдаемой вероятностью ошибки Q и вероятностью отсчетов в контрольных временных окнах q. Одно условие очевидно и следует из нормировки матрицы плотности (62), (73):

$$\lambda_0+\lambda_1+\lambda_2+\lambda_3 = 1-\frac{q}{2}, \quad \overline{\lambda}_0+\overline{\lambda}_1+\overline{\lambda}_2+\overline{\lambda}_3 = 1. \tag{79}$$

Из симметрии относительно 0 и 1 следует, что

$$\lambda_0 = (1-q)(1-Q), \quad \lambda_1 = \frac{q}{2}(1-Q), \\ \lambda_2 = (1-q)Q, \quad \lambda_3 = \frac{q}{2}Q. \tag{80}$$

Далее, если ввести величину

$$\zeta = \frac{q/2}{1-q/2}, \tag{81}$$

которая имеет смысл отношения числа отсчетов в контрольных временных окнах к числу отсчетов в информационных временных окнах, то формула (25) для длины ключа принимает особенно простой вид:

$$\frac{r}{n} = 1 - h(Q) - h(\zeta). \tag{82}$$

Критические значения наблюдаемых параметров Q и ζ, до которых возможно распределение секретных ключей, находятся из условия обращения в нуль длины ключа, $r = 0$, которое дает целую область на плоскости (Q, ζ). Обсуждение смысла данной формулы будет удобнее сделать несколько позднее.

3.1.2. Вычисление критической ошибки с использованием критерия, основанного на границе Холево

В предыдущем разделе была рассмотрена стойкость квантового распределения ключей, когда Алиса использует запутанное состояние из двух подсистем. В реальных оптоволоконных системах обычно используются состояния одной подсистемы, т. е. Алиса готовит одно из состояний (53)–(56) и напрямую посылает на приемную сторону. Хотя с формальной точки зрения оба протокола эквивалентны, для конструирования оптической схемы для атаки Евы на передаваемый ключ необходимо иметь явный вид унитарного оператора, описывающего действие Евы. Когда вид унитарного оператора известен явно, можно получить оптическую схему, которая реализует его экспериментально. В предыдущем способе рассмотрения такой унитарный оператор явно вообще не фигурировал.

Пусть Алиса готовит случайно одно из информационных состояний (53)–(56) и посылает в канал связи. Действия Евы сводятся к приготовлению своего вспомогательного состояния $|E\rangle_E$, которое приводится во взаимодействие с каждым передаваемым состоянием. После совместной эволюции состояние Евы и передаваемое состояние изменяются. Свое модифицированное состояние Ева оставляет у себя, а модифицированное состояние посылает к Бобу. Цель Евы состоит в том, чтобы выбрать такое взаимодействие (унитарный оператор U_{BE}), которое в конце протокола позволит ей получить максимум информации, допускаемый законами квантовой механики, при измерении своего модифицированного состояния при наблюдаемой ошибке на приемной стороне. Для выяснения действия унитарного оператора U_{BE} на произвольное информационное состояние достаточно выяснить его действие на базисные состояния, локализованные во временных окнах 1, 2, 3. Далее, учитывая свойства линейности оператора, можно получить его действие на произвольные информационные состояния (53)–(56).

Действие U_{BE} на базисные состояния может быть представлено в виде

$$U_{BE}(|1\rangle_B \otimes |E\rangle_E) = |1\rangle_B \otimes |\phi_1^1\rangle_E + \\ + |2\rangle_B \otimes |\phi_1^2\rangle_E + |3\rangle_B \otimes |\phi_1^3\rangle_E, \tag{83}$$

$$U_{BE}(|2\rangle_B \otimes |E\rangle_E) = |1\rangle_B \otimes |\phi_2^1\rangle_E + \\ + |2\rangle_B \otimes |\phi_2^2\rangle_E + |3\rangle_B \otimes |\phi_2^3\rangle_E, \tag{84}$$

$$U_{BE}(|3\rangle_B \otimes |E\rangle_E) = |1\rangle_B \otimes |\phi_3^1\rangle_E + \\ + |2\rangle_B \otimes |\phi_3^2\rangle_E + |3\rangle_B \otimes |\phi_3^3\rangle_E. \quad (85)$$

С учетом соотношений (69), (70) и (83)–(85) можно найти связь между состояниями Евы, имеем

$$\sqrt{\lambda_0^L}|e_0^L\rangle_E = \frac{1}{2}(|\phi_1^1\rangle_E + |\phi_2^2\rangle_E), \\ \sqrt{\lambda_1^L}|e_1^L\rangle_E = \frac{1}{2}(|\phi_1^2\rangle_E + |\phi_2^1\rangle_E), \quad (86)$$

$$\sqrt{\lambda_2^L}|e_2^L\rangle_E = \frac{1}{2}(|\phi_1^1\rangle_E - |\phi_2^2\rangle_E), \\ \sqrt{\lambda_3^L}|e_3^L\rangle_E = \frac{1}{2}(|\phi_1^2\rangle_E - |\phi_2^1\rangle_E), \quad (87)$$

$$\sqrt{q}|q_0^L\rangle_E = |\phi_1^3\rangle_E + |\phi_2^3\rangle_E, \\ \sqrt{q}|q_1^L\rangle_E = |\phi_1^3\rangle_E - |\phi_2^3\rangle_E. \quad (88)$$

Аналогично для правого базиса:

$$\sqrt{\lambda_0^R}|e_0^R\rangle_E = \frac{1}{2}(|\phi_2^1\rangle_E + |\phi_3^2\rangle_E), \\ \sqrt{\lambda_1^R}|e_1^R\rangle_E = \frac{1}{2}(|\phi_2^2\rangle_E + |\phi_3^1\rangle_E), \quad (89)$$

$$\sqrt{\lambda_2^R}|e_2^R\rangle_E = \frac{1}{2}(|\phi_2^1\rangle_E - |\phi_3^2\rangle_E), \\ \sqrt{\lambda_3^R}|e_3^R\rangle_E = \frac{1}{2}(|\phi_2^2\rangle_E - |\phi_3^1\rangle_E), \quad (90)$$

$$\sqrt{q}|q_0^R\rangle_E = |\phi_1^1\rangle_E + |\phi_2^1\rangle_E, \\ \sqrt{q}|q_1^R\rangle_E = |\phi_1^1\rangle_E - |\phi_2^1\rangle_E. \quad (91)$$

Правые части выражений (83)–(85) представляют собой разложение запутанного совместного, после действия U_{BE}, состояния Боб–Ева по базисным векторам в пространстве $\mathcal{H}_B \otimes \mathcal{H}_E$. В каждой отдельной строке i векторы $|\phi_i^j\rangle_E$ $(j = 1, 2, 3)$ попарно ортогональны, но не обязаны быть попарно ортогональными в разных строках. Условие унитарности приводит к соотношению

$$U_{BE}({}_B\langle i| \otimes {}_E\langle E|)(|j\rangle_B \otimes |E\rangle_E)U_{BE}^{+} = \delta_{i,j},$$

что с учетом условия симметрии между базисами дает

$${}_E\langle\phi_i^i|\phi_i^i\rangle_E = 1 - q, \quad i = 1, 2, 3; \quad (92)$$

$${}_E\langle\phi_j^i|\phi_j^i\rangle_E = \frac{q}{2}, \quad i = 2, 3, \quad j = 1, 2, 3, \quad i \neq j; \quad (93)$$

$${}_E\langle\phi_1^1|\phi_2^2\rangle_E = {}_E\langle\phi_2^2|\phi_3^3\rangle_E = (1 - q)\cos\alpha, \\ {}_E\langle\phi_1^2|\phi_2^1\rangle_E = {}_E\langle\phi_3^2|\phi_2^3\rangle_E = \frac{q}{2}\cos\alpha, \quad (94)$$

где α — угол между векторами. В формуле (94) нет оснований считать ортогональными векторы с указанными комбинациями индексов. Это следует из того факта, что при скалярном умножении, например, строки из (83) на ортогональный вектор (84), перед слагаемым ${}_E\langle\phi_1^1|\phi_2^2\rangle_E$ возникает нулевой коэффициент $({}_B\langle 1|2\rangle_B = 0)$, поэтому скалярное произведение ${}_E\langle\phi_1^1|\phi_2^2\rangle_E$ не обязано быть нулевым. Аналогично для других подобных пар векторов.

Используя формулы (79), (80) и (86)–(91), можно найти связь косинуса угла в (87) с наблюдаемой ошибкой на приемной стороне, имеем

$$Q = \frac{1 - \cos\alpha}{2}. \quad (95)$$

3.1.3. Явный вид возмущенных квантовых состояний подслушивателя

Приведем теперь явный вид модифицированных состояний Евы. Соотношениям (86)–(91) удовлетворяют следующие функции:

$$|\phi_1^1\rangle_E = \sqrt{1 - q}|\tau_1\rangle_E, \quad |\phi_1^2\rangle_E = \sqrt{\frac{q}{2}}|\tau_2\rangle_E, \\ |\phi_1^3\rangle_E = \sqrt{\frac{q}{2}}|\tau_3\rangle_E, \quad (96)$$

$$|\phi_2^1\rangle_E = \sqrt{\frac{q}{2}}(\cos\alpha|\tau_2\rangle_E + \sin\alpha|\tau_4\rangle_E), \\ |\phi_2^2\rangle_E = \sqrt{1 - q}(\cos\alpha|\tau_1\rangle_E + \sin\alpha|\tau_5\rangle_E), \quad (97)$$

$$|\phi_2^3\rangle_E = \sqrt{\frac{q}{2}}(\cos\alpha|\tau_6\rangle_E + \sin\alpha|\tau_7\rangle_E), \quad (98)$$

$$|\phi_3^1\rangle_E = \sqrt{\frac{q}{2}}|\tau_5\rangle_E, \\ |\phi_3^2\rangle_E = \sqrt{1 - q}|\tau_6\rangle_E, \quad |\phi_3^3\rangle_E = \sqrt{\frac{q}{2}}|\tau_1\rangle_E. \quad (99)$$

Здесь $|\tau_i\rangle_E$ — семь ортогональных базисных функций в пространстве $\mathcal{H}_E$.

Таким образом, для осуществления описанной атаки на ключ Ева должна иметь вспомогательную квантовую систему с пространством состояний размерности 7. В оптических экспериментах практически единственная возможность состоит в использовании не одной системы с семью состояниями, а трех

систем с двумя состояниями. Семь базисных состояний τ_i могут быть представлены как состояния трех двухуровневых систем $|s_1\rangle \otimes |s_2\rangle \otimes |s_3\rangle$, где базисные состояния $\{|s_i\rangle\} = \{|1\rangle, |2\rangle\}$ — однофотонные состояния, локализованные во временных окнах 1 и 2. Использование оптических элементов — светоделителей, оптических линий, а также нелинейных оптических элементов — позволяет реализовать унитарный оператор U_{BE}, перепутывающий передаваемые и вспомогательные состояния фотонов. Реализация такой оптической схемы представляет собой отдельную задачу, поэтому здесь она обсуждаться не будет. Отметим лишь, что для реализации такой схемы уже достаточно представления возмущенных состояний Евы в виде (96)–(99).

3.1.4. Вычисление частичных матриц плотности σ_E и σ_B

Для вычисления длины ключа с использованием критерия, основанного на границе Холево, необходимо вычислить модифицированные взаимодействием матрицы плотности Боба и Евы. Матрицы плотности, входящие в информацию Холево (26), даются следующими выражениями:

в базисе L

$$\sigma_E^L = \frac{|\phi_1^1\rangle_{EE}\langle\phi_1^1| + |\phi_2^2\rangle_{EE}\langle\phi_2^2| + |\phi_1^2\rangle_{EE}\langle\phi_1^2| + |\phi_2^1\rangle_{EE}\langle\phi_2^1|}{2(1-q/2)}, \tag{100}$$

в базисе R

$$\sigma_E^R = \frac{|\phi_2^2\rangle_{EE}\langle\phi_2^2| + |\phi_3^3\rangle_{EE}\langle\phi_3^3| + |\phi_2^3\rangle_{EE}\langle\phi_2^3| + |\phi_3^2\rangle_{EE}\langle\phi_3^2|}{2(1-q/2)}. \tag{101}$$

Частичные матрицы плотности Боба в базисе L имеют вид

$$\sigma_B^L = \frac{1}{2}\left(|1\rangle_{BB}\langle 1| + |2\rangle_{BB}\langle 2|\right), \tag{102}$$

соответственно в базисе R —

$$\sigma_B^R = \frac{1}{2}\left(|2\rangle_{BB}\langle 2| + |3\rangle_{BB}\langle 3|\right). \tag{103}$$

С учетом (102), (103) находим

$$\begin{gathered} S(\sigma_B^L) = S(\sigma_B^R) = 1, \\ S(\sigma_E^L) = S(\sigma_E^R) = h(\zeta) + h(Q), \end{gathered} \tag{104}$$

что окончательно дает выражение (82).

3.1.5. Обсуждение результатов в случае ортогональных состояний внутри базисов

Допустимая критическая ошибка, до которой гарантируется секретное распределение ключей, определяется из условия

$$1 - h(\zeta_c) - h(Q_c) = 0. \tag{105}$$

Информация легитимных пользователей о ключе,

$$C(Q) = 1 - h(Q), \tag{106}$$

представляет собой пропускную способность бинарного симметричного классического канала связи. Информация подслушивателя равна

$$C_{1,\infty}(\sigma_E) = \overline{C}(\sigma_E) = h(\zeta). \tag{107}$$

Область секретности протокола приведена на рис. 2.

Интересно отметить, что взаимная информация между Алисой и Бобом зависит только от величины ошибки Q. Информация Евы о ключе эффективно зависит только от вероятности отсчетов ζ в контрольных временных окнах[8)]. Этот факт имеет прозрачную физическую интерпретацию. Поскольку Еве неизвестно, какой из базисов будет выбран — левый L или правый R, из-за неортогональности любого состояния из левого базиса и любого состояния из правого (напомним, что состояния перекрываются во временном окне 2) принципиально невозможно достоверно с вероятностью единица различить состояния левого и правого базисов. Из-за неортогональности состояний получение информации об одном из состояний неизбежно будет приводить к их возмущению [41]. Возмущение приведет к отсчетам во временном окне 3 на приемной стороне Боба для искаженных состояний из левого, и во временном окне 1 для состояний из правого базиса.

[8)] Напомним, что у наиболее изученного протокола BB84 информация Алиса–Боб равна $1 - h(Q)$, информация Евы $\chi_E(\sigma_B) = h(Q)$, соответственно критическая ошибка определяется из уравнения $1 - h(Q) = h(Q)$. Данный протокол является однопараметрическим, информация всех участников определяется лишь одним параметром — ошибкой Q.

Интересной особенностью данного протокола является следующее свойство. Действия Евы приводят к ошибкам в информационной последовательности Q и отсчетам в контрольных временных слотах (q). Эти параметры Ева может выбирать независимо один от другого. Если отсчеты в контрольных окнах отсутствуют, $q = 0$, Ева не получает никакой информации о ключе. При этом допустимая ошибка, до которой гарантируется секретность ключей, достигает теоретического предела $Q = 50\,\%$. Сама по себе оптоволоконная схема квантовой криптографии также имеет неидеальности, которые приводят к появлению ошибки Q. Одной из таких неидеальностей является разбалансировка волоконного интерферометра Маха–Цандера [40], которая приводит к ошибкам в информационной последовательности 0 и 1. Такие ошибки неотличимы от ошибок, вносимых Евой. Поэтому, если разбалансировка достигает такой критической величины, что она дает критическую ошибку Q_c, протокол передачи ключей приходится прерывать. Однако разбалансировка интерферометра не приводит к сдвигам состояний во времени и не приводит к отсчетам в контрольных временных окнах, $q = 0$. В этом случае при разбалансировке можно продолжать передачу ключей и гарантировать их секретность вплоть до теоретического предела ошибок $Q = 50\,\%$. Напомним, что ошибка $Q = 50\,\%$ отвечает полной потере видности интерференционной картины на приемной стороне.

3.2. Неортогональные состояния внутри базисов

Рассмотренный выше протокол квантового распределения ключей с ортогональными сигнальными состояниями внутри базисов, хотя и обеспечивает в однофотонном случае максимально допустимую критическую ошибку из всех известных протоколов, но не обеспечивает достаточную длину передачи ключей. В реальных системах используются квазиоднофотонные состояния сильно ослабленного (обычно до уровня $\mu = 0.1$–0.2, μ — среднее число фотонов в когерентном состоянии) лазерного излучения. Как известно, последнее имеет пуассоновскую статистику по числу фотонов, т. е. при $n > 1$ с вероятностью $p(n) = e^{-\mu}\mu^n/n!$ (n — фоковские числа заполнения) будут встречаться неоднофотонные посылки. Поскольку в квантовой механике нет формальных ограничений на неразрушающее измерение числа фотонов (но не их состояния), подслушиватель может определить число фотонов в каждой посылке. Далее он может блокировать все однофотонные посылки, а из многофотонных оставить часть фотонов у себя, а остальные послать Бобу через свой канал с меньшими потерями (в пределе вообще без потерь). После согласования базисов Алисой и Бобом подслушиватель может провести измерения в известном базисе и из-за достоверной различимости ортогональных состояний внутри базиса иметь полную информацию о значении бита в каждой многофотонной посылке. Таким образом, передача секретных ключей невозможна, если длина канала связи (соответственно потери в нем) такова, что подслушиватель может блокировать все однофотонные посылки.

Ситуацию можно улучшить, если сделать состояния внутри базисов достоверно неразличимыми — неортогональными. Если используются только четыре состояния в двух базисах (например, только состояния в левом базисе), то, как показал предыдущий анализ [25], протокол теряет секретность, если длина канала связи и потери в нем таковы, что подслушиватель может блокировать все одно-, двух- и трехфотонные посылки и оставлять посылки с большим числом фотонов.

Ниже показано, что модификация нашего протокола квантового распределения ключей для случая неортогональных состояний внутри базиса при неоднофотонном источнике и потерях в канале связи обеспечивает секретность ключей до таких длин линии связи, при которых подслушивателю необходимо блокировать одно-, двух-, трех-, четырех- и пятифотонные посылки, чтобы получить полную информацию о ключе. Поэтому данный протокол обеспечивает секретность ключей при наибольшей длине линии связи из всех известных протоколов квантовой криптографии. При этом схема не требует радикальной модификации оптоволоконной части по сравнению с существующими базовыми схемами.

3.2.1. Однофотонный случай

Получим сначала длину ключа в однофотонном случае для протокола с контрольными временными окнами и с неортогональными состояниями внутри базисов, поскольку такая ситуация еще никем не исследовалась. Кроме того, эти результаты необходимы при выводе длины ключа при неоднофотонном источнике, потерях в канале связи и неидеальных фотодетекторах на приемной стороне.

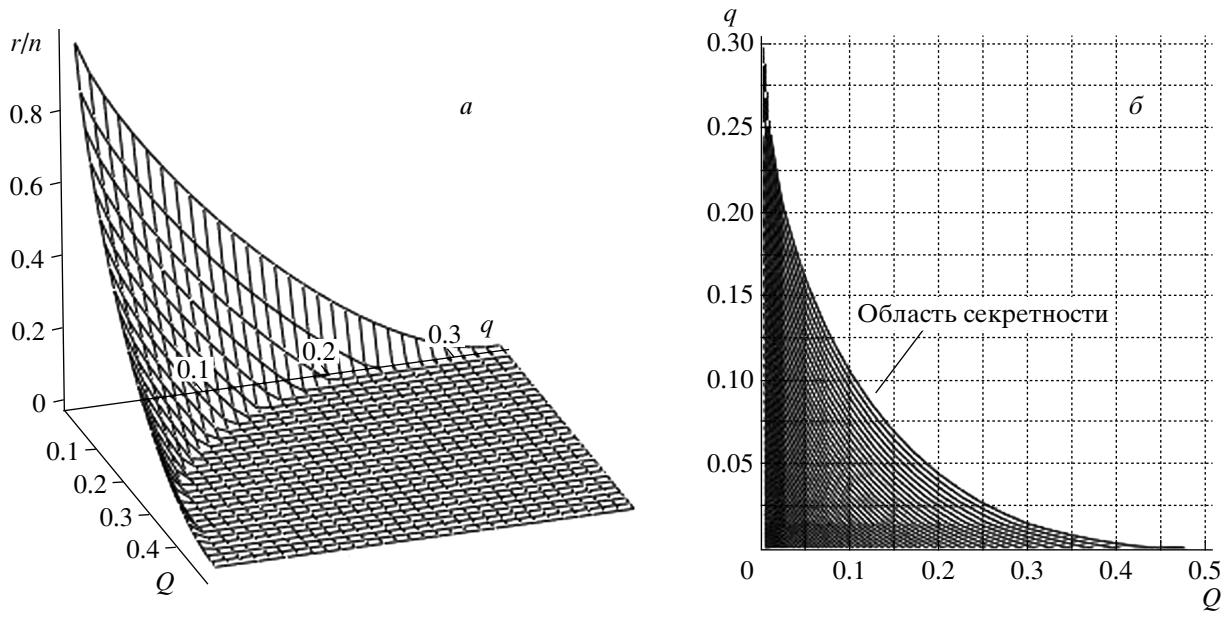

Рис. 2. *а*) Длина секретного ключа в пересчете на одну позицию $\frac{r}{n}(Q,q) = 1 - h(Q) - h(\zeta(q))$. *б*) Область секретности протокола на плоскости (Q,q)

Информационные состояния в левом базисе могут быть представлены в виде

$$|0^{L_a}\rangle = \cos\frac{\eta}{2}|1\rangle + \sin\frac{\eta}{2}|2\rangle,$$
$$|1^{L_a}\rangle = \cos\frac{\eta}{2}|1\rangle - \sin\frac{\eta}{2}|2\rangle, \tag{108}$$

$$|0^{L_b}\rangle = \sin\frac{\eta}{2}|1\rangle - \cos\frac{\eta}{2}|2\rangle,$$
$$|1^{L_b}\rangle = \sin\frac{\eta}{2}|1\rangle + \cos\frac{\eta}{2}|2\rangle, \tag{109}$$

в правом базисе —

$$|0^{R_a}\rangle = \cos\frac{\eta}{2}|2\rangle + \sin\frac{\eta}{2}|3\rangle,$$
$$|1^{R_a}\rangle = \cos\frac{\eta}{2}|2\rangle - \sin\frac{\eta}{2}|3\rangle, \tag{110}$$

$$|0^{R_b}\rangle = \sin\frac{\eta}{2}|2\rangle - \cos\frac{\eta}{2}|3\rangle,$$
$$|1^{R_b}\rangle = \sin\frac{\eta}{2}|2\rangle + \cos\frac{\eta}{2}|3\rangle. \tag{111}$$

Отметим, что для дальнейшего рассмотрения важно, чтобы набор неортогональных состояний в каждом из базисов не мог быть переведен в состояния в другом базисе посредством одного и того же унитарного поворота. Конфигурация состояний показана на рис. 3.

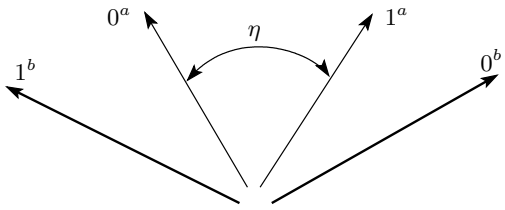

Рис. 3. Геометрия состояний, жирными векторами показаны состояния, относящиеся к базису «a», обычными — к базису «b». Состояния 0 и 1 из разных базисов ортогональны

3.2.2. Унитарное преобразование подслушивателя

Опишем явным образом атаку Евы в однофотонном случае. Атака Евы описывается действием унитарного оператора U_{BE} на сигнальные состояния и вспомогательное состояние Евы $|E\rangle_E$. Имеем

$$
\begin{aligned}
&|\widetilde{0^{L_a}}\rangle_{BE} = U_{BE}(|0^{L_a}\rangle_B \otimes |E\rangle_E) = \\
&= |0^{L_a}\rangle_B \otimes |\varphi_1^{0_{L_a}}\rangle_E + |0^{L_b}\rangle_B \otimes |\varphi_2^{0_{L_a}}\rangle_E + \\
&\qquad + |3\rangle_B \otimes |\varphi_3^{0_{L_a}}\rangle_B, \\
&|\widetilde{1^{L_a}}\rangle_{BE} = U_{BE}(|1^{L_a}\rangle_B \otimes |E\rangle_E) = \\
&= |1^{L_a}\rangle_B \otimes |\varphi_1^{1_{L_a}}\rangle_E + |1^{L_b}\rangle_B \otimes |\varphi_2^{1_{L_a}}\rangle_E + \\
&\qquad + |3\rangle_B \otimes |\varphi_3^{1_{L_a}}\rangle_E, \\
&|\widetilde{0^{L_b}}\rangle_{BE} = U_{BE}(|0^{L_b}\rangle_B \otimes |E\rangle_E) = \\
&= |0^{L_b}\rangle_B \otimes |\varphi_1^{0_{L_b}}\rangle_E + |0^{L_a}\rangle_B \otimes |\varphi_2^{0_{L_b}}\rangle_E + \\
&\qquad + |3\rangle_B \otimes |\varphi_3^{0_{L_b}}\rangle_E, \\
&|\widetilde{1^{L_b}}\rangle_{BE} = U_{BE}(|1^{L_b}\rangle_B \otimes |E\rangle_E) = \\
&= |1^{L_b}\rangle_B \otimes |\varphi_1^{1_{L_b}}\rangle_E + |1^{L_a}\rangle_B \otimes |\varphi_2^{1_{L_b}}\rangle_E + \\
&\qquad + |3\rangle_B \otimes |\varphi_3^{1_{L_b}}\rangle_E, \\
&|\widetilde{0^{R_a}}\rangle_{BE} = U_{BE}(|0^{R_a}\rangle_E \otimes |E\rangle_E) = \\
&= |1\rangle_B \otimes |\varphi_3^{0_{R_a}}\rangle_E + |0^{R_a}\rangle_B \otimes |\varphi_1^{0_{R_a}}\rangle_E + \\
&\qquad + |0^{R_b}\rangle_B \otimes |\varphi_2^{0_{R_a}}\rangle_E, \\
&|\widetilde{1^{R_a}}\rangle_{BE} = U_{BE}(|1^{R_a}\rangle_B \otimes |E\rangle_E) = \\
&= |1\rangle_B \otimes |\varphi_3^{1_{R_a}}\rangle_E + |1^{R_a}\rangle_B \otimes |\varphi_1^{1_{R_a}}\rangle_E + \\
&\qquad + |1^{R_b}\rangle_B \otimes |\varphi_2^{1_{R_a}}\rangle_E, \\
&|\widetilde{0^{R_b}}\rangle_{BE} = U_{BE}(|0^{R_b}\rangle_B \otimes |E\rangle_E) = \\
&= |1\rangle_B \otimes |\varphi_3^{0_{R_b}}\rangle_E + |0^{R_b}\rangle_B \otimes |\varphi_1^{0_{R_b}}\rangle_E + \\
&\qquad + |0^{R_a}\rangle_B \otimes |\varphi_2^{0_{R_b}}\rangle_E, \\
&|\widetilde{1^{R_b}}\rangle_{BE} = U_{BE}(|1^{R_b}\rangle_B \otimes |E\rangle_E) = \\
&= |1\rangle_B \otimes |\varphi_3^{1_{R_b}}\rangle_E + |1^{R_b}\rangle_B \otimes |\varphi_1^{1_{R_b}}\rangle_E + \\
&\qquad + |1^{R_a}\rangle_B \otimes |\varphi_2^{1_{R_b}}\rangle_E.
\end{aligned} \tag{112}
$$

Выражения (112) фактически представляют собой разложение состояний (возмущенное сигнальное состояние и состояние Евы) $|i^{\widetilde{L_{a,b},R_{a,b}}}\rangle_{BE}$ $(i = 0, 1)$ по ортогональным базисным состояниям в пространстве $\mathcal{H}_B \otimes \mathcal{H}_E$. В каждой строке состояния в $\mathcal{H}_E$ попарно ортогональны, состояния же из разных строк не обязаны быть все попарно ортогональны. Имеем

$$
\begin{aligned}
&{}_E\langle\varphi_1^{0_{L_a}}|\varphi_2^{0_{L_a}}\rangle_E = {}_E\langle\varphi_2^{0_{L_a}}|\varphi_3^{0_{L_a}}\rangle_E = \\
&\qquad = {}_E\langle\varphi_1^{0_{L_a}}|\varphi_3^{0_{L_a}}\rangle_E = 0,
\end{aligned} \tag{113}
$$

$$
\begin{aligned}
&{}_E\langle\varphi_1^{1_{L_a}}|\varphi_2^{1_{L_a}}\rangle_E = {}_E\langle\varphi_2^{1_{L_a}}|\varphi_3^{1_{L_a}}\rangle_E = \\
&\qquad = {}_E\langle\varphi_1^{1_{L_a}}|\varphi_3^{1_{L_a}}\rangle_E = 0,
\end{aligned} \tag{114}
$$

$$
\begin{aligned}
&{}_E\langle\varphi_1^{0_{R_a}}|\varphi_2^{0_{R_a}}\rangle_E = {}_E\langle\varphi_2^{0_{R_a}}|\varphi_3^{0_{R_a}}\rangle_E = \\
&\qquad = {}_E\langle\varphi_1^{0_{R_a}}|\varphi_3^{0_{R_a}}\rangle_E = 0,
\end{aligned} \tag{115}
$$

$$
\begin{aligned}
&{}_E\langle\varphi_1^{1_{R_a}}|\varphi_2^{1_{R_a}}\rangle_E = {}_E\langle\varphi_2^{1_{R_a}}|\varphi_3^{1_{R_a}}\rangle_E = \\
&\qquad = {}_E\langle\varphi_1^{1_{R_a}}|\varphi_3^{1_{R_a}}\rangle_E = 0.
\end{aligned} \tag{116}
$$

Разложение (112) на первый взгляд должно содержать большое число параметров, однако из-за симметрии между базисами и состояниями внутри базисов оказывается только три параметра, описывающих U_{BE}. Для того чтобы воспользоваться симметрийными соображениями, необходимо записать разложения (112) через базисные векторы во временных окнах, имеем

$$
\begin{aligned}
&U_{BE}(|1\rangle_B \otimes |E\rangle_E) = |\widetilde{1}\rangle_{BE} = |1\rangle_B \otimes |\psi_1^1\rangle_E + \\
&\qquad + |2\rangle_B \otimes |\psi_1^2\rangle_E + |3\rangle_B \otimes |\psi_1^3\rangle_E, \\
&U_{BE}(|2\rangle_B \otimes |E\rangle_E) = |\widetilde{2}\rangle_{BE} = |1\rangle_B \otimes |\psi_2^1\rangle_E + \\
&\qquad + |2\rangle_B \otimes |\psi_2^2\rangle_E + |3\rangle_B \otimes |\psi_3^2\rangle_E, \\
&U_{BE}(|3\rangle_B \otimes |E\rangle_E) = |\widetilde{3}\rangle_{BE} = |1\rangle_B \otimes |\psi_3^1\rangle_E + \\
&\qquad + |2\rangle_B \otimes |\psi_3^2\rangle_E + |3\rangle_B \otimes |\psi_3^3\rangle_E,
\end{aligned} \tag{117}
$$

где $|\psi_k^j\rangle_E \in \mathcal{H}_E$ — базисные векторы, которые в каждой строке попарно ортогональны. Кроме того, из унитарности U_{BE} следует, что

$$
\begin{aligned}
&{}_E\langle\psi_1^1|\psi_2^1\rangle_E = {}_E\langle\psi_1^2|\psi_2^2\rangle_E = {}_E\langle\psi_1^3|\psi_2^3\rangle_E = 0, \\
&{}_E\langle\psi_2^1|\psi_3^1\rangle_E = {}_E\langle\psi_2^2|\psi_3^2\rangle_E = {}_E\langle\psi_2^3|\psi_3^3\rangle_E = 0, \\
&{}_E\langle\psi_1^1|\psi_3^1\rangle_E = {}_E\langle\psi_1^2|\psi_3^2\rangle_E = {}_E\langle\psi_1^3|\psi_3^3\rangle_E = 0.
\end{aligned} \tag{118}
$$

Симметрия между левым и правым базисами, а также условие нормировки дают

$$
{}_E\langle\psi_1^3|\psi_1^3\rangle = \langle\psi_2^3|\psi_2^3\rangle = \langle\psi_2^1|\psi_2^1\rangle = \langle\psi_3^1|\psi_3^1\rangle = q, \tag{119}
$$

$$
\begin{aligned}
&{}_E\langle\psi_2^2|\psi_2^2\rangle_E = {}_E\langle\psi_1^1|\psi_1^1\rangle_E = \\
&\qquad = {}_E\langle\psi_3^3|\psi_3^3\rangle_E = 1 - 2q.
\end{aligned} \tag{120}
$$

Далее удобно перейти к нормированным состояниям $|\overline{\psi}_j^i\rangle$:

$$
\begin{gathered}
|\overline{\psi}_1^1\rangle = \frac{1}{\sqrt{1-2q}}|\psi_1^1\rangle, \quad |\overline{\psi}_2^2\rangle = \frac{1}{\sqrt{1-2q}}|\psi_2^2\rangle, \\
|\overline{\psi}_3^3\rangle = \frac{1}{\sqrt{1-2q}}|\psi_3^3\rangle, \\
|\overline{\psi}_2^1\rangle = \frac{1}{\sqrt{q}}|\psi_2^1\rangle, \quad |\overline{\psi}_3^1\rangle = \frac{1}{\sqrt{q}}|\psi_3^1\rangle, \\
|\overline{\psi}_1^2\rangle = \frac{1}{\sqrt{q}}|\psi_1^2\rangle, \quad |\overline{\psi}_3^2\rangle = \frac{1}{\sqrt{q}}|\psi_3^2\rangle, \\
|\overline{\psi}_1^3\rangle = \frac{1}{\sqrt{q}}|\psi_1^3\rangle, \quad |\overline{\psi}_2^3\rangle = \frac{1}{\sqrt{q}}|\psi_2^3\rangle.
\end{gathered}
$$

Тогда представление (117) примет вид

$$
\begin{aligned}
&U_{BE}(|1\rangle_B\otimes|E\rangle_E)=|\widetilde{1}\rangle_{BE}=\sqrt{1-2q}|1\rangle_B\otimes\\
&\otimes|\overline{\psi}_1^1\rangle_E+\sqrt{q}|2\rangle_B\otimes|\overline{\psi}_1^2\rangle_E+\sqrt{q}|3\rangle_B\otimes|\overline{\psi}_1^3\rangle_E,\\
&U_{BE}(|2\rangle_B\otimes|E\rangle_E)=|\widetilde{2}\rangle_{BE}=\\
&=\sqrt{q}|1\rangle_B\otimes|\overline{\psi}_2^1\rangle_E+\sqrt{1-2q}|2\rangle_B\otimes|\overline{\psi}_2^2\rangle_E+\\
&\qquad+\sqrt{q}|3\rangle_B\otimes|\overline{\psi}_2^3\rangle_E,\\
&U_{BE}(|3\rangle_B\otimes|E\rangle_E)=|\widetilde{3}\rangle_{BE}=\\
&=\sqrt{q}|1\rangle_B\otimes|\overline{\psi}_3^1\rangle_E+\sqrt{q}|2\rangle_B\otimes|\overline{\psi}_3^2\rangle_E+\\
&\qquad+\sqrt{1-2q}|3\rangle_B\otimes|\overline{\psi}_3^3\rangle_E.
\end{aligned}
\tag{121}
$$

В дальнейшем потребуются скалярные произведения векторов в $\mathcal{H}_E$, фигурирующих в формулах (118)–(120). Воспользуемся связью между векторами в $\mathcal{H}_E$, имеем

$$
\begin{aligned}
|\varphi_{0_{L_a}}^1\rangle&=\cos\frac{\eta}{2}\left(\cos\frac{\eta}{2}|\psi_1^1\rangle+\sin\frac{\eta}{2}|\psi_2^1\rangle\right)+\\
&\quad+\sin\frac{\eta}{2}\left(\cos\frac{\eta}{2}|\psi_1^2\rangle+\sin\frac{\eta}{2}|\psi_2^2\rangle\right),\\
|\varphi_{0_{L_a}}^2\rangle&=\cos\frac{\eta}{2}\left(\sin\frac{\eta}{2}|\psi_1^1\rangle-\cos\frac{\eta}{2}|\psi_2^1\rangle\right)+\\
&\quad+\sin\frac{\eta}{2}\left(\sin\frac{\eta}{2}|\psi_1^2\rangle-\cos\frac{\eta}{2}|\psi_2^2\rangle\right),\\
|\varphi_{0_{L_a}}^3\rangle&=\cos\frac{\eta}{2}|\psi_3^1\rangle+\sin\frac{\eta}{2}|\psi_3^2\rangle,\\
|\varphi_{1_{L_a}}^1\rangle&=\cos\frac{\eta}{2}\left(\cos\frac{\eta}{2}|\psi_1^1\rangle-\sin\frac{\eta}{2}|\psi_2^1\rangle\right)-\\
&\quad-\sin\frac{\eta}{2}\left(\cos\frac{\eta}{2}|\psi_1^2\rangle-\sin\frac{\eta}{2}|\psi_2^2\rangle\right),\\
|\varphi_{1_{L_a}}^2\rangle&=\cos\frac{\eta}{2}\left(\sin\frac{\eta}{2}|\psi_1^1\rangle+\cos\frac{\eta}{2}|\psi_2^1\rangle\right)-\\
&\quad-\sin\frac{\eta}{2}\left(\sin\frac{\eta}{2}|\psi_1^2\rangle+\cos\frac{\eta}{2}|\psi_2^2\rangle\right),\\
|\varphi_{1_{L_a}}^3\rangle&=\cos\frac{\eta}{2}|\psi_3^1\rangle-\sin\frac{\eta}{2}|\psi_3^2\rangle,\\
|\varphi_{0_{L_b}}^1\rangle&=\sin\frac{\eta}{2}\left(\sin\frac{\eta}{2}|\psi_1^1\rangle-\cos\frac{\eta}{2}|\psi_2^1\rangle\right)-\\
&\quad-\cos\frac{\eta}{2}\left(\sin\frac{\eta}{2}|\psi_1^2\rangle-\cos\frac{\eta}{2}|\psi_2^2\rangle\right),\\
|\varphi_{0_{L_b}}^2\rangle&=\sin\frac{\eta}{2}\left(\cos\frac{\eta}{2}|\psi_1^1\rangle+\sin\frac{\eta}{2}|\psi_2^1\rangle\right)-\\
&\quad-\cos\frac{\eta}{2}\left(\cos\frac{\eta}{2}|\psi_1^2\rangle+\sin\frac{\eta}{2}|\psi_2^2\rangle\right),\\
|\varphi_{0_{L_b}}^3\rangle&=\sin\frac{\eta}{2}|\psi_3^1\rangle-\cos\frac{\eta}{2}|\psi_3^2\rangle,\\
|\varphi_{1_{L_b}}^1\rangle&=\sin\frac{\eta}{2}\left(\sin\frac{\eta}{2}|\psi_1^1\rangle+\cos\frac{\eta}{2}|\psi_2^1\rangle\right)+\\
&\quad+\cos\frac{\eta}{2}\left(\sin\frac{\eta}{2}|\psi_1^2\rangle+\cos\frac{\eta}{2}|\psi_2^2\rangle\right),\\
|\varphi_{1_{L_b}}^2\rangle&=\sin\frac{\eta}{2}\left(\cos\frac{\eta}{2}|\psi_1^1\rangle-\sin\frac{\eta}{2}|\psi_2^1\rangle\right)+\\
&\quad+\cos\frac{\eta}{2}\left(\cos\frac{\eta}{2}|\psi_1^2\rangle-\sin\frac{\eta}{2}|\psi_2^2\rangle\right),\\
|\varphi_{1_{L_b}}^3\rangle&=\sin\frac{\eta}{2}|\psi_3^1\rangle+\cos\frac{\eta}{2}|\psi_3^2\rangle.
\end{aligned}
\tag{122}
$$

Аналогично можно получить соотношения для компонент правого базиса, но из экономии места они приводиться не будут. Имеем

$$
\begin{aligned}
{}_E\langle\varphi_3^{0_{L_a}}|\varphi_3^{0_{L_a}}\rangle_E&={}_E\langle\varphi_3^{1_{L_a}}|\varphi_3^{1_{L_a}}\rangle_E=\\
&={}_E\langle\varphi_3^{0_{L_b}}|\varphi_3^{0_{L_b}}\rangle_E={}_E\langle\varphi_3^{1_{L_b}}|\varphi_3^{1_{L_b}}\rangle_E=\\
&={}_E\langle\varphi_3^{0_{R_a}}|\varphi_3^{0_{R_a}}\rangle_E={}_E\langle\varphi_3^{1_{R_a}}|\varphi_3^{1_{R_a}}\rangle_E=\\
&={}_E\langle\varphi_3^{0_{R_b}}|\varphi_3^{0_{R_b}}\rangle_E={}_E\langle\varphi_3^{1_{R_b}}|\varphi_3^{1_{R_b}}\rangle_E=q.
\end{aligned}
\tag{123}
$$

Недостающие соотношения можно получить, опять воспользовавшись требованием унитарности преобразования U_{BE}, которое сводится к требованию сохранения углов — ортогональности некоторых пар состояний Евы в (118)–(120). Имеем

$$
\begin{aligned}
\langle\varphi_1^{0_{L_a}}|\varphi_2^{0_{L_a}}\rangle&=\sin\frac{\eta}{2}\cos^3\frac{\eta}{2}\times\\
&\times\left(\langle\psi_1^1|\psi_1^1\rangle-\langle\psi_1^2|\psi_1^2\rangle-\langle\psi_1^1|\psi_2^2\rangle-\langle\psi_2^1|\psi_1^2\rangle\right)+\\
&+\sin^3\frac{\eta}{2}\cos\frac{\eta}{2}\left(\langle\psi_2^1|\psi_2^1\rangle-\langle\psi_2^2|\psi_2^2\rangle+\right.\\
&\left.+\langle\psi_2^2|\psi_1^1\rangle+\langle\psi_1^2|\psi_2^1\rangle\right)=\sin\frac{\eta}{2}\cos^3\frac{\eta}{2}\times\\
&\times\left(1-3q-(\langle\psi_1^1|\psi_2^2\rangle+\langle\psi_2^1|\psi_1^2\rangle)\right)+\\
&+\sin^3\frac{\eta}{2}\cos\frac{\eta}{2}\left(3q-1+\langle\psi_1^1|\psi_2^2\rangle+\langle\psi_2^1|\psi_1^2\rangle\right)=\\
&=\sin\frac{\eta}{2}\cos\frac{\eta}{2}\left(\cos^2\frac{\eta}{2}-\sin^2\frac{\eta}{2}\right)\times\\
&\times\left(1-3q-(\langle\psi_1^1|\psi_2^2\rangle+\langle\psi_2^1|\psi_1^2\rangle)\right)=0,
\end{aligned}
$$

а значит,

$$
1-3q=\langle\psi_1^1|\psi_2^2\rangle+\langle\psi_2^1|\psi_1^2\rangle. \tag{124}
$$

Соотношения в правой части (124) можно обозначить как

$$
\begin{aligned}
\langle\psi_1^1|\psi_2^2\rangle&=(1-2q)\langle\overline{\psi}_1^1|\overline{\psi}_2^2\rangle=(1-2q)\cos\alpha,\\
\langle\psi_2^1|\psi_1^2\rangle&=q\langle\overline{\psi}_2^1|\overline{\psi}_1^2\rangle=q\cos\beta,
\end{aligned}
\tag{125}
$$

где $\cos\alpha$ и $\cos\beta$ являются двумя дополнительными параметрами, параметризующими U_{BE}. Окончательно с учетом (124), (125) получаем

$$
1-3q=(1-2q)\cos\alpha+q\cos\beta. \tag{126}
$$

Таким образом, атака Евы описывается полностью унитарным оператором U_{BE}, который параметризуется тремя независимыми параметрами q, $\cos\alpha$ и $\cos\beta$. Данные параметры должны выбираться Евой таким образом, чтобы обеспечить максимум информации о передаваемом ключе при наблюдаемой на приемной стороне вероятности ошибки Q в информационной последовательности и наблюдаемой вероятности q отсчетов в контрольных временных окнах.

3.2.3. Измерения на приемной стороне

Перейдем теперь к измерениям на приемной стороне. Из-за симметрии относительно базисов достаточно рассмотреть измерения только в базисе L_a. Далее удобнее использовать не два, а одно измерение, которое имеет три исхода и описывается следующим разложением единицы в $\mathcal{H}_B$:

$$I_B = \mathcal{M}_0^{L_a} + \mathcal{M}_1^{L_a} + \mathcal{M}_?^{L_a} + |3\rangle_{BB}\langle 3|. \qquad (127)$$

$$\mathcal{M}_0^{L_a} = \frac{1}{1+\cos\eta}|1_\perp^{L_a}\rangle_{BB}\langle 1_\perp^{L_a}| = \frac{1}{1+\cos\eta}|1^{L_b}\rangle_{BB}\langle 1^{L_b}|, \qquad (128)$$

$$\mathcal{M}_1^{L_a} = \frac{1}{1+\cos\eta}|0_\perp^{L_a}\rangle_{BB}\langle 0_\perp^{L_a}| = \frac{1}{1+\cos\eta}|0^{L_b}\rangle_{BB}\langle 0^{L_b}|, \qquad (129)$$

$$\mathcal{M}_?^{L_a} = I_B - \mathcal{M}_0^{L_a} - \mathcal{M}_1^{L_a} - |3\rangle_{BB}\langle 3|. \qquad (130)$$

Операторозначные меры $\mathcal{M}$ в формулах (127)–(130) отвечают исходам измерений, которые интерпретируются как 0, 1 или исход с неопределенным результатом ?. Также возможно получение отсчета в контрольном временном окне 3 для левого базиса, и окне 1 для правого.

3.2.4. Вычисление информации на приемной стороне

Состояния на приемной стороне получаются взятием частичного следа по $\mathcal{H}_E$. С учетом (112) находим

$$\sigma_B^{0_{L_a}} = \mathrm{Tr}_E\{|\widetilde{0^{L_a}}\rangle_{BE\,BE}\langle\widetilde{0^{L_a}}|\} = {}_E\langle\varphi_1^{0_{L_a}}|\varphi_1^{0_{L_a}}\rangle_E|0^{L_a}\rangle_B B\langle 0^{L_a}| + {}_E\langle\varphi_2^{0_{L_a}}|\varphi_2^{0_{L_a}}\rangle_E|0^{L_b}\rangle_{BB}\langle 0^{L_b}| + {}_E\langle\varphi_3^{0_{L_a}}|\varphi_3^{0_{L_a}}\rangle_E|3\rangle_{BB}\langle 3|, \qquad (131)$$

$$\sigma_B^{1_{L_a}} = \mathrm{Tr}_E\{|\widetilde{1^{L_a}}\rangle_{BE\,BE}\langle\widetilde{1^{L_a}}|\} = {}_E\langle\varphi_1^{1_{L_a}}|\varphi_1^{1_{L_a}}\rangle_E|1^{L_a}\rangle_{BB}\langle 1^{L_a}| + {}_E\langle\varphi_2^{1_{L_a}}|\varphi_2^{1_{L_a}}\rangle_E|1^{L_b}\rangle_{BB}\langle 1^{L_b}| + {}_E\langle\varphi_3^{1_{L_a}}|\varphi_3^{1_{L_a}}\rangle_E|3\rangle_{BB}\langle 3|, \qquad (132)$$

$$\sigma_B^{0_{L_b}} = \mathrm{Tr}_E\{|\widetilde{0^{L_b}}\rangle_{BE\,BE}\langle\widetilde{0^{L_b}}|\} = {}_E\langle\varphi_1^{0_{L_b}}|\varphi_1^{0_{L_b}}\rangle_E|0^{L_b}\rangle_{BB}\langle 0^{L_b}| + {}_E\langle\varphi_2^{0_{L_b}}|\varphi_2^{0_{L_b}}\rangle_E|0^{L_a}\rangle_{BB}\langle 0^{L_a}| + {}_E\langle\varphi_3^{0_{L_b}}|\varphi_3^{0_{L_b}}\rangle_E|3\rangle_{BB}\langle 3|, \qquad (133)$$

$$\sigma_B^{1_{L_b}} = \mathrm{Tr}_E\{|\widetilde{1^{L_b}}\rangle_{BE\,BE}\langle\widetilde{1^{L_b}}|\} = {}_E\langle\varphi_1^{1_{L_b}}|\varphi_1^{1_{L_b}}\rangle_E|1^{L_b}\rangle_{BB}\langle 1^{L_b}| + {}_E\langle\varphi_2^{1_{L_b}}|\varphi_2^{1_{L_b}}\rangle_E|1^{L_a}\rangle_{BB}\langle 1^{L_a}| + {}_E\langle\varphi_3^{1_{L_b}}|\varphi_3^{1_{L_b}}\rangle_E|3\rangle_{BB}\langle 3|. \qquad (134)$$

Аналогичное представление имеет место в правом базисе.

При вычислении взаимной информации Алиса–Боб $C(Q)$, которая входит в уравнение для длины ключа, достаточно вычислить переходные вероятности для канала связи Алиса–Боб. С учетом формул (120)–(127) и (131)–(134) имеем

$$p_{X|Y}(0_{L_a}|0) = \frac{1}{1+\cos\eta}\left[{}_E\langle\varphi_1^{0_{L_a}}|\varphi_1^{0_{L_a}}\rangle_E|_B\langle 0^{L_a}|1^{L_b}\rangle_E|^2 + {}_E\langle\varphi_2^{0_{L_a}}|\varphi_2^{0_{L_a}}\rangle_E|_B\langle 0^{L_b}|1^{L_b}\rangle_B|^2\right] = \frac{{}_E\langle\varphi_1^{0_{L_a}}|\varphi_1^{0_{L_a}}\rangle_E\sin^2\eta + {}_E\langle\varphi_2^{0_{L_a}}|\varphi_2^{0_{L_a}}\rangle_E\cos^2\eta}{1+\cos\eta}, \qquad (135)$$

$$p_{X|Y}(0^{L_a}|1) = \frac{{}_E\langle\varphi_2^{0_{L_a}}|\varphi_2^{0_{L_a}}\rangle_E}{1+\cos\eta}, \qquad (136)$$

$$p_{X|Y}(0^{L_a}|3) = {}_E\langle\varphi_3^{0_{L_a}}|\varphi_3^{0_{L_a}}\rangle_E. \qquad (137)$$

Первая из этих возможностей (135), имеющая условную вероятность $p_{X|Y}(0_{L_a}|0)$, означает отсутствие ошибки при передаче (послан 0, получен 0). Вторая возможность (136) означает ошибку на приемной стороне. Именно эту ошибку пользователи оценивают, раскрывая часть последовательности. Наконец, третья возможность (137) отвечает за отсчеты в контрольном временном окне, которых в отсутствие подслушивателя не должно было быть. Эти посылки служат для оценки величины q и в дальнейшем также отбрасываются.

Для вероятности ошибки на приемной стороне Боба находим с учетом (135)–(137)

$$Q = \frac{p_{X|Y}(0^{L_a}|1)}{p_{X|Y}(0^{L_a}|0) + p_{X|Y}(0^{L_a}|1)} = \frac{{}_E\langle\varphi_2^{0_{L_a}}|\varphi_2^{0_{L_a}}\rangle_E}{{}_E\langle\varphi_1^{0_{L_a}}|\varphi_1^{0_{L_a}}\rangle_E \sin^2\eta + {}_E\langle\varphi_2^{0_{L_a}}|\varphi_2^{0_{L_a}}\rangle_E(\cos^2\eta+1)}, \tag{138}$$

соответственно для вероятности правильного исхода —

$$1-Q = \frac{p_{X|Y}(0^{L_a}|0)}{p_{X|Y}(0^{L_a}|0) + p_{X|Y}(0^{L_a}|1)} = \frac{{}_E\langle\varphi_1^{0_{L_a}}|\varphi_1^{0_{L_a}}\rangle_E \sin^2\eta + {}_E\langle\varphi_2^{0_{L_a}}|\varphi_2^{0_{L_a}}\rangle_E \cos^2\eta}{{}_E\langle\varphi_1^{0_{L_a}}|\varphi_1^{0_{L_a}}\rangle_E \sin^2\eta + {}_E\langle\varphi_2^{0_{L_a}}|\varphi_2^{0_{L_a}}\rangle_E(\cos^2\eta+1)}. \tag{139}$$

Для подсчета вероятностей (135)–(137) исходов с определенным результатом на приемной стороне необходимо вычислить скалярные произведения ${}_E\langle\varphi_j^i|\varphi_n^m\rangle_E$. Сделаем это для ${}_E\langle\varphi_1^{0_{L_a}}|\varphi_1^{0_{L_a}}\rangle_E$. Используя соотношения (138), (139), имеем

$$\begin{aligned}
{}_E\langle\varphi_1^{0_{L_a}}|\varphi_1^{0_{L_a}}\rangle_E &= \cos^2\frac{\eta}{2}\left(\cos\frac{\eta}{2}{}_E\langle\psi_1^1| + \sin\frac{\eta}{2}{}_E\langle\psi_1^2|\right)\times\\
&\times\left(\cos\frac{\eta}{2}|\psi_1^1\rangle_E + \sin\frac{\eta}{2}|\psi_1^2\rangle_E\right) +\\
&+\cos\frac{\eta}{2}\sin\frac{\eta}{2}\left[\left(\cos\frac{\eta}{2}{}_E\langle\psi_1^1| + \sin\frac{\eta}{2}{}_E\langle\psi_1^2|\right)\times\right.\\
&\times\left(\cos\frac{\eta}{2}|\psi_2^1\rangle_E + \sin\frac{\eta}{2}|\psi_2^2\rangle_E\right) +\\
&+\left.\left(\cos\frac{\eta}{2}{}_E\langle\psi_2^1| + \sin\frac{\eta}{2}{}_E\langle\psi_2^2|\right)\left(\cos\frac{\eta}{2}|\psi_1^1\rangle + \sin\frac{\eta}{2}|\psi_1^2\rangle_E\right)\right] +\\
&+\sin^2\frac{\eta}{2}\left(\cos\frac{\eta}{2}{}_E\langle\psi_2^1| + \sin\frac{\eta}{2}\langle\psi_2^2|\right)\times\\
&\times\left(\cos\frac{\eta}{2}|\psi_2^1\rangle_E + \sin\frac{\eta}{2}|\psi_2^2\rangle\right) = \cos^4\frac{\eta}{2}{}_E\langle\psi_1^1|\psi_1^1\rangle_E +\\
&+\cos^2\frac{\eta}{2}\sin^2\frac{\eta}{2}\left({}_E\langle\psi_1^2|\psi_1^2\rangle_E + {}_E\langle\psi_1^1|\psi_2^2\rangle_E + {}_E\langle\psi_1^2|\psi_2^1\rangle_E +\right.\\
&\left.+\ {}_E\langle\psi_2^1|\psi_1^2\rangle_E + {}_E\langle\psi_2^2|\psi_1^1\rangle_E + {}_E\langle\psi_2^1|\psi_2^1\rangle_E\right) +\\
&+\sin^4\frac{\eta}{2}{}_E\langle\psi_2^2|\psi_2^2\rangle_E =\\
&= (1-2q)\left(\cos^4\frac{\eta}{2} + \sin^4\frac{\eta}{2}\right) +\\
&+2\cos^2\frac{\eta}{2}\sin^2\frac{\eta}{2}(q+\cos\alpha+\cos\beta) =\\
&= 1-2q+2\cos^2\frac{\eta}{2}\sin^2\frac{\eta}{2}(3q-1+\cos\alpha+\cos\beta) = 1-2q.
\end{aligned}$$

Аналогичными вычислениями можно показать, что

$$\begin{aligned}
{}_E\langle\varphi_1^{0_{L_a}}|\varphi_1^{0_{L_a}}\rangle_E &= {}_E\langle\varphi_1^{1_{L_a}}|\varphi_1^{1_{L_a}}\rangle_E =\\
&= {}_E\langle\varphi_1^{0_{L_b}}|\varphi_1^{0_{L_b}}\rangle_E = {}_E\langle\varphi_1^{1_{L_b}}|\varphi_1^{1_{L_b}}\rangle_E =\\
&= {}_E\langle\varphi_1^{0_{R_a}}|\varphi_1^{0_{R_a}}\rangle_E = {}_E\langle\varphi_1^{1_{R_a}}|\varphi_1^{1_{R_a}}\rangle_E =\\
&= {}_E\langle\varphi_1^{0_{R_b}}|\varphi_1^{0_{R_b}}\rangle_E = {}_E\langle\varphi_1^{1_{R_b}}|\varphi_1^{1_{R_b}}\rangle_E = 1-2q,
\end{aligned} \tag{140}$$

$$\begin{aligned}
{}_E\langle\varphi_2^{0_{L_a}}|\varphi_2^{0_{L_a}}\rangle_E &= {}_E\langle\varphi_2^{1_{L_a}}|\varphi_2^{1_{L_a}}\rangle_E =\\
&= {}_E\langle\varphi_2^{0_{L_b}}|\varphi_2^{0_{L_b}}\rangle_E = {}_E\langle\varphi_2^{1_{L_b}}|\varphi_2^{1_{L_b}}\rangle_E =\\
&= {}_E\langle\varphi_2^{0_{R_a}}|\varphi_2^{0_{R_a}}\rangle_E = {}_E\langle\varphi_2^{1_{R_a}}|\varphi_2^{1_{R_a}}\rangle_E =\\
&= {}_E\langle\varphi_2^{0_{R_b}}|\varphi_2^{0_{R_b}}\rangle_E = {}_E\langle\varphi_2^{1_{R_b}}|\varphi_2^{1_{R_b}}\rangle_E = q,
\end{aligned} \tag{141}$$

$$\begin{aligned}
{}_E\langle\varphi_1^{0_{L_a}}|\varphi_1^{0_{L_b}}\rangle_E &= {}_E\langle\varphi_1^{1_{L_a}}|\varphi_1^{1_{L_b}}\rangle_E =\\
&= {}_E\langle\varphi_1^{0_{R_a}}|\varphi_1^{0_{R_b}}\rangle_E = {}_E\langle\varphi_1^{1_{R_a}}|\varphi_1^{1_{R_b}}\rangle_E =\\
&= (1-2q)\cos\alpha,
\end{aligned} \tag{142}$$

$$\begin{aligned}
{}_E\langle\varphi_2^{0_{L_a}}|\varphi_2^{0_{L_b}}\rangle_E &= {}_E\langle\varphi_2^{1_{L_a}}|\varphi_2^{1_{L_b}}\rangle_E =\\
&= {}_E\langle\varphi_2^{0_{R_a}}|\varphi_2^{0_{R_b}}\rangle_E = {}_E\langle\varphi_2^{1_{R_a}}|\varphi_2^{1_{R_b}}\rangle_E = q\cos\beta.
\end{aligned} \tag{143}$$

Для вероятности ошибки и правильного исхода окончательно находим

$$Q = \frac{q}{(1-2q)\sin^2\eta + q\cos^2\eta + q}. \tag{144}$$

Таким образом, величина классической пропускной способности канала связи Алиса–Боб равна $C(Q)$, где вероятность ошибки Q определяется формулой (144).

3.2.5. Состояния подслушивателя

Для вычисления информации подслушивателя о ключе потребуется частичная матрица плотности σ_E, которая возникает после измерений на приемной стороне. Поскольку исходные состояния Боб–Ева описываются запутанным состоянием (112), матрица плотности Евы зависит от исходов измерений Боба. Далее для удобства вычислений введем новые нормированные состояния Евы. Обозначим

$$|\phi_1^k\rangle_E = \frac{1}{\sqrt{1-2q}}|\varphi_1^k\rangle_E, \quad |\phi_2^k\rangle_E = \frac{1}{\sqrt{q}}|\varphi_2^k\rangle_E,$$

$$|\phi_3^k\rangle_E = \frac{1}{\sqrt{q}}|\varphi_3^k\rangle_E,$$

$$k \in \{0_{L_a}, 0_{L_b}, 1_{L_a}, 1_{L_b}, 0_{R_a}, 0_{R_b}, 1_{R_a}, 1_{R_b}\}.$$

Теперь выражения (123)–(125) можно переписать в следующем виде:

$$\begin{aligned}
{}_E\langle\phi_1^{0_{L_a}}|\phi_1^{0_{L_a}}\rangle_E &= {}_E\langle\phi_1^{1_{L_a}}|\phi_1^{1_{L_a}}\rangle_E =\\
&= {}_E\langle\phi_1^{0_{L_b}}|\phi_1^{0_{L_b}}\rangle_E = {}_E\langle\phi_1^{1_{L_b}}|\phi_1^{1_{L_b}}\rangle_E = 1,
\end{aligned} \tag{145}$$

$$
{}_E\langle\phi_2^{0_{L_a}}|\phi_2^{0_{L_a}}\rangle_E = {}_E\langle\phi_2^{1_{L_a}}|\phi_2^{1_{L_a}}\rangle_E = \\
= {}_E\langle\phi_2^{0_{L_b}}|\phi_2^{0_{L_b}}\rangle_E = {}_E\langle\phi_2^{1_{L_b}}|\phi_2^{1_{L_b}}\rangle_E = 1, \quad (146)
$$

$$
{}_E\langle\phi_1^{0_{L_a}}|\phi_1^{0_{L_b}}\rangle_E = {}_E\langle\phi_1^{1_{L_a}}|\phi_1^{1_{L_b}}\rangle_E = \cos\alpha, \quad (147)
$$

$$
{}_E\langle\phi_2^{0_{L_a}}|\phi_2^{0_{L_b}}\rangle_E = {}_E\langle\phi_2^{1_{L_a}}|\phi_2^{1_{L_b}}\rangle_E = \cos\beta. \quad (148)
$$

Состояние Евы зависит от того, какое состояние было послано Алисой и какой результат был получен Бобом. Например, если послано состояние $|0^{L_a}\rangle$, то состояние Евы есть

$$
\sigma_E^{0^{L_a}} = \frac{\sqrt{\mathcal{M}_0^{L_a}}|0^{L_a}\rangle_{BE}{}_{BE}\langle 0_{L_a}|\sqrt{\mathcal{M}_0^{L_a}}^{\dagger}}{{}_{BE}\langle 0^{L_a}|\mathcal{M}_0^{L_a}|0^{L_a}\rangle_{BE}} = \\
= \frac{1}{(1-2q)\sin^2\eta + q\cos^2\eta} \times \\
\times \Big[(1-2q)\sin^2\eta|\phi_1^{0_{L_a}}\rangle_E{}_E\langle\phi_1^{0_{L_a}}| + \\
+ q\cos^2\eta|\phi_2^{0_{L_a}}\rangle_E{}_E\langle\phi_2^{0_{L_a}}| - \\
- \sqrt{q(1-2q)}\sin\eta\cos\eta(|\phi_1^{0_{L_a}}\rangle_E{}_E\langle\phi_2^{0_{L_a}}| + \\
+ |\phi_2^{0_{L_a}}\rangle_E{}_E\langle\phi_1^{0_{L_a}}|)\Big], \quad (149)
$$

если Бобом был получен правильный отсчет. Аналогично, если Бобом был получен ошибочный результат, то матрица плотности Евы имеет вид

$$
\sigma_{E_{err}}^{0^{L_a}} = |\phi_2^{0_{L_a}}\rangle_E{}_E\langle\phi_2^{0_{L_a}}|. \quad (150)
$$

Поскольку исходы измерений у Боба с неопределенным результатом отбрасываются, соответствующую матрицу плотности Евы не выписываем. Окончательно для матрицы плотности Евы после отбрасывания исходов с неопределенным результатом имеем

$$
\sigma_E^{0_{L_a}} = \frac{1}{(1-2q)\sin^2\eta + q\cos^2\eta + q} \times \\
\times \Big[(1-2q)\sin^2\eta|\phi_1^{0_{L_a}}\rangle_E{}_E\langle\phi_1^{0_{L_a}}| + \\
+ q(\cos^2\eta+1)|\phi_2^{0_{L_a}}\rangle_E{}_E\langle\phi_2^{0_{L_a}}| - \\
- \sqrt{q(1-2q)}\sin\eta\cos\eta(|\phi_1^{0_{L_a}}\rangle_E{}_E\langle\phi_2^{0_{L_a}}| + \\
+ |\phi_2^{0_{L_a}}\rangle_E{}_E\langle\phi_1^{0_{L_a}}|)\Big]. \quad (151)
$$

Аналогичное выражение имеет матрица плотности Евы, когда Алисой было послано состояние, отвечающее 1. Дальнейшая задача состоит в определении максимально возможного количества информации, которое Ева может извлечь из ансамбля квантовых состояний (149)–(151). Для упрощения дальнейших выкладок введем следующие обозначения:

$$
\gamma = \frac{(1-2q)\sin^2\eta}{(1-2q)\sin^2\eta + q\cos^2\eta + q}, \\
\delta = \frac{q(\cos^2\eta+1)}{(1-2q)\sin^2\eta + q\cos^2\eta + q}, \quad (152)
$$

$$
c = \frac{\sqrt{q(1-2q)}\sin\eta\cos\eta}{(1-2q)\sin^2\eta + q\cos^2\eta + q}. \quad (153)
$$

Тогда матрицы плотности Евы при посылке состояний $|0^{L_a}\rangle$ и $|1^{L_a}\rangle$ соответственно равны

$$
\sigma_E^{0^{L_a}} = \gamma|\phi_1^{0_{L_a}}\rangle_E{}_E\langle\phi_1^{0_{L_a}}| + \delta|\phi_2^{0_{L_a}}\rangle_E{}_E\langle\phi_2^{0_{L_a}}| - \\
- c(|\phi_1^{0_{L_a}}\rangle_E{}_E\langle\phi_2^{0_{L_a}}| + |\phi_2^{0_{L_a}}\rangle_E{}_E\langle\phi_1^{0_{L_a}}|), \quad (154)
$$

$$
\sigma_E^{1^{L_a}} = \gamma|\phi_1^{1_{L_a}}\rangle_E{}_E\langle\phi_1^{1_{L_a}}| + \delta|\phi_2^{1_{L_a}}\rangle_E{}_E\langle\phi_2^{1_{L_a}}| - \\
- c(|\phi_1^{1_{L_a}}\rangle_E{}_E\langle\phi_2^{1_{L_a}}| + |\phi_2^{1_{L_a}}\rangle_E{}_E\langle\phi_1^{1_{L_a}}|). \quad (155)
$$

3.2.6. Вычисление информации подслушивателя

Информация подслушивателя о ключе определяется величиной Холево, которая совпадает с классической пропускной способностью квантового канала связи Алиса–Ева, с учетом (149)–(151) имеем

$$
\chi(\sigma_E^{L_a}) = S\left(\frac{1}{2}(\sigma_E^{0_{L_a}} + \sigma_E^{1_{L_a}})\right) - \\
- \frac{1}{2}S(\sigma_E^{0_{L_a}}) - \frac{1}{2}S(\sigma_E^{1_{L_a}}), \quad (156)
$$

где

$$
\sigma_E^{L_a} = \frac{1}{2}(\sigma_E^{0_{L_a}} + \sigma_E^{1_{L_a}}).
$$

Для подсчета информации Холево требуется найти собственные значения трех матриц: $\sigma_E^{L_a}$, $\sigma_E^{0_{L_a}}$ и $\sigma_E^{1_{L_a}}$. Две последние матрицы, как нетрудно видеть, имеют одинаковые собственные значения и могут быть выписаны явным образом:

$$
\lambda_{1,2} = \frac{1}{2}\left(1 \pm \sqrt{1+4c^2-4\gamma\delta}\right).
$$

Чтобы вычислить собственные значения матрицы $\sigma_E^{L_a}$, найдем нули определителя матрицы $\sigma_E^{L_a} - \lambda I$.

Выпишем элементы этой матрицы в базисе $\{|\phi_1^{0_{L_a}}\rangle_E, |\phi_1^{1_{L_a}}\rangle_E, |\phi_2^{0_{L_a}}\rangle_E, |\phi_2^{1_{L_a}}\rangle_E\}$:

$$
\begin{aligned}
&{}_E\langle\phi_1^{0_{L_a}}|(\sigma_E^{L_a}-\lambda I)|\phi_1^{0_{L_a}}\rangle_E = \\
&\qquad = \frac{1}{2}\gamma(1+|{}_E\langle\phi_1^{0_{L_a}}|\phi_1^{1_{L_a}}\rangle_E|^2) + \\
&\qquad + \frac{1}{2}\delta|{}_E\langle\phi_1^{0_{L_a}}|\phi_2^{1_{L_a}}\rangle_E|^2 - \\
&-c_E\langle\phi_1^{0_{L_a}}|\phi_1^{1_{L_a}}\rangle_E{}_E\langle\phi_1^{0_{L_a}}|\phi_2^{1_{L_a}}\rangle_E - \lambda = m_{11}-\lambda, \\
&{}_E\langle\phi_1^{0_{L_a}}|(\sigma_E^{L_a}-\lambda I)|\phi_1^{1_{L_a}}\rangle_E = \\
&\quad = \gamma_E\langle\phi_1^{0_{L_a}}|\phi_1^{1_{L_a}}\rangle_E - c_E\langle\phi_1^{0_{L_a}}|\phi_2^{1_{L_a}}\rangle_E - \\
&\qquad - \lambda_E\langle\phi_1^{0_{L_a}}|\phi_1^{1_{L_a}}\rangle_E = m_{12}-\lambda n_{12}, \\
&{}_E\langle\phi_1^{0_{L_a}}|(\sigma_E^{L_a}-\lambda I)|\phi_2^{0_{L_a}}\rangle_E = \\
&\quad = \frac{1}{2}\gamma_E\langle\phi_1^{0_{L_a}}|\phi_1^{1_{L_a}}\rangle_E{}_E\langle\phi_1^{1_{L_a}}|\phi_2^{0_{L_a}}\rangle_E + \\
&\quad + \frac{1}{2}\delta_E\langle\phi_1^{0_{L_a}}|\phi_2^{1_{L_a}}\rangle_E{}_E\langle\phi_2^{0_{L_a}}|\phi_2^{1_{L_a}}\rangle_E - \\
&-\frac{1}{2}c(1+{}_E\langle\phi_1^{0_{L_a}}|\phi_1^{1_{L_a}}\rangle_E{}_E\langle\phi_2^{0_{L_a}}|\phi_2^{1_{L_a}}\rangle_E + \\
&\qquad + |{}_E\langle\phi_1^{0_{L_a}}|\phi_2^{1_{L_a}}\rangle_E|^2) = m_{13}, \qquad (157)\\
&{}_E\langle\phi_1^{0_{L_a}}|(\sigma_E^{L_a}-\lambda I)|\phi_2^{1_{L_a}}\rangle_E = \\
&\qquad = \frac{1}{2}{}_E\langle\phi_1^{0_{L_a}}|\phi_2^{1_{L_a}}\rangle_E - \\
&-\frac{1}{2}c({}_E\langle\phi_1^{0_{L_a}}|\phi_1^{1_{L_a}}\rangle_E + {}_E\langle\phi_2^{0_{L_a}}|\phi_2^{1_{L_a}}\rangle_E) - \\
&\qquad - \lambda_E\langle\phi_1^{0_{L_a}}|\phi_2^{1_{L_a}}\rangle_E = m_d-\lambda n_d, \\
&{}_E\langle\phi_2^{0_{L_a}}|(\sigma_E^{L_a}-\lambda I)|\phi_2^{0_{L_a}}\rangle_E = \\
&\qquad = \frac{1}{2}\gamma|{}_E\langle\phi_1^{1_{L_a}}|\phi_2^{0_{L_a}}\rangle_E|^2 + \\
&\qquad + \frac{1}{2}\delta(1+|{}_E\langle\phi_2^{0_{L_a}}|\phi_2^{1_{L_a}}\rangle_E|^2) - \\
&-c_E\langle\phi_2^{0_{L_a}}|\phi_2^{1_{L_a}}\rangle_E{}_E\langle\phi_2^{0_{L_a}}|\phi_1^{1_{L_a}}\rangle_E - \lambda = m_{33}-\lambda, \\
&{}_E\langle\phi_2^{0_{L_a}}|(\sigma_E^{L_a}-\lambda I)|\phi_2^{1_{L_a}}\rangle_E = \\
&\quad = \delta_E\langle\phi_2^{0_{L_a}}|\phi_2^{1_{L_a}}\rangle_E - c_E\langle\phi_1^{0_{L_a}}|\phi_2^{1_{L_a}}\rangle_E - \\
&\qquad - \lambda_E\langle\phi_2^{0_{L_a}}|\phi_2^{1_{L_a}}\rangle_E = m_{34}-\lambda n_{34}.
\end{aligned}
$$

Из (140)–(143) можно вывести следующие соотношения, встречающиеся среди выражений для элементов матрицы $\sigma_E^{L_a}$ в указанном базисе:

$$
\begin{aligned}
&{}_E\langle\phi_1^{0_{L_a}}|\phi_1^{1_{L_a}}\rangle_E = \cos^2\eta + \cos\alpha\sin^2\eta, \\
&{}_E\langle\phi_2^{0_{L_a}}|\phi_2^{1_{L_a}}\rangle_E = -\cos^2\eta + \cos\beta\sin^2\eta, \\
&{}_E\langle\phi_2^{0_{L_a}}|\phi_1^{1_{L_a}}\rangle_E = {}_E\langle\phi_1^{0_{L_a}}|\phi_2^{1_{L_a}}\rangle_E = \\
&= \frac{\sqrt{1-2q}}{\sqrt{q}}\sin\eta\cos\eta(1-\cos\alpha) = \\
&= \frac{\sqrt{q}}{\sqrt{1-2q}}\sin\eta\cos\eta(1+\cos\beta).
\end{aligned} \qquad (158)
$$

В итоге в силу симметрии и равенства некоторых элементов матрица получается следующей структуры:

$$
G = \begin{pmatrix}
m_{11}-\lambda & m_{12}-\lambda n_{12} & m_{13} & m_d-\lambda n_d \\
m_{12}-\lambda n_{12} & m_{11}-\lambda & m_d-\lambda n_d & m_{13} \\
m_{13} & m_d-\lambda n_d & m_{33}-\lambda & m_{34}-\lambda n_{34} \\
m_d-\lambda n_d & m_{13} & m_{34}-\lambda n_{34} & m_{33}-\lambda
\end{pmatrix},
$$

и для нахождения ее собственных значений требуется решить алгебраическое уравнение четвертой степени. Методы решения подобных уравнений хорошо известны.

3.2.7. Обсуждение результатов для случая неортогональных состояний внутри базиса

Критическая ошибка Q_c, до которой можно передавать ключи и гарантировать их секретность, с учетом (5) и (39), (41) определяется уравнением

$$
1-h(Q_c) = \max_{c_\alpha}\chi(Q_c, c_\alpha), \qquad (159)
$$

где параметр c_α определяется Евой так, чтобы максимизировать свою информацию о ключе. Длина секретного ключа, который может быть получен из оставшейся последовательности длины n, определяется как

$$
\frac{r}{n} = 1-h(Q)-\max_{c_\alpha}\chi(Q, c_\alpha). \qquad (160)
$$

Как было показано выше, протокол с ортогональными состояниями внутри базисов имеет два независимых параметра Q и q. При этом эффективно информация о ключе Боба зависит только от ошибки Q, а информация Евы эффективно зависит от q — вероятности отсчетов в контрольных временных окнах. В протоколе с неортогональными сигнальными состояниями внутри базисов из-за другой конфигурации векторов (рис. 3) величина ошибки Q и вероятность q оказываются однозначно связанными. Параметр $\cos\alpha$ — угол между состояниями Евы, от которого зависит информация Евы, — напрямую не связан с отсчетами в контрольных временных окнах (является ненаблюдаемым для Боба), поэтому на плоскости (Q, q) имеет место не область, а линия $q = q(Q)$ (см. формулу (144)) (рис. 4).

3.2.8. Случай несимметричной атаки

В случае оптимальной симметричной атаки Евы величина вероятности ошибки Q и вероятности от-

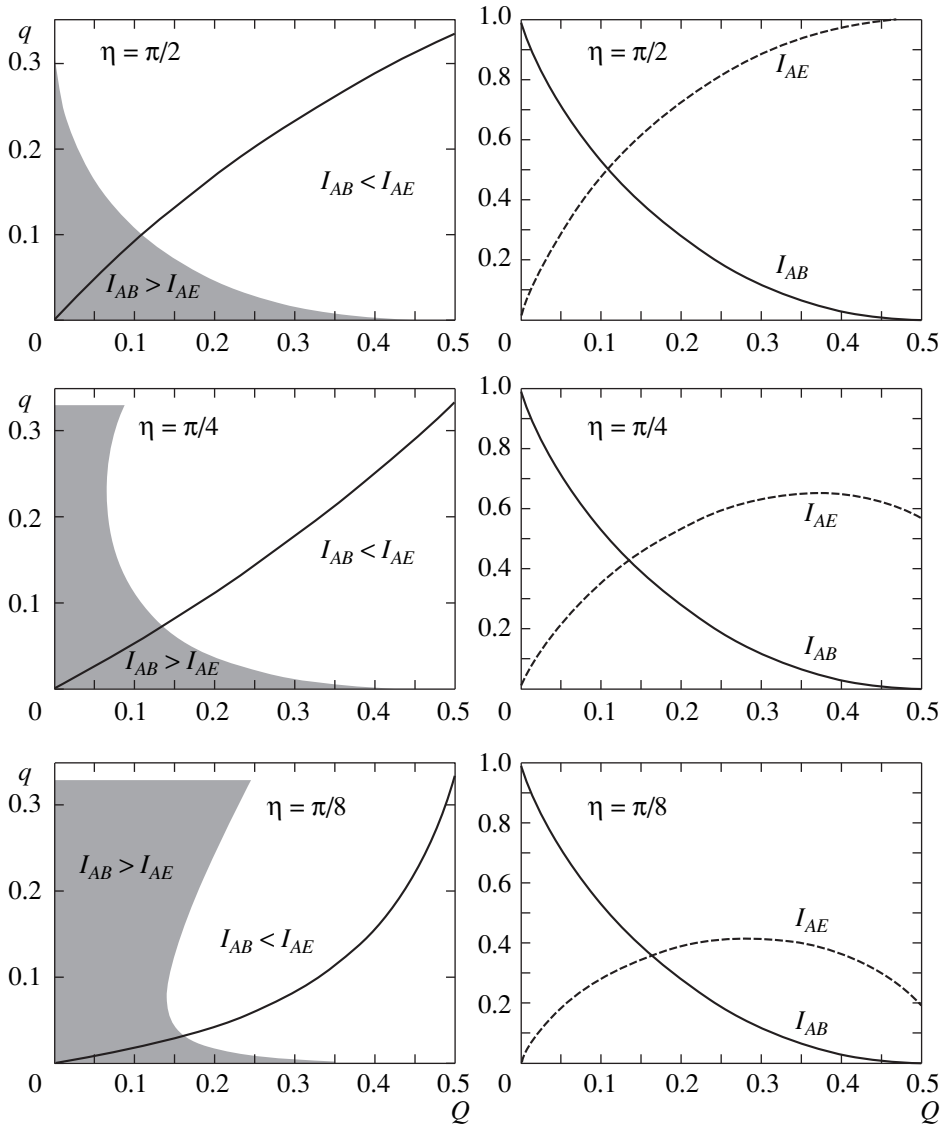

Рис. 4. Поведение взаимных информаций Алиса–Ева и Алиса–Боб на линии $q(Q)$. Левые графики — области секретности. Заштрихованные области отвечают $I_{AB}(Q,q) > I_{AE}(Q,q)$, поскольку взаимная информация Алиса–Ева зависит только от q, а взаимная информация Алиса–Боб — только от Q. Оптимальной атаке отвечает зависимость $q(Q)$, которая дается формулой (144). Правые графики — поведение взаимных информаций на линии $q(Q)$ из формулы (144). На всех графиках уже сделана максимизация взаимной информации I_{AE} (см. (159), (160)) по параметру c_α

счетов в контрольных временных окнах q одинаковы в левом и правом базисах. В реальной ситуации может оказаться, что данные величины различны в разных базисах. Можно снять требование симметричности атаки в левом и правом базисах и ввести новый параметр p, отвечающий за отсчеты в контрольном временном окне для правого базиса (в то время как в левом базисе эта величина по-прежнему связана с параметром q),

$$p_{X|Y}(0^{L_a}|3) = {}_E\langle\varphi_3^{0^{L_a}}|\varphi_3^{0^{L_a}}\rangle_E = {}_E\langle\varphi_3^{1^{L_a}}|\varphi_3^{1^{L_a}}\rangle_E = {}_E\langle\varphi_3^{0^{L_b}}|\varphi_3^{0^{L_b}}\rangle_E = {}_E\langle\varphi_3^{1^{L_b}}|\varphi_3^{1^{L_b}}\rangle_E = q, \quad (161)$$

$$p_{X|Y}(0^{R_a}|3) = {}_E\langle\varphi_3^{0^{R_a}}|\varphi_3^{0^{R_a}}\rangle_E = {}_E\langle\varphi_3^{1^{R_a}}|\varphi_3^{1^{R_a}}\rangle_E = {}_E\langle\varphi_3^{0^{R_b}}|\varphi_3^{0^{R_b}}\rangle_E = {}_E\langle\varphi_3^{1^{R_b}}|\varphi_3^{1^{R_b}}\rangle_E = p. \quad (162)$$

Для состояний $|\psi_j^i\rangle$ в разложении (123) это означает, что

$$
{}_E\langle\psi_1^3|\psi_1^3\rangle_E = {}_E\langle\psi_2^3|\psi_2^3\rangle_E = q,
$$
$$
{}_E\langle\psi_2^1|\psi_2^1\rangle_E = {}_E\langle\psi_3^1|\psi_3^1\rangle_E = p,
$$

а из соображений симметрии и требования нормировки состояний следует, что

$$
{}_E\langle\psi_1^1|\psi_1^1\rangle_E = {}_E\langle\psi_2^2|\psi_2^2\rangle_E = {}_E\langle\psi_3^3|\psi_3^3\rangle_E = 1-p-q,
$$
$$
{}_E\langle\psi_1^2|\psi_1^2\rangle_E = p, \quad {}_E\langle\psi_3^2|\psi_3^2\rangle_E = q.
$$

Результаты измерений на приемной стороне будут иметь следующие вероятности:

$$
\begin{aligned}
p_{X|Y}(0^{L_a}|0) &= \frac{(1-p-q)\sin^2\eta + p\cos^2\eta}{1+\cos\eta},\\
p_{X|Y}(0^{L_a}|1) &= \frac{p}{1+\cos\eta},\\
p_{X|Y}(0_{L_a}|3) &= q.
\end{aligned}
\tag{163}
$$

В свою очередь, соотношение (126) будет выглядеть как

$$
\begin{aligned}
1-2p-q &= (1-p-q)\cos\alpha_L + p\cos\beta_L,\\
1-p-2q &= (1-p-q)\cos\alpha_R + q\cos\beta_R.
\end{aligned}
\tag{164}
$$

Здесь $\cos\alpha_i$, $\cos\beta_j$ — значения параметров для левых и правых пар базисов: их уже нельзя приравнять друг другу, так как получится, что $q=p$, а это соответствует уже рассмотренному симметричному случаю.

Ошибка Боба в левом базисе после отбрасывания исходов с неопределенным результатом и посылок с отсчетами в контрольных временных окнах будет равна

$$
Q_L = \frac{p}{(1-p-q)\sin^2\eta + p\cos^2\eta + p},
\tag{165}
$$

аналогично в правом базисе —

$$
Q_R = \frac{q}{(1-p-q)\sin^2\eta + q\cos^2\eta + q}.
\tag{166}
$$

Если теперь строить на плоскости область секретности протокола в левом базисе, то эта область должна задаваться графиком зависимости от ошибки на приемной стороне Q_L и отсчетов в контрольном временном слоте q. Из формулы (165) видно, что в этом случае второй параметр Евы p явным образом выражается через величины Q_L и q:

$$
p = \frac{Q_L(1-q)\sin^2\eta}{1-2Q_L\cos^2\eta}.
$$

Это означает, что для такой атаки при получении точки (Q_L, q) будет автоматически получена точка (Q_R, p) на аналогичном графике в правом базисе, и для этой точки также можно определить, возможна ли передача ключа при данном наборе параметров правого базиса. Поэтому области секретности можно строить по данным только левого (или соответственно только правого) набора базисов. Алгоритм построения такой: для каждой точки (Q_L, q) необходимо вычислить длину ключа в левом базисе, а также параметры Q_R и q, из которых аналогичным образом находится длина ключа в правом наборе базисов.

На рис. 5 показаны графики зависимости длины ключа от параметров левого базиса для значения угла $\eta = \pi/6$.

4. КРИТИЧЕСКАЯ ДЛИНА ПЕРЕДАЧИ КЛЮЧЕЙ: НЕОДНОФОТОННЫЙ ИСТОЧНИК, НЕИДЕАЛЬНЫЕ ФОТОДЕТЕКТОРЫ, КВАНТОВЫЙ КАНАЛ СВЯЗИ С ЗАТУХАНИЕМ

4.1. Случай ортогональных состояний

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

Пусть заданы длина квантового канала связи L, потери в канале α, среднее число фотонов в лазерном импульсе μ, эффективности фотодетекторов $\eta_{1,2}$ и собственные темновые шумы в них $p_{1,2}$. Доля посылок с одним фотоном есть

$$
p_1 = \mu e^{-\mu},
\tag{167}
$$

соответственно вероятность посылок с числом фотонов более одного есть

$$
p_{>1} = 1 - e^{-\mu} - \mu e^{-\mu},
\tag{168}
$$

где $e^{-\mu}$ — вероятность вакуумной компоненты, т. е. состояния без фотонов. Доля фотонов, которые достигнут приемной стороны равна

$$
(p_1 + p_{>1})10^{-\alpha L/10},
\tag{169}
$$

где коэффициент поглощения для стандартных одномодовых оптических волокон типа SMF-28 составляет $\alpha = 0.18$—0.2 дБ/км. Пакеты с разным числом фотонов, вообще говоря, имеют разную вероятность поглощения. Вероятность достичь приемной стороны хотя бы одному фотону из k-фотонного пакета равна $1 - p_{loss}^k$ (в режиме линейного поглощения), что больше, чем $1 - p_{loss}$ (p_{loss} — вероятность поглощения одного фотона в линии). Наша оценка является консервативной в пользу Евы, поскольку число долетевших фотонов меньше и это позволяет Еве блокировать бóльшее число однофотонных посылок.

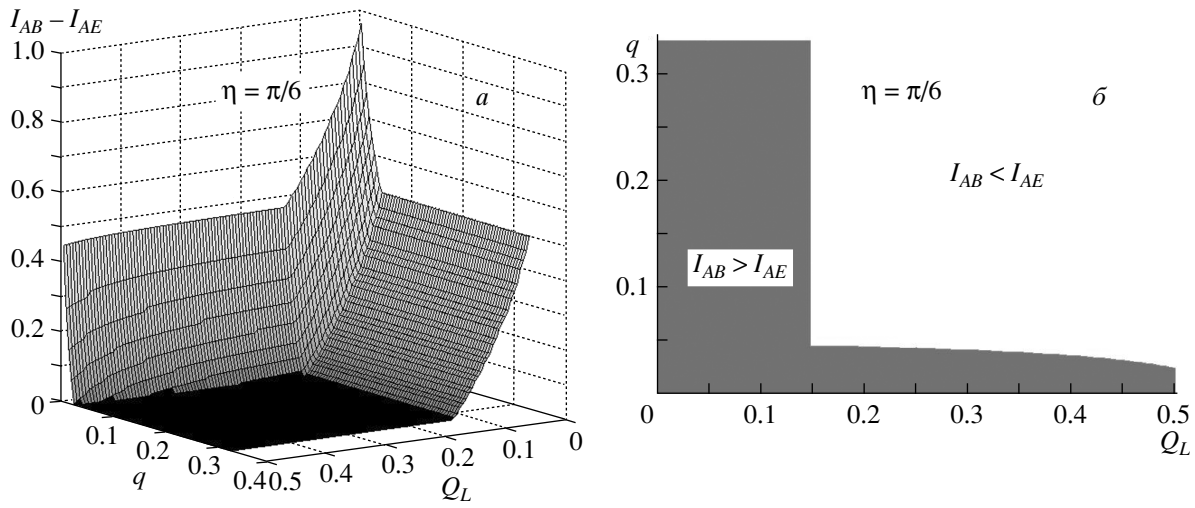

Рис. 5. *а*) Длина секретного ключа в пересчете на одну позицию как функция параметров Q_L, q. *б*) Области секретности. Серая область отвечает $I_{AB}(Q_L, q) > I_{AE}(Q_L, q)$. На всех графиках уже сделана максимизация взаимной информации I_{AE} (см. (159), (160)) по параметрам c_{α_L} и c_{β_R} (см. (164))

Вероятность долета фотонов (169) является константой протокола, которая подсчитывается легитимными пользователями заранее перед передачей ключей. Знание этой величины позволяет контролировать среднее число регистрируемых посылок на приемной стороне, которое Ева не должна изменять, в противном случае протокол будет прерван. Вероятность поглощения в канале связи составляет

$$(p_1 + p_{>1})(1 - 10^{-\alpha L/10}). \tag{170}$$

Этой долей фотонов подслушиватель может манипулировать по своему усмотрению.

Стратегия подслушивателя сводится к следующему. Не изменяя общей доли посылок, достигающих приемной стороны, подслушиватель может блокировать часть посылок, когда в канале присутствует один фотон, а часть однофотонных посылок подслушивателю придется оставить, чтобы не изменить общей вероятности достижения приемной стороны.

Доля однофотонных посылок, которые Ева вынуждена оставить, составляет

$$p_Q = p_1 - (p_1 + p_{>1})(1 - 10^{-\alpha L/10}) = \\ = \mu e^{-\mu} - (1 - e^{-\mu})(1 - 10^{-\alpha L/10}). \tag{171}$$

Доля однофотонных посылок, которые Ева блокирует, есть $p_1 - p_Q$. Соответственно, Ева оставляет все многофотонные посылки. Доля таких посылок с учетом формул (169)–(171) равна

$$p_{>1} = 1 - e^{-\mu} - \mu e^{-\mu}. \tag{172}$$

Эффективная ошибка на приемной стороне возникает только от тех однофотонных посылок, которые Ева из-за недостаточных потерь в линии связи не может блокировать. Для эффективной вероятности ошибки $\tilde{Q}$ имеем

$$\tilde{Q} = Q\frac{(1 - q/2)p_Q}{(1 - q/2)p_Q + p_{>1}} + \\ + 0\frac{p_1}{(1 - q/2)p_Q + p_{>1}}. \tag{173}$$

Смысл выражения (173) сводится к тому, что ошибки возникают только из однофотонных посылок, которые Ева не может блокировать из-за недостаточных потерь в линии связи. Длина ключа в этом случае составляет

$$\frac{r}{n} = 1 - h(\tilde{Q}) - \frac{(1 - q/2)p_Q h(\zeta) + p_{>1}}{(1 - q/2)p_Q + p_{>1}}. \tag{174}$$

Критическая длина квантового канала связи L_1, при которой Ева может блокировать все однофотонные посылки, определяется из условия

$$L_1 = -\frac{10}{\alpha}\log_{10}\left(1 - \frac{\mu e^{-\mu}}{1 - e^{-\mu}}\right). \tag{175}$$

Состояния внутри базисов ортогональны (достоверно различимы), поэтому из многофотонных посылок, оставляя одно состояние у себя в квантовой памяти до стадии раскрытия базисов легитимными пользователями, а затем измеряя уже в правильном

базисе, можно извлечь всю информацию о ключе, не производя ошибок на приемной стороне.

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

4.2. Случай неортогональных состояний

Здесь рассмотрен наиболее интересный случай неортогональных состояний внутри базисов. Пусть длина линии превышает критическую длину (175). При неортогональных состояниях даже при известном базисе Ева будет иметь лишь частичную информацию. С ростом длины линии (соответственно потерь) Ева может блокировать посылки, содержащие два, три и т. д. фотонов. Из неоднофотонных посылок Еве выгодней оставить у себя как можно большее число фотонов, а один фотон из каждой многофотонной посылки отправить к Бобу через свой канал с меньшими потерями (в пределе без потерь). Чем больше фотонов из многофотонных посылок Ева оставит у себя, тем больше информации она сможет получить. Дальнейшая задача будет сводиться к вычислению информации Евы в зависимости от длины линии связи.

Будем считать, что фотодетекторы на приемной стороне не различают число фотонов. Это имеет место для лавинных фотодетекторов на основе InGaAs:P, работающих в стробируемом режиме. Отметим, что на сегодняшний день известны эксперименты со сверхпроводящими фотодетекторами, которые способны различать посылки с числом фотонов до трех [42].

Ниже показано, что протокол позволяет распределять секретные ключи при длинах линии связи, когда $L_1 < L < L_5$. При больших длинах линии связи ($L > L_5$), когда Ева может блокировать все посылки вплоть до пятифотонных, распределение секретных ключей становится невозможным.

В квантовой криптографии линия связи за пределами передающей и приемной станций не контролируется, поэтому никто не запрещает Еве иметь доступ к исходным, неискаженным затуханием состояниям, покидающим приемную станцию. Данные информационные квазиоднофотонные состояния получаются ослаблением когерентного состояния. Поскольку от посылки к посылке относительная фаза в состояниях не фиксирована, подслушиватель «видит» в канале связи усредненное по фазе когерентное состояние, которое описывается матрицей плотности

$$\sigma_B(i,b) = \sum_{k=0}^{\infty} p_k (|i^b\rangle_A^{\otimes k})({}^{\otimes k}{}_A\langle i^b|), \quad p_k = \frac{\mu^k}{k!}, \quad i = 0,1, \quad b = +L, \times L, +R, \times R, \tag{176}$$

где $|i^b\rangle_A$ — исходные состояния Алисы в (108)–(111), μ — среднее число фотонов в когерентном состоянии. Рассмотрение, представленное ниже, применимо и для источника с произвольным распределением по числу фотонов, а не только для когерентного состояния.

При $L > L_1$ все однофотонные посылки блокированы и Ева, используя неразрушающие измерения, определяет число фотонов k в каждой посылке. Один из k фотонов она направляет Бобу через свой канал без потерь, а себе оставляет $k-1$ фотонов для измерений после раскрытия базисов Алисой и Бобом. После отбрасывания результатов с неопределенным исходом информация Боба в битах в пересчете на одну оставленную позицию составляет $I(A;B) = 1$ (при идеальных фотодетекторах). Учтем теперь неидеальность фотодетекторов. В этом случае Боб имеет дело, как и ранее, с однофотонными состояниями. На приемной стороне Боб случайно и равновероятно выбирает измерения в одном из двух базисов. Формально измерения описываются следующими разложениями единицы:

$$I_B = \mathcal{M}_{0^b} + \mathcal{M}_{1^b} + A_{?,b},$$
$$\mathcal{M}_{0^b} = \frac{I - |1^b\rangle\langle 1^b|}{1 + |\langle 0^b|1,b\rangle|}, \quad \mathcal{M}_{1^b} = \frac{I - |0^b\rangle\langle 0^b|}{1 + |\langle 0^b|1^b\rangle|}, \tag{177}$$
$$\mathcal{M}_{?,b} = I - \mathcal{M}_{0^b} - \mathcal{M}_{1^b}.$$

Отсчеты с неопределенным исходом отбрасываются. Вероятность отсчетов с определенным исходом с учетом формул (108)–(111) и (177) есть

$$P\{|0^b\rangle\langle 0^b|\mathcal{M}_{0^b}\} = P\{|1^b\rangle\langle 1^b|\mathcal{M}_{1,b}\} = 1 - \cos\eta. \tag{178}$$

Доля посылок, оставшихся на приемной стороне после измерений Боба, с учетом (168)–(172) и (178), равна

$$p_{detect} = (1 - e^{-\mu} - (e^{-\mu\Gamma} - e^{-\mu}))(1 - \cos\eta). \tag{179}$$

Учтем теперь неидеальность фотодетекторов. Лавинные фотодетекторы в телекоммуникационном диапазоне длин волн 1.3–1.55 мкм работают в стробируемом режиме (фотодетектор активируется посредством подачи короткого импульса напряжения

длительности 1–2 нс в момент возможного прихода информационного состояния), поэтому темновые отсчеты с определенной вероятностью имеют место только в момент стробирования независимо от прихода состояния. В реальных системах квантовой криптографии используется обычно пара лавинных фотодетекторов (см., например, [43]), которые обозначим $\overline{D}_0$ и $\overline{D}_1$. Темновые шумы изменяют эффективную ошибку на приемной стороне. Пусть квантовые эффективности фотодетекторов равны η_0 и η_1 (обычно в этом спектральном диапазоне $\eta_{0,1} \approx 10$–$40\,\%$). Поскольку при $L > L_1$ состояния поступают на приемную сторону через модифицированный Евой канал без искажений, ошибка на приемной стороне обусловлена только темновыми шумами. Обозначим вероятности темновых отсчетов во временном окне стробирования для двух детекторов как $p_{d0}^{(0)}$ и $p_{dark}^{(1)}$.

Фотоотсчеты в детекторах $\overline{D}_0$ и $\overline{D}_1$ можно разбить на следующие множества[9]. A_0 и A_1 — множества отсчетов от информационных состояний. D_0 и D_1 — множества темновых отсчетов соответственно в детекторах $\overline{D}_0$ и $\overline{D}_1$. Напомним, что оба детектора стробируются одновременно, поэтому темновые отсчеты могут иметь место одновременно (в одном и том же стробе) в двух фотодетекторах. A_1 — множество одновременных отсчетов только от информационных состояний A_0 и темновых отсчетов D_0. A_2 — множество одновременных отсчетов только от информационных состояний A_0 и темновых отсчетов D_1. A_3 — множество одновременных отсчетов от A_0, D_0 и D_1. A_4 — множество одновременных отсчетов только D_0 и D_1. Множества A_0 и A_1 не пересекаются, поскольку Алиса посылает либо 0, либо 1. Одновременные события в одном временном стробе в одном детекторе от информационного состояния и темнового шума воспринимаются как один фотоотсчет. Одновременные фотоотсчеты в двух детекторах в одном временном стробе отбрасываются. Вероятность отсчета от информационных состояний 0 и 1 равна

$$P_{info} = \Pr\{A_0 + A_1 - A_0 \cap D_1 - A_1 \cap D_0\} = \\ = \eta_0(L) + \eta_1(L) - \eta_0(L)p_{dark}^{(0)} - \eta_1(L)p_{dark}^{(1)}. \quad (180)$$

Вероятность исходов только от темновых отсчетов равна

$$P_{dark} = P\{D_0 + D_1 - 2(D_0 \cap D_1 - A_0 \cap D_0 \cap D_1 - \\ - A_1 \cap D_0 \cap D_1) - (A_0 \cap D_0 - A_0 \cap D_0 \cap D_1) - \\ - (A_1 \cap D_0 - A_1 \cap D_0 \cap D_1) - \\ - (A_1 \cap D_1 - A_1 \cap D_0 \cap D_1) - \\ - (A_0 \cap D_1 - A_0 \cap D_0 \cap D_1)\} = \\ = p_{dark}^{(0)} + p_{dark}^{(1)} - (\eta_0(L) + \eta_1(L))(p_{dark}^{(0)} + p_{dark}^{(1)}) + \\ + 4(\eta_0(L) + \eta_1(L))p_{dark}^{(0)}p_{dark}^{(1)} - 2p_{dark}^{(0)}p_{dark}^{(1)}. \quad (181)$$

Состояния, отвечающие 0 и 1, посылаются равновероятно, поэтому только половина из каждого непересекающегося множества темновых отсчетов будет давать правильные отсчеты. Другая половина отсчетов будет ошибочной. Для вероятности ошибки на приемной стороне у Боба имеем

$$Q(L) = \frac{P_{dark}/2}{P_{info} + P_{dark}}. \quad (182)$$

Ошибка принимает особенно простое выражение при $\eta_0(L) = \eta_1(L) = \eta(L)$, $p_{dark}^{(0)} = p_{dark}^{(1)} = p_{dark}$. С точностью до линейных членов по $\eta(L)$, p_{dark} имеем

$$Q(L) = \frac{p_{dark}/2}{\eta(L) + p_{dark}}. \quad (183)$$

Так как информационные состояния достигают приемной стороны через канал Евы неискаженными, ошибка обусловлена только темновыми отсчетами и исходы с неопределенным результатом отбрасываются, поэтому взаимная информация между Алисой и Бобом равна пропускной способности классического симметричного бинарного канала связи с величиной ошибки $Q(L)$. Имеем $C(Q) = 1 - h(Q(L))$.

Рассмотрим теперь действия подслушивателя. При заданной длине линии связи Ева блокирует посылки либо полностью, либо частично с наименьшим числом фотонов. Из оставшихся она один фотон посылает Бобу, а остальные оставляет у себя. Вероятность потерь — доля посылок, исчезающих в канале связи длины L, — имеет вид

$$p_{loss}(L) = \sum_{k=1}^{\infty} p_k(1 - \Gamma(L))^k, \\ \Gamma(L) = 10^{-\alpha L/10}. \quad (184)$$

Здесь $\alpha \approx 0.2$ дБ/км. Для когерентного состояния доля потерянных посылок составляет $p_{loss}(L) = e^{-\mu\Gamma} - e^{-\mu}$ (при $L \to \infty$, $\Gamma(L) \to 0$, $p_{loss}(L) \to 1 - e^{-\mu}$ — исходная общая доля непустых посылок). При больших длинах ($L > L_1$, $p_{loss}(L_1) = p_1$) Ева может блокировать все однофотонные посылки, при атаке на которые она неизбежно производила

[9] Темновые отсчеты подсчитываются аналогично методу, изложенному в работе [43].

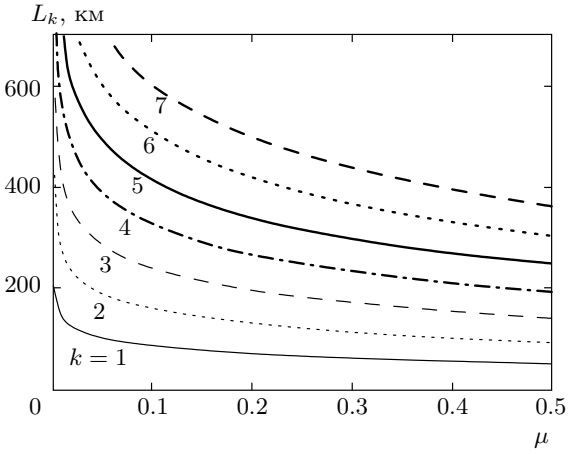

Рис. 6. Зависимости длины линии L_k от среднего числа фотонов μ в когерентном состоянии, начиная с которых Ева может блокировать посылки, содержащие k фотонов

бы ошибки на приемной стороне. С дальнейшим ростом длины линии подслушиватель может блокировать двух-, трех-, ... k-фотонные посылки. Иначе говоря, при длинах $L < L_1 < L < L_2 < L \ldots < L_k \ldots$ Ева может блокировать частично, а начиная с некоторой длины — полностью, k-фотонные посылки. Зависимости длин L_k от среднего числа фотонов μ в когерентном состоянии приведены на рис. 6.

Доля оставшихся посылок при длине L, которые Ева не может блокировать и вынуждена сохранить, составляет

$$p_k(L) = p_k(1-\theta(p_{loss}(k,L))) + (p_k - p_{loss}(k,L)) \times \\ \times \theta(p_{loss}(k,L))\theta(p_k - p_{loss}(k,L)), \quad (185)$$

где

$$p_{loss}(k,L) = p_{loss}(L) - \sum_{m=1}^{k-1} p_m.$$

Далее из каждой посылки, содержащей $k > 1$ фотонов, Ева один фотон направляет Бобу через свой канал связи с меньшими потерями (в предельном случае вообще без потерь), а остальные оставляет у себя в квантовой памяти до процедуры разглашения базисов легитимными пользователями. Однако даже после разглашения базисов из-за неортогональности состояний внутри базиса Ева не будет достоверно знать каждый передаваемый бит.

При длине линии связи $L > L_1$ после разглашения базисов Ева имеет дело с ансамблем квантовых состояний:

$$\sigma_E(0^b) = \sum_{k=2}^{\infty} p_k(L)(|0^b\rangle_A^{\otimes(k-1)})(^{\otimes(k-1)}{}_A\langle 0^b|), \\ \sigma_E(1^b) = \sum_{k=2}^{\infty} p_k(L)(|1^b\rangle_A^{\otimes(k-1)})(^{\otimes(k-1)}{}_A\langle 1^b|), \quad (186) \\ \sigma_E = \frac{1}{2}\left(\sigma_E(0^b) + \sigma_E(1^b)\right).$$

Здесь базис b считается известным. Состояния посылаются Алисой равновероятно.

Количество информации в битах на одну посылку, которое может быть получено из ансамбля квантовых состояний (186), определяется фундаментальной границей Холево [32], которая является достижимой и совпадает с классической пропускной способностью $\chi(\sigma_E) = \overline{C}(L)$ квантового канала связи между Алисой и Евой с информационными состояниями (186). Имеем

$$\overline{C}(L) = \sum_{m=2}^{\infty} \overline{p}_m(L)\overline{C}(\cos^{m-1}\eta), \quad (187)$$

где

$$\overline{p}_m(L) = \frac{p_m(L)}{N(L)}, \quad N(L) = \sum_{m=2}^{\infty} p_m(L) \quad (188)$$

и

$$\overline{C}(x) = -\left(\frac{1-x}{2}\right)\log_2\left(\frac{1-x}{2}\right) - \\ -\left(\frac{1+x}{2}\right)\log_2\left(\frac{1+x}{2}\right) \quad (189)$$

— классическая пропускная способность квантового канала связи [32]. Из формул (187)–(189) видно, что при длине линии связи $L > L_1$ информация Евы о передаваемом ключе фактически определяется энтропией фон Неймана источника на передающей стороне Алисы, в котором распределение по числам заполнения фотонов сдвинуто на единицу в меньшую сторону, из-за того что один фотон должен быть направлен Евой на приемную сторону к Бобу.

Длина секретного ключа равна

$$\frac{r}{n} = 1 - h(Q(L)) - \sum_{m=2}^{\infty} \overline{p}_m(L)\overline{C}(\cos^{m-1}\eta). \quad (190)$$

Здесь n — число посылок, которые остаются после отбрасывания исходов с неопределенным результатом и согласования базисов. При критической длине линии связи L_c длина ключа обращается в нуль, $r(L_c) = 0$.

4.3. Обсуждение результатов

Взаимные информации Алиса–Боб и Алиса–Ева в зависимости от длины оптоволоконной линии связи при различной вероятности темновых отсчетов представлены на рис. 7. Критическая длина линии связи L_c определяется из условия $r(L_c) = 0$.

При типичных вероятностях темновых отсчетов для лавинных детекторов на основе InGaAs $p_{dark} = 10^{-5}$ отсч./строб, как следует из рис. 7, предельная длина линии связи составляет приблизительно 80 км. Такой уровень темновых отсчетов является типичным при охлаждении лавинных фотодетекторов до температуры -50–60°C. При охлаждении до азотных температур достижим уровень темновых шумов $p_{dark} = 10^{-7}$ отсч./строб. Предельная длина линии связи в этом случае составляет около 170 км. И наконец, при вероятности темновых отсчетов $p_{dark} = 10^{-12}$ отсч./строб достижима длина 400 км. Уровень темновых отсчетов достигается в ряде экспериментов для сверхпроводящих детекторов на основе NbN [42], при этом типичная квантовая эффективность таких детекторов не превышает 10 %. Для сверхпроводящих детекторов не требуется стробирование, поэтому данная величина является вероятностью темновых отсчетов в пересчете на длительность строба.

Описанная выше стратегия представляет Еве максимально возможную допустимую законами квантовой механики вероятностную информацию о битах ключа, которая дается границей Холево и достигается на коллективных измерениях. Возможна стратегия, которая дает Еве достоверную информацию о каждой позиции. При этом полная информация о ключе естественно меньше, чем граница Холево. Данная стратегия сводится к следующему. Имеется четыре базиса $+L$, $\times L$ и $+R$, $\times R$, внутри базисов состояния неортогональны, поэтому для получения достоверной информации Еве необходима как минимум пятифотонная компонента. Ева использует четыре фотона для индивидуальных измерений, которые аналогичны (177). Пятый фотон направляется к Бобу только в том случае, если получен результат с определенным исходом для измерений над всеми четырьмя фотонами (исходы $\mathcal{M}_{0,1^{+L}}$, $\mathcal{M}_{0,1^{\times L}}$ и $\mathcal{M}_{0,1^{+R}}$, $\mathcal{M}_{0,1^{\times R}}$), что дает возможность Еве после раскрытия базисов однозначно определить передаваемый бит. Если получен результат измерения с неопределенным исходом $\mathcal{M}_{?^b}$ хотя бы для одного из четырех фотонов, то посылка блокируется. Вероятность исхода с определенным результатом для четырех

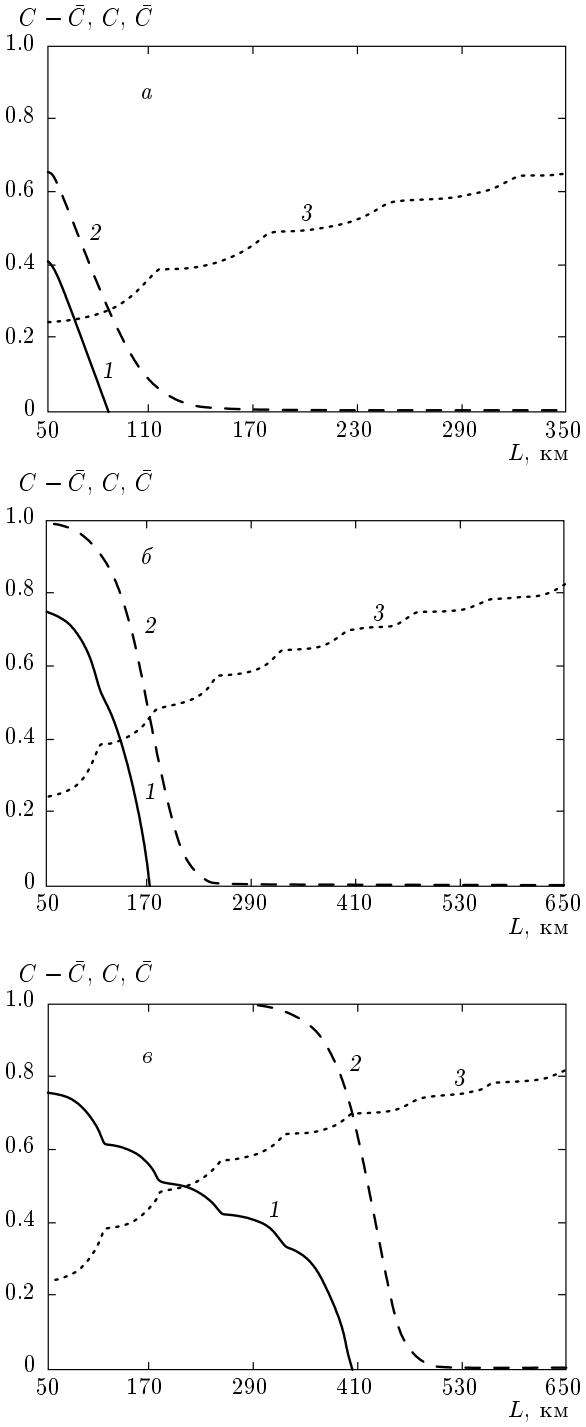

Рис. 7. Зависимости от длины линии связи L $C(Q(L)) - \overline{C}(L)$ (кривые *1*), $C(Q(L))$ (кривые *2*), $\overline{C}(L)$ (кривые *3*). Квантовая эффективность фотодетекторов η_{quan} и среднее число фотонов в когерентном состоянии одинаковы для всех кривых и равны соответственно $\eta_{0,1} = \eta_{quan} = 0.1$, $\mu = 0.2$. Угол между состояниями $\eta = \pi/8$. Вероятности темновых отсчетов на строб $p_{dark} = 10^{-5}$ (*а*), 10^{-7} (*б*), 10^{-12} (*в*)

фотонов равна $(1-\cos\eta)^4$ (например, при $\eta=\pi/8$ эта величина меньше 10^{-4}). Это означает, что такая стратегия начинает работать тогда, когда потери в канале связи позволяют Еве блокировать почти все пятифотонные посылки (долю посылок, которые еще нельзя блокировать, не более 10^{-4}).

Такая стратегия возможна, если длина линии связи превышает $L > L_5$. При длине линии связи $L > L_5$ секретное распределение ключей становится невозможным. Однако, как следует из рис. 6, 7, при типичных рабочих значениях среднего числа фотонов в состоянии $\mu = 0.1$–0.2, взаимная информация Алиса–Боб и Алиса–Ева, достижимая при коллективных измерениях, сравнивается при меньших длинах, чем L_5, поэтому данная атака Евы неэффективна. Уже при меньших длинах определяющую роль начинают играть темновые отсчеты, которые по существу определяют критическую длину.

5. ЗАКЛЮЧЕНИЕ

Предложен новый протокол квантового распределения ключей и исследована его стойкость. В случае строго однофотонного источника и ортогональных состояний внутри базиса данный протокол обеспечивает самую большую критическую ошибку, до которой гарантируется секретность распределения ключей. Для данного протокола достигается теоретический предел в 50 %. Предел по ошибке в 50 % является теоретическим пределом, до которого вообще можно передавать информацию, но в данном случае гарантируется еще и секретность ключей.

При неоднофотонном источнике и потерях в канале связи более эффективным является протокол с неортогональными состояниями внутри базисов. Данный протокол также обеспечивает наибольшую длину по сравнению с другими известными протоколами. Например, для протокола SARG04 [25] невозможно распределять ключи, если затухание таково, что подслушиватель может блокировать все трехфотонные посылки. В нашем случае секретность сохраняется при большем затухании. Затухание должно быть таково, чтобы Ева имела возможность блокировать все пятифотонные посылки. Протокол обеспечивает большую длину линии связи также по сравнению с квантовой криптографией с имитирующими состояниями [2, 44] и протоколами с большим числом базисов, которые требуют многоплечевых интерферометров Маха–Цандера. Для последних практически невозможно обеспечить долгосрочную временную стабильность. Увеличение числа базисов в данном протоколе происходит за счет временных сдвигов состояний в разных базисах, поэтому достаточно использования стандартных одноплечевых интерферометров. Кроме того, при значении угла $\eta = \pi/4$ вообще не требуется переделка стандартной конфигурации оптоволоконной части (нет необходимости вводить асимметричные оптоволоконные светоделители).

Один из авторов (С. Н. М.) выражает благодарность коллегам по Академии криптографии РФ за поддержку. Работа выполнена при частичной финансовой поддержке РФФИ (грант № 08-02-00559).

ЛИТЕРАТУРА

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

2. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, arXiv:quant-ph/0802.4155.

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

4. H. F. Chau, Phys. Rev. A **66**, 060302-1 (2002).

5. A. Acin, J. Bae, E. Bagan, M. Big, L. I. Masanes, and R. Munoz-Tapia, Phys. Rev. A **73**, 012327-1 (2006).

6. N. Gisin and S. Wolf, Phys. Rev. Lett. **83**, 4200 (1999).

7. G. Smith, J. M. Renes, and J. A. Smolin, arXiv:quant-ph/0607018.

8. G. M. Nikolopoulos, K. S. Ranade, and G. Alber, Phys. Rev. A **73**, 032325-1 (2006).

9. C. Branciard, N. Gisin, B. Kraus, and V. Scarani, Phys. Rev. A **72**, 032301-1 (2005).

10. J. Bae and A. Acin, arXiv:quant-ph/0610048.

11. S. Watanabe, R. Matsumoto, and T. Uyematsu, arXiv:quant-ph/0705.2904.

12. C. E. Shannon, Bell Syst. Tech. J. **27**, 397; **27**, 623 (1948).

13. Р. Галлагер, *Теория информации и надежная связь*, Сов. радио, Москва (1974).

14. T. Gaebel, I. Popa, A. Gruber, M. Domhan, F. Jelezko, and J. Wrachtrup, New J. Phys. **6**, 98 (2004).

15. S. Fasel, O. Alibart, A. Beveratos, S. Tanzilli, H. Zbinden, P. Baldi, and N. Gisin, arXiv:quant-ph/0408136.

16. T. B. Pittman, B. CJacobs, and J. D. Franson, arXiv:quant-ph/0408093.

17. M. Hennrich, T. Legero, A. Kuhn, and G. Rempe, arXiv:quant-ph/0406034.

18. O. Alibart, D. B. Ostrowsky, and P. Baldi, arXiv:quant-ph/0405075.

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

20. N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).

21. D. Mayers, J. ACM **48**, 351 (2001).

22. P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

23. S. Watanabe, R. Matsumoto, and T. Uyematsu, arXiv:quant-ph/0412070.

24. C. Branciard, N. Gisin, B. Kraus, and V. Scarani, Phys. Rev. A **72**, 032301 (2005).

25. V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901-1 (2004).

26. R. Renner, arXiv:quant-ph/0512258.

27. C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).

28. J. L. Carter and M. N. Wegman, J. Comp. Syst. Sci. **18**, 143 (1979).

29. B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).

30. М. А. Наймарк, Изв. АН СССР, матем. сер. **4**, 277 (1940).

31. М. Нильсен, И. Чанг, *Квантовые вычисления и квантовая информация*, Мир, Москва (2006). [M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, Cambridge (2001).]

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

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

34. P. Busch, M. Grabowski, and P. J. Lahti, Springer Lect. Notes Phys. **31** (1995).

35. C. H. Bennett and P. W. Shor, IEEE Trans. Inf. Theory **44**, 2724 (1998).

36. P. Shor, arXiv:quant-ph/0304102.

37. A. S. Holevo, *Statistical Structure of Quantum Theory*, Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, Hong Kong, Barselona, Budapest (2001).

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

39. С. Н. Молотков, А. В. Тимофеев, Письма в ЖЭТФ **85**, 632 (2007).

40. С. П. Кулик, С. Н. Молотков, А. П. Маккавеев, Письма в ЖЭТФ **95**, 324 (2007).

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

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

43. С. Н. Молотков, ЖЭТФ **134**, 39 (2008).

44. W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901-1 (2003).