ЖЭТФ, 2020, том 157, вып. 6, стр. 963–990

TROJAN-HORSE-АТАКИ, DECOY STATE-МЕТОД И ПОБОЧНЫЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ В КВАНТОВОЙ КРИПТОГРАФИИ

С. Н. Молотков*

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

Академия криптографии Российской Федерации
121552, Москва, Россия

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

Центр квантовых технологий,
Московский государственный университет им. М. В. Ломоносова
119899, Москва, Россия

Поступила в редакцию 16 октября 2019 г.,
после переработки 23 декабря 2019 г.
Принята к публикации 23 декабря 2019 г.

Ранние доказательства секретности ключей в системах квантовой криптографии основывались на предположении, что передающая и принимающая станции полностью изолированы от внешнего мира — подслушивателя. Однако такое условие невозможно реализовать на практике, поскольку системы квантовой криптографии являются открытыми системами в том смысле, что подслушиватель может иметь косвенный доступ, например, через волоконную линию связи к критическим элементам аппаратуры (фазовым модуляторам, модуляторам интенсивности и пр.), используя активное зондирование состояния этих элементов. Состояние элементов несет информацию о передаваемом ключе. Кроме того, подслушиватель может использовать пассивное детектирование побочного излучения приемной и передающей аппаратуры. Сигналы в побочных каналах утечки информации могут иметь крайне низкую интенсивность и фактически являются квантовыми. Подслушиватель может использовать совместное измерение квантовых информационных состояний в линии связи и состояний в различных побочных каналах утечки информации. В работе рассмотрены как пассивные атаки с измерением побочного излучения, так и активные атаки, связанные с зондированием состояния фазового модулятора, модулятора интенсивности, а также обратного переизлучения однофотонных лавинных детекторов, которое возникает при регистрации информационных состояний на приемной стороне. Рассмотрены также комбинированные атаки. Сделано обобщение Decoy State-метода с учетом атак активного зондирования и получены границы для параметров состояний в побочных каналах связи, при которых гарантируется секретное распределение ключей на заданную длину линии связи.

DOI: 10.31857/S0044451020060012

1. ВВЕДЕНИЕ

Носителями информации в классической области являются классические сигналы — состояния классических систем. Законы классической физики не накладывают принципиальных ограничений на точность невозмущающих измерений состояний классических объектов — сигналов. Применительно к задачам передачи и защиты информации это означает, что классический сигнал может быть сколь угодно точно и без возмущения измерен. После такого измерения в принципе сигнал может быть воспроизведен — скопирован. Фактически это означа-

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

ет, что при передаче информации при помощи классических сигналов, в принципе, возможно недетектируемое подслушивание таких сигналов. То есть в рамках классической физики нет запретов на сколь угодно точное и невозмущающее подслушивание передаваемых сигналов.

Принципиально и качественно новая ситуация возникает при переходе в область микромира, когда носителями информации являются квантовые объекты. Неизвестное квантовое состояние не может быть скопировано [1], что является следствием фундаментальных соотношений неопределенностей Гейзенберга – Робертсона [2, 3]. Осознание данного обстоятельства привело к качественно новой ситуации в области защиты информации. Возникло целое научное направление — квантовая криптография. За достаточно короткое время, использование фундаментальных запретов квантовой теории на различимость квантовых состояний было доведено до практических применений в области защиты информации. Квантовая криптография, синоним квантового распределения секретных ключей, решает центральную проблему симметричной криптографии — распределение общего секрета (секретного ключа) между пространственно-удаленными пользователями через открытые и доступные для подслушивания каналы связи.

Система квантовой криптографии представляет собой распределенное физическое устройство, в котором приготовление и измерение квантовых состояний происходит в пространственно-удаленных местах, соединенных линией связи. В отличие от классической физики, где наблюдаемым отвечают функции координат и времени, в квантовой теории наблюдаемым величинам сопоставляются эрмитовы операторы. Это обстоятельство приводит к фундаментальным соотношениям неопределенностей Гейзенберга – Робертсона [2, 3] для некоммутирующих операторов A и B, отвечающих двум наблюдаемым:

$$\Delta_A \Delta_B \geq \frac{1}{2}|\langle\psi|[A,B]|\psi\rangle|,$$

$$\Delta_A = \sqrt{\langle\psi|A^2|\psi\rangle - \langle\psi|A|\psi\rangle^2},$$

$$\Delta_B = \sqrt{\langle\psi|B^2|\psi\rangle - \langle\psi|B|\psi\rangle^2}, \quad [A,B] = A\cdot B - B\cdot A.$$

С формальной точки зрения это означает, что некоммутирующие эрмитовы операторы не могут иметь общей системы собственных векторов.

На ранних стадиях развития квантовой криптографии часто произносились слова, что секретность ключей гарантируется фундаментальными соотношениями неопределенностей, но не было явно показано, как секретность ключей связана с соотношениями неопределенностей Гейзенберга – Робертсона. Действительно, прямой связи данных соотношений неопределенностей и секретности ключей не видно. Соотношения неопределенностей означают лишь следующее. Если квантовая система находится в состоянии $|\psi\rangle$, то измерение наблюдаемой A в каждом акте измерения будет давать одно из собственных значений наблюдаемой A a_i с вероятностью $p(a_i) = |\langle a_i|\psi\rangle|^2$, где $|a_i\rangle$ — собственный вектор наблюдаемой A, отвечающей собственному числу a_i. Результаты измерений наблюдаемой A квантовой системы в состоянии $|\psi\rangle$ имеют дисперсию Δ_A.

В другой серии измерений наблюдаемой B системы в том же квантовом состоянии $|\psi\rangle$ возникают собственные числа b_i оператора B с вероятностью $p(b_i) = |\langle b_i|\psi\rangle|^2$, которые имеют разброс результатов измерений с дисперсией Δ_B. Произведение дисперсий результатов наблюдений в двух разных экспериментах отлично от нуля, если операторы наблюдаемых не коммутируют. Это и есть стандартная интерпретация соотношений Гейзенберга – Робертсона.

Существуют две причины, по которым данные соотношения еще не удается напрямую использовать для задач переработки и передачи информации. Первая причина — в данных соотношениях нет информационного аспекта, т. е. нет понятия информации. Вторая причина состоит в том, что правая часть данных соотношений неопределенностей может быть равна нулю даже для некоммутирующих наблюдаемых. Если операторы ограничены и имеют конечный набор собственных функций, то правая часть неравенства будет равна нулю, если система находится в одном из собственных состояний одного из операторов, например, $|\psi\rangle = |a_j\rangle$. Второе упомянутое обстоятельство было известно давно — нахождение системы в одном из собственных состояний одного из операторов приводит к отсутствию разброса результатов измерений (нулевая дисперсия) одной из наблюдаемых.

Информационный аспект соотношений неопределенностей возник после работ [4–6], в которых соотношения неопределенностей для некоммутирующих наблюдаемых были переформулированы непосредственно в терминах энтропии Шеннона, которая является мерой информации. Согласно [4–6] энтропийные соотношения неопределенностей принимают вид

$$H(A) + H(B) \geq -2\log(\max_{i,j}|\langle a_i|b_j\rangle|),$$

где энтропии Шеннона

$$H(A) = -\sum_i p(a_i)\log(p(a_i)),$$

$$H(B) = -\sum_i p(b_i)\log(p(b_i)),$$

$\log \equiv \log_2$. Данные энтропийные соотношения неопределенностей имеют теоретико-информационную интерпретацию. Важно подчеркнуть, что правые части энтропийных неравенств не зависят от квантового состояния, а зависят только от наблюдаемых, в отличие от соотношений Гейзенберга – Робертсона.

Пусть квантовая система находится в состоянии $|\psi\rangle$. Пусть проводятся измерения наблюдаемой A, вероятность получить исход i есть $p(a_i) = |\langle a_i|\psi\rangle|^2$. Далее, мерой информации i-го исхода является $\log(1/p(a_i))$ — чем реже появляется событие, тем больше информации оно несет. До того как исход произошел, нехватка информации — неопределенность о том, какой будет исход, есть $\log(1/p(a_i))$. Поскольку сам исход имеет место с вероятностью $p(a_i)$, средняя нехватка информации по всем исходам при измерении наблюдаемой A есть $H(A)$. После возникновения исхода измерений происходит приращение информации на соответствующую величину. Аналогично, нехватка информации до появления исходов при измерении наблюдаемой B есть $H(B)$.

Сумма нехваток информаций при измерении двух наблюдаемых не может быть нулем, если наблюдаемые не коммутируют — не имеют общей системы собственных векторов. Важно, что нижняя граница (правая часть неравенства) суммы нехваток информаций не зависит от того, в каком состоянии $|\psi\rangle$ находится квантовая система, а зависит только от наблюдаемых. Однако и данные энтропийные соотношения неопределенностей еще неприменимы напрямую к задачам квантовой криптографии, поскольку относятся только к одной квантовой системе.

В задачах квантовой криптографии квантовое состояние в общем случае описывает три квантовые системы, имеющиеся в распоряжении Алисы (передающая сторона), Боба (принимающая сторона) и Евы (подслушиватель). В общем случае три квантовые системы находятся в общем квантовом запутанном состоянии. Обобщение энтропийных соотношений неопределенностей на составные квантовые системы было сделано в работе [7]. Пусть имеется составная квантовая система в состоянии $|\psi\rangle_{ABE}$, тогда имеет место неравенство (см. детали ниже)

$$H(X|E) + H(X|B) \geq 1,$$

которое интерпретируются следующим образом. Пусть в результате работы протокола квантового распределения ключей Алиса имеет битовую строку X, а Ева и Боб имеют в своем распоряжении квантовые системы. Далее, $H(X|E)$ есть нехватка информации Евы о битовой строке Алисы при условии, что Ева имеет в своем распоряжении квантовую систему E, коррелированную с битовой строкой Алисы. Аналогично $H(X|B)$ — нехватка информации Боба о битовой строке Алисы при условии, что Боб имеет в своем распоряжении квантовую систему B.

Нехватка информации Боба $H(X|B)$ напрямую связана с наблюдаемыми ошибками на приемной стороне. Для оценки величины ошибок Алисе и Бобу не требуется явно знать квантовое состояние Евы, достаточно обменов информации по открытому каналу связи для оценки вероятности ошибки на стороне Боба. Вторжение Евы в квантовый канал связи приводит к ошибкам на приемной стороне, величина ошибок позволяет получить верхнюю границу утечки информации (соответственно ее нехватку) к Еве при вторжении в квантовый канал связи. Важно, что при использовании энтропийных соотношений неопределенностей для составных систем не требуется строить явно атаки Евы на передаваемые квантовые состояния.

Для исправления ошибок Алиса должна сообщить Бобу через открытый классический канал связи информацию не менее $H(X|B)$ битов, которая также доступна Еве. В итоге нехватка информации Евы $H(X|E)$ уменьшается на величину $H(X|B)$. После коррекции ошибок Бобом нехватка информации Евы, с учетом энтропийных соотношений неопределенностей, становится не менее (в пересчете на одну позицию ключа) $H(X|E) - H(X|B) \geq 1 - H(X|B) - H(X|B) = 1 - 2H(X|B)$. Неформально, данное количество информации недоступно Еве и является общим секретом Алисы и Боба — секретным ключом. Иными словами, фундаментальные энтропийные соотношения неопределенностей позволяют связать утечку (соответственно нехватку) информации к Еве через наблюдаемую ошибку у Боба.

Сказанное справедливо, пока не учитываются побочные каналы утечки информации, например, излучение аппаратуры, активное зондирование элементов аппаратуры и пр. Данные каналы утечки являются «бонусом» для Евы в том смысле, что Ева может получить дополнительную информацию о передаваемых квантовых состояниях косвенно, например, измеряя побочное излучение аппаратуры, при

этом Ева не будет производить ошибок на приемной стороне. Иными словами, утечка информации по побочным каналам не связана с ошибкой на приемной стороне и требуется явное включение в рассмотрение атак, связанных с квантово-механическими измерениями состояний в побочных каналах, что и является целью данной работы.

Целью работы является выяснение вопроса о том, как зависит длина секретного ключа от параметров квантовых состояний в побочных каналах. Критические для секретности побочные каналы утечки информации более менее очевидны, и только требуется правильно их включить в общую схему доказательства секретности ключей.

После вводной части перейдем к более содержательной постановке задачи. Квантовая криптография — квантовое распределение ключей решает центральную проблему симметричной криптографии — проблему распределения секретных ключей по открытым и доступным для подслушивания каналам связи, и должна гарантировать безусловную секретность ключей [8–10]. По сути, квантовая криптография — способ синхронизации двух независимых случайных последовательностей на передающей (Алиса) и приемной (Боб) сторонах при помощи посылки и измерения квантовых состояний. Под безусловной секретностью понимается тот факт, что секретность распределяемых ключей гарантируется фундаментальными законами квантовой теории, а не техническими или вычислительными возможностями нарушителя (Ева).

Фундаментальные законы квантовой теории позволяют связать наблюдаемую ошибку на приемной стороне с верхней границей утечки информации к подслушивателю.

Для ряда протоколов квантового распределения ключей, например, BB84 [8] и ряда других, в случае, когда источник информационных состояний является строго однофотонным, удается найти верхнюю границу утечки информации, не конструируя явно атаки подслушивателя на передаваемые квантовые состояния. Верхняя граница может быть найдена только по наблюдаемой ошибке на приемной стороне. Такая оценка базируется на фундаментальных энтропийных соотношениях неопределенностей [11–13].

Утечка информации к подслушивателю выражается в терминах условной энтропии фон Неймана Алиса–Ева, или сглаженной условной минимальной энтропии Реньи [11, 13]. В случае конечных последовательностей утечка выражается через сглаженную минимальную энтропию, которая в асимптотическом пределе длинных последовательностей переходит в условную энтропию фон Неймана. Длина секретного ключа — число общих, никому неизвестных секретных битовых позиций, выражается как разность условной энтропии Алиса–Ева и информации, расходуемой на коррекцию ошибок (leak), через открытый аутентичный классический канал связи. Данная информация является открытой и всем доступной. С формальной точки зрения анализ криптографической стойкости протокола квантового распределения ключей сводится к вычислению утечки информации к Еве — вычислению условной квантовой энтропии, которая содержит всю информацию об атаках Евы. На сегодняшний день, в случае строго однофотонного источника информационных квантовых состояний и только при атаках на передаваемые квантовые состояния в квантовом канале связи, секретность передаваемых ключей можно считать надежно доказанной. При этом доказательство базируется только на фундаментальных законах квантовой теории — энтропийных соотношениях неопределенностей [11–14], которые являются, в определенном смысле, аналогом стандартных соотношений неопределенностей Гейзенберга – Робертсона и проявлением фундаментальных ограничений квантовой теории на измеримость двух некоммутирующих наблюдаемых.

В реальной ситуации источник квантовых состояний представляет собой ослабленное когерентное состояние. Нестрогая однофотонность источника и потери в квантовом канале связи открывают возможности для ряда атак, которые отсутствовали в однофотонном случае [10]. Это PNS-атака (Photon Number Splitting) — атака с неразрушающим измерением числа фотонов в квантовом канале связи, атака с измерениями с определенным исходом (Unambiguous Measurements, UM), Beam Split-атака — прозрачная атака, не приводящая к возмущению передаваемых состояний, основанная на отведении части информационных состояний из квантового канала связи к подслушивателю. Данная атака основана на том факте, что на линейных оптических элементах когерентные состояния преобразуются самоподобно, без изменения структуры.

На сегодняшний день принята следующая точка зрения на детектирование различных атак, связанных с неоднофотонностью источника. Считается, что весь секретный ключ определяется только долей однофотонной компоненты состояний. Все многофотонные компоненты состояний консервативно в пользу подслушивателя считаются известными Еве. Поэтому задача сводится фактически к оценке доли

однофотонной компоненты на приемной стороне.

Считается, что таким универсальным методом для оценки доли однофотонной компоненты, хотя это строго до конца не доказано, является Decoy State-метод, который сводится к модуляции интенсивности когерентных состояний, и который исходно был разработан для детектирования только PNS-атаки. Отметим, забегая вперед, что при наличии побочных каналов утечки информации, существуют атаки активного зондирования, к детектированию которых Decoy State-метод не чувствителен.

В основании Decoy State-метода лежат следующие посылки (предположения), без которых метод неприменим. Предположение о рандомизации фаз когерентных состояний в разных посылках. Для достижения такой рандомизации приходится использовать технические решения, которые дают такую рандомизацию.

Если считать, что фазы когерентных состояний в разных посылках являются случайными и равновероятно распределенными на отрезке $[0, 2\pi]$, то состояния в канале связи представляют собой статистическую смесь фоковских состояний с разным числом фотонов. Распределение по числу фотонов является пуассоновским. Использование когерентных состояний с разным средним числом фотонов и рандомизированными фазами позволяет получить оценку для доли однофотонной компоненты и ошибки в однофотонной компоненте. Информация в многофотонных компонентах «отдается» подслушивателю, считается ему известной.

Для однофотонной компоненты, зная оценку ошибки в этой компоненте на приемной стороне, можно воспользоваться фундаментальными результатами для утечки информации к Еве, которые следуют из фундаментальных соотношений неопределенностей.

В этом смысле, с оговорками, сделанными выше, секретность ключей для реальных неоднофотонных источников и атак только на передаваемые квантовые состояния в канале можно считать надежно доказанной.

Действительно, квантовая криптография гарантирует безусловную секретность ключей, если учитывать только атаки на передаваемые квантовые состояния, когда подслушиватель не имеет ни прямого, ни косвенного доступа к передающей (Алисе) и принимающей (Бобу) станциям.

В реальности системы квантовой криптографии являются открытыми системами, в том смысле, что подслушиватель (Ева) может иметь косвенный доступ к приемо-передающей аппаратуре, используя зондирующее излучение. Обычно такие атаки называются атаками на техническую реализацию или Trojan-horse-атаки [15–23]. Без устойчивости системы к таким атакам невозможно всерьез говорить о секретности распределяемых ключей.

При учете таких атак возникает принципиально новая ситуация, поскольку предыдущие разработанные методы анализа криптостойкости систем квантового распределения ключей (КРК) напрямую уже не применимы. Требуется разработка новых подходов, которые могли бы детектировать как предыдущие атаки, так и новые, а также различные комбинации старых и новых атак.

Все атаки на системы квантовой криптографии условно можно разделить на четыре класса:

1) атаки непосредственно на информационные квантовые состояния в канале связи;

2) пассивные атаки, использующие детектирование побочного электромагнитного излучения от аппаратуры приемной и передающей станций;

3) активные атаки, использующие зондирование внешним излучением состояния элементов аппаратуры: фазовых модуляторов, лавинных детекторов, модуляторов интенсивности, детектирование переизлучения лавинных детекторов в линию связи при их срабатывании и т. д.;

4) навязывание нужных для нарушителя (модификация) изменений штатной работы элементов системы, например, ослепление лавинных детекторов и атака Detectors Mismatch [15, 17–23].

При учете атак на техническую реализацию напрямую воспользоваться энтропийными соотношениями неопределенностей для вычисления верхней границы утечки информации к подслушивателю оказывается уже невозможным и приходится явно строить всевозможные атаки подслушивателя на квантовые состояния с учетом побочных каналов утечки.

Первый класс атак подразумевает, что подслушиватель не имеет ни прямого, ни косвенного доступа к приемо-передающей аппаратуре. Секретность ключей при таких атаках гарантируется фундаментальными ограничениями квантовой теории на различимость квантовых состояний даже при не строго однофотонном источнике состояний.

Второй класс атак связан с пассивным детектированием слабых (фактически квантовых) побочных сигналов от работы элементов приемной и передающей аппаратуры — излучения от фазовых модуляторов, модуляторов интенсивности, генераторов случайных чисел, от схемы стробирования лавин-

ных детекторов, обратного переизлучения лавинных детекторов при их срабатывании и др.

Третий класс атак использует активное зондирование через волоконную линию связи состояния активных элементов системы, например, фазовых модуляторов, которые несут информацию о передаваемом ключе. Зондирование внешним излучением модуляторов интенсивности представляет собой отдельную задачу, в отличие от зондирования фазовых модуляторов, поскольку состояние модулятора интенсивности в отличие от зондирования фазовых модуляторов не дает «прямой» информации о передаваемом бите ключа, а лишь о состоянии decoy state, т. е. информацию об интенсивности передаваемого состояния.

Четвертый класс — атаки, при которых внешним зондированием изменяют штатную работу элементов, например, лавинных детекторов.

Для систем с фазовым кодированием атаки с ослеплением лавинных детекторов, которые предлагались ранее, оказываются неэффективными и приводят к детектированию атаки [21, 22]. Других модификаций атаки с ослеплением еще не было предложено. Аналогично детектируется атака Detectors Mismatch [23].

Попытки обобщения Decoy State-метода [24–26] при активном зондировании модулятора интенсивности были предприняты в ряде работ [27, 28]. Это обобщение, по сути, является попыткой сведения к задаче оптимизации — решению системы уравнений с бесконечным числом неизвестных (вероятностей в искаженных пуассоновских распределениях), которая решается численно методами линейного программирования и путем усечения сумм искаженных пуассоновских распределений. То есть в работах [27, 28] сделана попытка рассматривать утечку информации по побочным каналам только на основании фундаментальных принципов, что вряд ли возможно. Подсчет утечки информации при атаке только на передаваемые квантовые состояния возможен на основе только фундаментальных принципов, так как структура посылаемых в канал связи квантовых состояний известна, но структура квантовых состояний в побочных каналах связи неизвестна. Например, структура побочного излучения передающей станции при приготовлении информационных квантовых состояний, в силу огромного числа степеней свободы передающей аппаратуры (излучение квантового генератора случайных чисел, фазового модулятора, различных внутренних передающих шин аппаратуры и пр.), точно неизвестна, поэтому невозможно обойтись без каких-то модельных соображений о структуре побочного излучения.

Ниже предлагается аналитический метод, который позволяет получить явные формулы для длины секретного ключа при зондировании модулятора интенсивности, а также при комбинированных атаках. Побочные каналы утечки, на наш взгляд, невозможно рассматривать без знания работы конкретной реализации систем КРК. Иначе говоря, побочные каналы утечки нельзя рассматривать без каких-то дополнительных модельных соображений, в отличие от атак только на передаваемые квантовые состояния. Метод позволяет физически осмысленно включать в рассмотрение различные побочные каналы утечки информации. Побочные каналы утечки информации в квантовой криптографии также приходится рассматривать на квантовом уровне, в отличие от побочных каналов в классической криптографии. Оказывается невозможным рассматривать часть сигналов классическим, а часть сигналов квантовым образом. На это существует, по крайней мере, две причины. Во-первых, интенсивность сигналов в побочных каналах может быть предельно слабой, т. е. побочный сигнал является, по сути, квантовым. Во-вторых, подслушиватель может проводить совместные коллективные измерения побочного квантового сигнала и квантового информационного состояния. Такое совместное измерение дает больше информации подслушивателю, чем отдельные аддитивные измерения информационных квантовых состояний и квантового побочного сигнала, поэтому все рассмотрение изначально должно быть квантовым.

2. ОБЩАЯ ИДЕОЛОГИЯ АНАЛИЗА TROJAN-HORSE-АТАК НА СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

С формальной точки зрения учет всевозможных атак сводится к вычислению условной энтропии фон Неймана Алиса–Ева (или сглаженной энтропии Реньи) с учетом детектирования состояний в побочных каналах, а также атак на квантовые состояния в канале связи.

Общая идеология учета различных атак будет сводится к следующему. Поскольку при атаках на техническую реализацию уже не удается воспользоваться энтропийными соотношениями неопределенностей, приходится строить атаки Евы явно. Невозможность использовать энтропийные соотношения неопределенностей при подсчете утечек информации по побочным каналам связана с тем, что в энтропийных соотношениях неопределеннос-

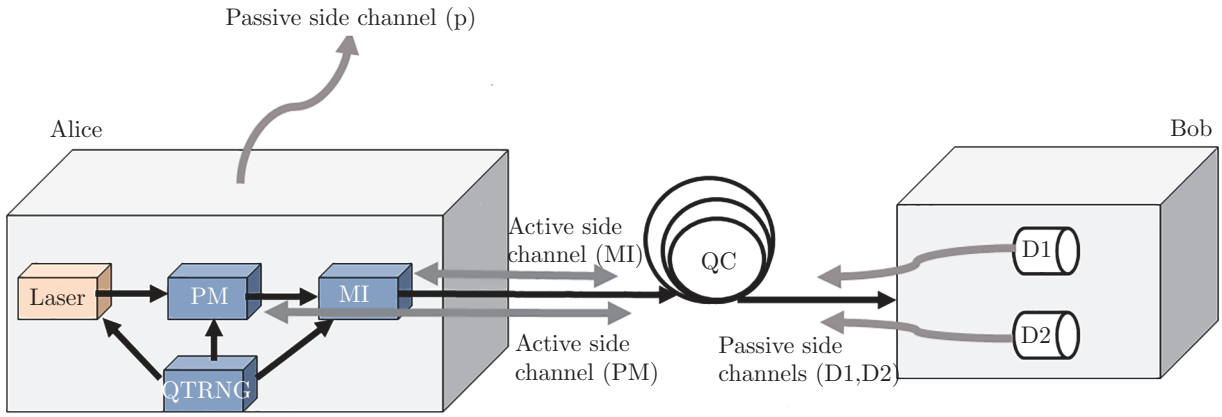

Рис. 1. Схематическое изображение передающей (Alice), принимающей (Bob) станций и различных побочных каналов утечки информации. Приняты следующие обозначения: Laser — лазер, QTRNG — квантовый генератор случайных чисел, PM — фазовый модулятор, MI — модулятор интенсивности, QC — квантовый канал связи. Passive side channel (p) — побочный канал утечки, связанный с полным излучением аппаратуры передающей станции, Active side channel (PM), (MI) — побочные каналы утечки, связанные с активным зондированием фазового модулятора и модулятора интенсивности, Passive side channels (D1, D2) — каналы утечки, связанные с переизлучением лавинных детекторов D1 и D2

тей нехватка информации Евы о битовой строке Алисы выражается через нехватку информации Боба на приемной станции, которая выражается через возмущение (наблюдаемую ошибку) информационных состояний, детектируемых на приемной стороне. При побочных каналах утечки информации измерение сигналов в побочном канале не производит ошибок на приемной стороне, поэтому не детектируется через возмущение информационных состояний на стороне Боба. По этой причине энтропийных соотношений неопределенностей даже в однофотонном случае уже недостаточно для подсчета полной утечки информации к подслушивателю. Приходится учитывать данную утечку явным образом еще и при условии, что точный вид квантового состояния в побочном канале полностью точно неизвестен.

Будем решать задачу в несколько этапов. Для различных атак: с пассивным детектированием излучения, активным зондированием фазового модулятора, а также совместных атак на квантовые состояния в канале и побочное (пассивное и активное) излучение, будут получены явные формулы для длины секретного ключа для однофотонной компоненты. Информация, которую можно получить из многофотонных компонент информационных состояний, как упоминалось, «отдается» подслушивателю.

На следующих этапах будет учтено детектирование переизлучения лавинных детекторов. Далее будут получены формулы с учетом всех побочных каналов утечки информации совместно с атакой на квантовые состояния в канале.

Затем (второй этап анализа) будет изложен модифицированный Decoy State-метод, который позволяет получить оценки для доли однофотонной компоненты с учетом зондирования модулятора интенсивности.

Далее будут приведены формулы для длины секретного ключа, где будет использована оценка доли однофотонной компоненты по модифицированному Decoy State-методу. Однофотонная компонента уже будет включать в себя совместные атаки с учетом всех побочных каналов утечки и атак на информационные квантовые состояния в квантовом канале связи.

При разработке методики расчетов будем рассматривать протокол BB84, вся идеология расчетов переносится и на другие протоколы. «Обкатку» идеологии расчетов имеет смысл проводить на хорошо известном протоколе, для которого известны точные результаты в разных предельных ситуациях.

На данном этапе учитываются активные атаки на станцию Алисы, методика расчета позволяет учесть атаки на станцию Боба.

Удобно графически изобразить атаки на техническую реализацию. Схематически атаки с пассивным детектированием побочного излучения и активным зондированием элементов системы представлены на рис. 1.

3. УЧЕТ РАЗЛИЧНЫХ АТАК: КАЧЕСТВЕННОЕ РАССМОТРЕНИЕ

Защита от пассивного детектирования побочного излучения при работе аппаратуры сводится к экранированию системы. Интенсивность сигналов непосредственно от работы самих элементов известна (может и должна быть измерена при специальных исследованиях), поэтому, выбирая уровень экранировки аппаратуры, можно указать верхнюю границу интенсивности побочного излучения, которое доступно для детектирования подслушивателем.

При атаке с зондированием внешним излучением интенсивность входного излучения, которая, вообще говоря, неизвестна, определяется подслушивателем. Поэтому интенсивность отраженных состояний от элементов системы также неизвестна.

Возможны два способа детектирования атаки с активным зондированием. Первый — активный способ, когда детектируется сам зондирующий сигнал различными сторожевыми детекторами. Возможен второй, более удобный, надежный и простой способ «пассивной» защиты [28]. При этом способе нужно знать верхнюю границу интенсивности отраженных состояний. Зная верхнюю границу интенсивности входного зондирующего излучения, можно указать и верхнюю границу интенсивности отраженных состояний, поскольку коэффициенты потерь в приемной части системы известны. Будем рассматривать именно этот способ защиты от атак активного зондирования. Граница по максимальной интенсивности отраженных зондирующих состояний может быть получена из тех соображений, что интенсивность входного излучения не может превышать границу термического разрушения волокна (см. подробный анализ в работах [20–31], а также [32]). Данным способом определяется верхняя граница интенсивности входного зондирующего излучения, соответственно, верхняя граница интенсивности выходного отраженного зондирующего излучения. Вводя в систему пассивные оптические элементы с нужными коэффициентами ослабления, можно гарантировать верхнюю границу интенсивности отраженных состояний, доступных для измерения подслушивателем.

Активное зондирование фазового модулятора и модулятора интенсивности принципиально отличаются друг от друга в том смысле, что активное зондирование состояния фазового модулятора несет непосредственно информацию о передаваемом ключе, а активное зондирование модулятора интенсивности не несет непосредственно информацию о ключе, а лишь об интенсивности когерентных состояний, используемых в Decoy State-методе. Информация об интенсивности когерентных состояний может быть опосредовано использована для определения передаваемых битов ключа. Активное зондирование модулятора интенсивности дает дополнительную информацию подслушивателю о том, какой тип состояния передается — информационное состояние или состояние «ловушка». Это приводит к тому, что стандартный Decoy State-метод перестает работать, поэтому требуется его модификация с учетом активного зондирования модулятора интенсивности (см. ниже).

Учет каждого канала утечки информации сводится к введению в рассмотрение квантовых состояний, отвечающих за данный канал. Секретная часть ключа набирается из однофотонной части когерентных состояний, поэтому, кроме унитарной атаки непосредственно на квантовые состояния в квантовом канале связи, возможна совместная атака на информационные квантовые состояния в канале, на квантовое состояние от излучения передающей (приемной) аппаратуры, на отраженное квантовое состояние от фазового модулятора, на квантовое состояние, связанное с переизлучением лавинных детекторов. Квантовые состояния в побочных каналах определяются конкретной реализацией аппаратуры. Отраженные зондирующие квантовые состояния от модулятора интенсивности учитываются на следующем этапе анализа при оценке доли однофотонной компоненты состояний, при этом используется модифицированный Decoy State-метод. Данный подход позволяет получить явные аналитические формулы для длины секретного ключа, которые имеют простую и интуитивно понятную физическую интерпретацию. Ниже будут определены параметры побочного излучения и параметры отраженного излучения, при которых возможно секретное распределение ключей на заданную длину линии связи.

4. КАКИЕ ВЕЛИЧИНЫ ТРЕБУЕТСЯ ВЫЧИСЛЯТЬ ДЛЯ ОЦЕНКИ ДЛИНЫ СЕКРЕТНОГО КЛЮЧА?

При вычислении длины секретного ключа в асимптотическом пределе длинных последовательностей необходимо знать условную энтропию фон Неймана Алиса–Ева. Поправки к длине секретного ключа при конечных передаваемых последовательностях в дальнейшем выражаются

через эту величину, ε-поправки возникают и подсчитываются фактически классическим образом как поправки при оценке параметров уже классических распределений, что может быть проведено на следующем этапе анализа.

Ограничимся пределом асимптотически длинных последовательностей. Длина секретного ключа ℓ_n дается общей формулой [11]

$$\ell = \frac{\ell_n}{n} = H^{\varepsilon}_{min}(X|E) - \text{leak}, \tag{1}$$

где n — число зарегистрированных посылок в базисе, leak — информация в битах в пересчете на одну посылку, фактически израсходованная на коррекцию ошибок Алисой и Бобом, $H^{\varepsilon}_{min}(X|E)$ — условная сглаженная минимальная энтропия, $X \in \mathcal{X} = \{0,1\}^n$ — битовая строка Алисы, E — квантовая система Евы, коррелированная с битовой строкой. Неформально $H^{\varepsilon}_{min}(X|E)$ есть дефицит информации подслушивателя о битовой строке Алисы. Данная величина включает в себя всевозможные атаки Евы.

В асимптотическом пределе $n \to \infty$ сглаженная минимальная энтропия в (1) переходит в условную энтропию фон Неймана [11]:

$$\begin{gathered} H^{\varepsilon}_{min}(X|E) \to H(X|E), \\ H(X|E) = H(\rho_{XE}|\rho_E) = H(\rho_{XE}) - H(\rho_E), \end{gathered} \tag{2}$$

где $H(\rho) = -\mathrm{Tr}\{\rho \log(\rho)\}$, ρ_{XE} — матрица плотности Алиса–Ева, которая содержит всю информацию об атаках Евы.

Без побочных сигналов и активного зондирования условная энтропия Алиса–Ева для однофотонных состояний может быть оценена из фундаментальных энтропийных соотношений неопределенностей [12, 13]:

$$H(X^+|E) + H(X^\times|Y^\times) \geq 1. \tag{3}$$

Индексы $+$ и $\times$ относятся к прямому и сопряженному базисам протокола BB84, $H(X^\times|Y^\times) = h(Q)$ — классическая энтропия Алиса–Боб, $Y^\times \in \mathcal{Y} = \{0,1\}^n$ — битовая строка Боба, содержащая наблюдаемые ошибки с вероятностью Q, $h(Q) = -Q\log(Q) - (1-Q)\log(1-Q)$ — бинарная энтропийная функция Шеннона. Как видно из (3), утечка информации к подслушивателю в базисе $+$ оценивается через возмущение состояний (ошибку Q) на приемной стороне в сопряженном базисе $\times$, соответственно наоборот.

С учетом (1)–(3) получается известная формула для длины ключа в однофотонном случае [9–11, 13]:

$$\ell = \lim_{n\to\infty} \frac{\ell_n}{n} = 1 - 2h(Q). \tag{4}$$

При учете побочных каналов утечки информации и активном зондировании напрямую воспользоваться энтропийными соотношениями неопределенностей для оценки условной энтропии Алиса–Ева уже не удается и приходится строить атаки Евы явно. Ниже будут рассмотрены различные атаки с учетом побочных каналов утечки информации.

5. ПОБОЧНЫЙ КАНАЛ УТЕЧКИ, СВЯЗАННЫЙ С ИЗЛУЧЕНИЕМ АППАРАТУРЫ ПЕРЕДАЮЩЕЙ СТАНЦИИ

Кроме атаки непосредственно на информационные состояния в канале связи, Ева может пассивно детектировать побочное излучение, вызванное работой аппаратуры передающей станции. Данный канал утечки информации описывается введением квантового состояния, которое описывает побочное излучение.

Атака Евы на однофотонные информационные состояния в квантовом канале связи определяется унитарным оператором, который определяется Евой. Оптимальная унитарная атака, достигающая нижнюю границу энтропийных соотношений неопределенностей (3), может быть построена явно [14]. Для унитарной атаки на информационные состояния в базисе $+$ имеем (см. детали, например, в [14])

$$\begin{aligned} |0^+\rangle_X \otimes |0^+\rangle_Y \to |0^+\rangle_X \otimes U_{BE}(|0^+\rangle_Y \otimes |E\rangle_Q) = \\ = |0^+\rangle_X \otimes [\sqrt{1-Q}|0^+\rangle_Y \otimes |\Phi_{0^+}\rangle_Q + \\ + \sqrt{Q}|1^+\rangle_Y \otimes |\Theta_{0^+}\rangle_Q], \end{aligned} \tag{5}$$

где $|0^+\rangle_X$ — эталонное состояние на стороне Алисы, доступное только ей, $|0^+\rangle_Y \to$ — состояние, которое посылается к Бобу через квантовый канал связи, U_{BE} — унитарный оператор Евы, который содержит способ атаки Евы на передаваемое в квантовом канале состояние Боба, $|E\rangle_Q$ — исходное вспомогательное состояние Евы — ancilla, $|\Phi_{0^+}\rangle_Q$ и $|\Theta_{0^+}\rangle_Q$ — искаженные состояния, возникающие из вспомогательного состояния Евы.

Формула (5) представляет собой разложение Шмидта, параметр Q пока является свободным. Ниже увидим, что Q есть наблюдаемая ошибка на приемной стороне, которая возникает при атаке на квантовые состояния в канале связи. Детектирование побочного излучения не приводит к ошибкам. Индекс «Q» (от Quantum) у состояний Евы символизирует атаку на квантовые информационные состояния. Аналогичное выражение имеет место, ког-

да в канал передается состояние $|1^+\rangle_X \otimes |1^+\rangle_Y$. Имеем

$$|1^+\rangle_X \otimes |1^+\rangle_Y \to |1^+\rangle_X \otimes U_{BE}(|1^+\rangle_Y \otimes |E\rangle_Q) = \\ = |1^+\rangle_X \otimes [\sqrt{1-Q}|1^+\rangle_Y \otimes |\Phi_{1^+}\rangle_Q + \\ + \sqrt{Q}|0^+\rangle_Y \otimes |\Theta_{1^+}\rangle_Q]. \quad (6)$$

В формуле (6) обозначения и состояния аналогичны используемым в формуле (5). Аналогичные выражения имеют место в сопряженном базисе $\times$.

Измерения Боба в базисе $+$ даются разложением единицы I_{Y+}:

$$I_{Y+} = |0^+\rangle_{YY}\langle 0^+| + |1^+\rangle_{YY}\langle 1^+|, \quad (7)$$

аналогично в сопряженном базисе $\times$.

После измерений Боба матрица плотности Алиса–Боб–Ева принимает вид

$$\rho_{XYQ} = \frac{1}{2}|0^+\rangle_{X\,X}\langle 0^+| \otimes [(1-Q) \times \\ \times |0^+\rangle_{YY}\langle 0^+| \otimes |\Phi_{0^+}\rangle_{QQ}\langle \Phi_{0^+}| + \\ + Q|1^+\rangle_{YY}\langle 1^+| \otimes |\Theta_{0^+}\rangle_{QQ}\langle \Theta_{0^+}|] + \\ + \frac{1}{2}|1^+\rangle_{X\,X}\langle 1^+| \otimes [(1-Q)|1^+\rangle_{YY}\langle 1^+| \otimes |\Phi_{1^+}\rangle_{QQ} \times \\ \times \langle \Phi_{1^+}| + Q|0^+\rangle_{YY}\langle 0^+| \otimes |\Theta_{1^+}\rangle_{QQ}\langle \Theta_{1^+}|]. \quad (8)$$

Учтем теперь побочное излучение аппаратуры Алисы, которое пассивно может детектироваться Евой. С формальной точки зрения возникает дополнительный канал утечки информации, который необходимо включить в анализ.

Детектирование побочного излучения не приводит к ошибкам на приемной стороне, поскольку не затрагивает напрямую информационные квантовые состояния в канале, однако влияет на длину секретного ключа. Уже в этом месте видно, что анализ секретности систем КРК с учетом побочного излучения не может быть сделан только с использованием энтропийных соотношений неопределенностей, которые связывают утечку информации к Еве с возмущением (ошибкой) информационных состояний на стороне Боба.

Состояния побочного излучения «привязаны» к состояниям Алисы в том смысле, что приготовление того или иного информационного состояния Алисой приводит к побочному излучению аппаратуры. Причем интенсивность данного излучения может быть как предельно слабой, так и интенсивной (при неаккуратной экранировке аппаратуры). Независимо от интенсивности побочный сигнал следует рассматривать как квантовый. Интенсивный классический сигнал также можно рассматривать как квантовый, поскольку квантовое описание является более общим и включает классическое описание как предельный случай, когда сигнал содержит большое число фотонов. Вся разница состоит только в степени различимости сигналов, отвечающих приготавливаемому 0 или 1. Чем интенсивней сигнал, тем больше степень различимости пары сигналов для 0 и 1. Более формально, для классических сигналов вероятность различения стремится к единице, соответственно, вероятность ошибки различения стремится к нулю. С понижением интенсивности сигнала вероятность различения уменьшается. В пределе отсутствия побочного сигнала бесконечно сильная (полная) экранировка — сигнал для обоих приготавливаемых состояний для 0 и 1 — отвечает вакуумному состоянию излучения. При этом вероятность различения стремится к нулю, соответственно вероятность ошибки различения стремится к $1/2$.

Таким образом, чтобы описать любой уровень интенсивности побочных сигналов, необходимо ввести пару квантовых состояний, отвечающих приготовлению 0 или 1. Сам явный вид квантовых состояний не потребуется, поскольку различимость состояний определяется только их скалярным произведением, которое есть вероятность различения состояний. Вероятность различения может и должна быть измерена экспериментально для данной аппаратуры.

Отметим еще один важный факт. Введение побочного излучения как квантового состояния позволяет учесть комбинированные совместные измерения побочного излучения и квантовых состояний в канале (при условии, что побочный сигнал рассматривается как квантовый). Еще раз отметим, что детектирование побочного излучения эффективно увеличивает различимость квантовых информационных состояний и при этом не приводит к ошибке на приемной стороне (см. ниже формулу (18)) для длины секретного ключа.

Идея включения пассивного побочного излучения состоит во введении двух дополнительных квантовых состояний в каждом базисе $+$ и $\times$ (далее индекс базиса опускаем, поскольку анализ аналогичен для каждого базиса), описывающих побочное излучение. Наиболее общим описанием квантового состояния является описание при помощи матрицы плотности. Умозрительно можно провести полную квантовую томографию побочного излучения во всех спектральных диапазонах для данной конкретной реализации системы КРК. Однако из-за огромного числа степеней свободы передающей ап-

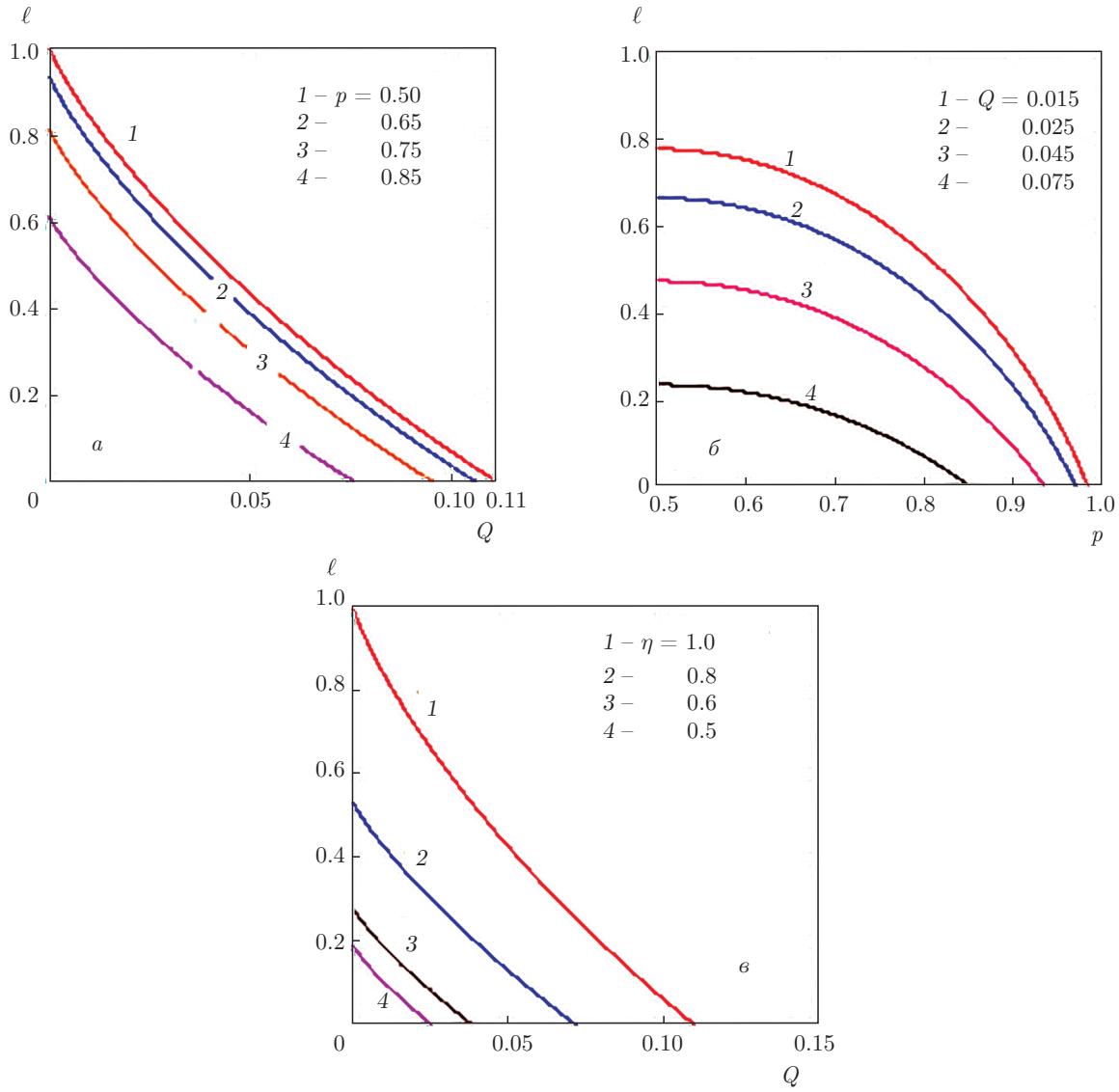

Рис. 2. Зависимости от Q, p длины секретного ключа в пересчете на одну позицию для однофотонного случая при различных побочных каналах утечки информации. *а*) Зависимости длины секретного ключа от наблюдаемой ошибки на приемной стороне Q при различных значениях вероятности различимости p состояния побочного излучения аппаратуры передающей станции. *б*) Зависимости длины секретного ключа от вероятности различимости p состояний побочного излучения передающей аппаратуры при различных значениях наблюдаемой ошибки Q на приемной стороне. *в*) Зависимости длины секретного ключа от наблюдаемой ошибки на приемной стороне Q для случая активного зондирования фазового модулятора (параметр перекрытия — различимости η состояний, отраженных от фазового модулятора излучения)

паратуры никто таких измерений в полном объеме не делал и вряд ли сможет сделать. Неизбежно приходится прибегать к каким-то модельным соображениям относительно квантовой структуры матрицы плотности побочного излучения. Как увидим ниже, необязательно точно знать структуру матрицы плотности для побочного излучения, для 0 и 1. Для анализа достаточно знать степень различимости (вероятности ошибки различения, далее параметр p) квантовых состояний побочного излучения, которые отвечают приготовлению информационного состояния 0 и 1. Параметр p подлежит экспериментальному определению и является параметром данной аппаратуры.

Таким образом, учет побочного излучения от аппаратуры Алисы сводится к введению дополнитель-

ного канала между Алисой и Евой. Приготовление состояний $|0^+\rangle_{XX}\langle 0^+|$ и $|1^+\rangle_{XX}\langle 1^+|$ Алисой приводит к побочному излучению, которое пассивно детектируется Евой. Дополнительный побочный канал Алиса–Ева описывается матрицей плотности:

$$|0^+\rangle_{XX}\langle 0^+| \to |0^+\rangle_{XX}\langle 0^+| \otimes [(1-p)|e_0\rangle_{S_AS_A} \times \times \langle e_0| + p|e_1\rangle_{S_AS_A}\langle e_1|], \quad (9)$$

$$|1^+\rangle_{XX}\langle 1^+| \to |1^+\rangle_{XX}\langle 1^+| \otimes [(1-p)|e_1\rangle_{S_AS_A} \times \times \langle e_1| + p|e_0\rangle_{S_AS_A}\langle e_0|]. \quad (10)$$

Логика здесь следующая. Поскольку состояние аппаратуры Алисы Еве полностью неизвестно, Ева «видит» в побочном канале (индекс «S_A» — от Side Channel Alice–Eve) не чистые квантовые состояния $|e_0\rangle_{S_A}$ или $|e_1\rangle_{S_A}$, а статистическую смесь — матрицу плотности. Отметим, во избежание недоразумений, что индексы «0» и «1» в состояниях выше не более чем обозначение и не привязаны напрямую к индексам информационных состояний 0 и 1 (это отчетливо будет видно при обсуждении рис. 2*б*)). Различение состояний при детектировании происходит с вероятностью ошибки p. Сами состояния $|e_0\rangle_{S_A}$ или $|e_1\rangle_{S_A}$ можно считать ортогональными, поскольку ошибка их различения уже заложена в матрицу плотности побочного канала — фактически матрица плотности сразу записана в диагональном представлении. Итак, наличие побочного излучения можно свести к дополнительному бинарному каналу между Алисой и Бобом с ошибкой p. Отметим, что возможны и другие побочные каналы, например, квантовый гауссовский канал. Без ограничения общности данный канал можно считать симметричным для 0 и 1. Обобщение на случай, когда Ева различает 0 и 1 в побочном канале с разной вероятностью (несимметричный канал) проводится простым способом. Только лишь для того, чтобы не загромождать выкладки несложными техническими деталями вычислений, ограничимся симметричным случаем.

Важно отметить, как будет видно ниже, что Ева может использовать совместные коллективные измерения квантового состояния побочного излучения и искаженных состояний ancilla, которые возникают при атаке на информационные квантовые состояния. Отметим, забегая вперед, что формулы, приведенные ниже для оценки длины секретного ключа при различных атаках, включают в себя коллективные совместные измерения побочных квантовых сигналов и информационных состояний в квантовом канале связи.

6. ПОБОЧНЫЙ КАНАЛ УТЕЧКИ, СВЯЗАННЫЙ С АКТИВНЫМ ЗОНДИРОВАНИЕМ ФАЗОВОГО МОДУЛЯТОРА НА ПЕРЕДАЮЩЕЙ СТАНЦИИ

Учет квантового канала утечки, связанного с активным зондированием состояния фазового модулятора, проводится аналогичным способом — введением дополнительного квантового канала связи, с той лишь разницей, что состояние отраженного излучения задается Евой посредством задания входного зондирующего излучения. После отражения от фазового модулятора зондирующего излучения Ева имеет в своем распоряжении квантовое состояние $|E_0\rangle_{Q_A}$, если фазовый модулятор был в состоянии приготовления информационного состояния, отвечающего логическому 0. Например, Ева может зондировать когерентным состоянием, поскольку все внутреннее устройство системы КРК считается известным Еве, и Ева может откалибровать на части посылок отраженные состояния, включая фазу отраженного когерентного зондирующего состояния. Поэтому в пользу Евы будем считать, что отраженное состояние является чистым квантовым состоянием. В этом случае вместо (9), (10) имеем с учетом отраженного квантового состояния:

$$|0^+\rangle_{XX}\langle 0^+| \otimes [(1-p)|e_0\rangle_{S_AS_A} \times \times \langle e_0| + p|e_1\rangle_{S_AS_A}\langle e_1|] \otimes |E_0\rangle_{Q_AQ_A}\langle E_0|. \quad (11)$$

Аналогично, для случая приготовления информационного состояния, отвечающего логической 1 имеем

$$|1^+\rangle_{XX}\langle 1^+| \otimes [(1-p)|e_1\rangle_{S_AS_A}\langle e_1| + p|e_0\rangle_{S_AS_A} \times \times \langle e_0|] \otimes |E_1\rangle_{Q_AQ_A}\langle E_1|. \quad (12)$$

В зависимости от реализации системы КРК возможно активное зондирование состояния фазового модулятора на приемной станции. Для отдельных реализаций систем КРК фазовый модулятор на приемной станции отсутствует (например, в системе [14]), это снимает вопросы, связанные с зондированием фазового модулятора на приемной станции и утечками на приемной станции по данному побочному каналу, что улучшает защищенность системы. Имея в виду такие реализации системы КРК, активное зондирование фазового модулятора на приемной станции не учитываем, как не актуальное.

7. ПОБОЧНЫЙ КАНАЛ УТЕЧКИ, СВЯЗАННЫЙ С ПЕРЕИЗЛУЧЕНИЕМ ЛАВИННЫХ ДЕТЕКТОРОВ НА ПРИЕМНОЙ СТАНЦИИ

Еще одним реальным каналом утечки информации является переизлучение лавинных детекторов при срабатывании. Известно, что рождение лавины носителей при регистрации фотонов в лавинных детекторах приводит к обратному излучению из-за рекомбинации неравновесных носителей из лавины, которое можно регистрировать и тем самым узнать, какой из лавинных детекторов сработал: отвечающий регистрации 0 или регистрации 1. Обычно в системах КРК используются два лавинных детектора, в заданном базисе один отвечает за регистрацию 0, второй — за регистрацию 1. На формальном уровне это означает, что к состояниям $|0^+\rangle_{YY}\langle 0^+|$ и $|1^+\rangle_{YY}\langle 1^+|$ на приемной стороне нужно «привязать» квантовые состояния — матрицы плотности, отвечающие квантовому состоянию обратного излучения. Поскольку переизлученное квантовое состояние заведомо некогерентное, описание с помощью матрицы плотности является естественным. Аналогично (9)–(12) получаем, что каждое квантовое состояние для 0 и 1 на приемной стороне нужно заменить,

$$|0^+\rangle_{YY}\langle 0^+| \to |0^+\rangle_{YY}\langle 0^+| \otimes [(1-d)|d_0\rangle_{S_BS_B} \times \times \langle d_0| + d|d_1\rangle_{S_BS_B}\langle d_1|], \quad (13)$$

$$|1^+\rangle_{YY}\langle 1^+| \to |1^+\rangle_{YY}\langle 1^+| \otimes [(1-d)|d_1\rangle_{S_BS_B} \times \times \langle d_1| + d|d_0\rangle_{S_BS_B}\langle d_0|], \quad (14)$$

где d — вероятность ошибки различения одного из двух переизлученных квантовых состояний, $|d_{0,1}\rangle_{S_B}$ — квантовые состояния обратного излучения, которые по тем же соображениям, как и в случае пассивного побочного излучения в (9), (10) можно считать без ограничения общности ортогональными. Опять, лишь для того чтобы не загромождать вычисления простыми, но не достаточно короткими выкладками, считаем данный побочный канал симметричным. Обобщение на общий несимметричный случай делается аналогично.

Матрица плотности Алиса–Боб–Ева с учетом упомянутых выше побочных каналов утечки информации принимает вид

$$\begin{aligned}\rho_{XYS_AQ_AQS_B} = {}& \frac{1}{2}|0^+\rangle_{XX}\langle 0^+| \otimes [(1-p)|e_0\rangle_{S_AS_A} \times \\ & \times \langle e_0| + p|e_1\rangle_{S_AS_A}\langle e_1|] \otimes |E_0\rangle_{Q_AQ_A}\langle E_0| \otimes \\ & \otimes \big[(1-Q)|0^+\rangle_{YY}\langle 0^+| \otimes |\Phi_{0^+}\rangle_{QQ}\langle \Phi_{0^+}| \otimes \\ & \otimes [(1-d)|d_0\rangle_{S_BS_B}\langle d_0| + d|d_1\rangle_{S_BS_B}\langle d_1|] + \\ & + Q|1^+\rangle_{YY}\langle 1^+| \otimes |\Theta_{0^+}\rangle_{QQ}\langle \Theta_{0^+}| \otimes \\ & \otimes [(1-d)|d_1\rangle_{S_BS_B}\langle d_1| + d|d_0\rangle_{S_BS_B}\langle d_0|]] + \\ & + \frac{1}{2}|1^+\rangle_{XX}\langle 1^+| \otimes [(1-p)|e_1\rangle_{SS}\langle e_1| + p|e_0\rangle_{SS} \times \\ & \times \langle e_0|] \otimes |E_1\rangle_{Q_AQ_A}\langle E_1| \otimes \big[(1-Q)|1^+\rangle_{YY}\langle 1^+| \otimes \\ & \otimes |\Phi_{1^+}\rangle_{QQ}\langle \Phi_{1^+}| \otimes [(1-d)|d_1\rangle_{S_BS_B}\ \langle d_1| + \\ & + d|d_0\rangle_{S_BS_B}\langle d_0|] + Q|0^+\rangle_{YY}\langle 0^+| \otimes |\Theta_{1^+}\rangle_{QQ} \times \\ & \times \langle \Theta_{1^+}| \otimes [(1-d)|d_0\rangle_{S_BS_B}\langle d_0| + d|d_1\rangle_{S_BS_B} \times \\ & \times \langle d_1|]]\,. \quad (15)\end{aligned}$$

Напомним, что канал утечки, связанный с зондированием модулятора интенсивности, будет проведен на следующем этапе при модификации Decoy State-метода.

8. УТЕЧКА ИНФОРМАЦИИ ПРИ КОРРЕКЦИИ ОШИБОК

Коррекция ошибок в «сырых» ключах также может рассматриваться как побочный канал утечки через открытый классический канал связи, через который легитимные пользователи передают корректирующую информацию — синдром ошибок и пр. Принципиальное отличие данного побочного канала от других побочных каналов состоит в том, что Алиса и Боб точно знают, какую информацию они раскрывают через данный канал, в отличие от других побочных каналов.

Матрица плотности Алиса–Боб ρ_{XY}, определяющая количество информации, расходуемое при коррекции ошибок, дается частичным следом по всем состояниям Евы в (15), включая побочные каналы. Имеем

$$\begin{aligned}\rho_{XY} = {}& \frac{1}{2}|0^+\rangle_{XX}\langle 0^+| \otimes [(1-Q)|0^+\rangle_{YY} \times \\ & \times \langle 0^+| + Q|1^+\rangle_{XX}\langle 1^+|] + \frac{1}{2}|1^+\rangle_{XX} \times \\ & \times \langle 1^+| \otimes [(1-Q)|1^+\rangle_{YY}\langle 1^+| + Q|0^+\rangle_{XX}\langle 0^+|]. \quad (16)\end{aligned}$$

Для матрицы плотности Боба ρ_Y находим

$$\rho_Y = \frac{1}{2}[|0^+\rangle_{YY}\langle 0^+| + |1^+\rangle_{YY}\langle 1^+|]. \quad (17)$$

Условная энтропия Алиса–Боб есть минимальное количество информации в битах, расходуемое на

коррекцию ошибок. В шенноновском пределе с учетом (16) получаем

$$H(X|Y) = H(\rho_{XY}|\rho_Y) = \\ = H(\rho_{XY}) - H(|\rho_Y) = h(Q). \quad (18)$$

Отметим, что в информацию $h(Q)$ в (18), расходуемую на коррекцию ошибок, не входят параметры побочного излучения, поскольку измерение состояний в побочных каналах (пусть даже вместе с информационными) не приводит к ошибкам на приемной стороне, что, на наш взгляд, естественно с точки зрения физической интуиции.

9. ПОЛНАЯ УТЕЧКА ИНФОРМАЦИИ К ПОДСЛУШИВАТЕЛЮ

В формулу для длины секретного ключа входит условная энтропия Алиса–Ева, которая выражается через матрицы плотности $\rho_{XS_AQ_AQS_B}$ и $\rho_{S_AQ_AQS_B}$. Неформально, данная величина отвечает за нехватку информации Евы о битовой строке Алисы при условии, что Ева имеет в своем распоряжении квантовые системы, отвечающие всевозможным каналам утечки информации. С учетом (15) получаем

$$\rho_{XS_AQ_AQS_B} = \frac{1}{2}|0^+\rangle_{X\,X}\langle 0^+| \otimes [(1-p)|e_0\rangle_{S_AS_A} \times \\ \times \langle e_0| + p|e_1\rangle_{S_AS_A}\langle e_1|] \otimes |E_0\rangle_{Q_AQ_A}\langle E_0| \otimes \\ \otimes [(1-Q)|\Phi_{0^+}\rangle_{QQ}\langle\Phi_{0^+}| \otimes [(1-d)|d_0\rangle_{S_BS_B} \times \\ \times \langle d_0| + d|d_1\rangle_{S_BS_B}\langle d_1|] + Q|\Theta_{0^+}\rangle_{QQ}\langle\Theta_{0^+}| \otimes \\ \otimes [(1-d)|d_1\rangle_{S_BS_B}\langle d_1| + d|d_0\rangle_{S_BS_B}\langle d_0|]] + \\ + \frac{1}{2}|1^+\rangle_{X\,X}\langle 1^+| \otimes [(1-p)|e_1\rangle_{SS} \times \\ \times \langle e_1| + p|e_0\rangle_{SS}\langle e_0|] \otimes |E_1\rangle_{Q_AQ_A} \times \\ \times \langle E_1| \otimes [(1-Q)|\Phi_{1^+}\rangle_{QQ}\langle\Phi_{1^+}| \otimes [(1-d)|d_1\rangle_{S_BS_B} \times \\ \times \langle d_1| + d|d_0\rangle_{S_BS_B}\langle d_0|] + Q|\Theta_{1^+}\rangle_{QQ} \times \\ \times \langle\Theta_{1^+}| \otimes [(1-d)|d_0\rangle_{S_BS_B}\langle d_0| + d|d_1\rangle_{S_BS_B} \times \\ \times \langle d_1|]]\,. \quad (19)$$

Собственные числа (19) равны

$$\frac{1}{2}(1-Q)(1-p)(1-d), \quad \frac{1}{2}Q(1-p)(1-d), \\ \frac{1}{2}(1-Q)p(1-d), \quad \frac{1}{2}Qp(1-d), \quad (20)$$

$$\frac{1}{2}(1-Q)(1-p)\,d, \quad \frac{1}{2}Q(1-p)\,d, \\ \frac{1}{2}(1-Q)pd, \quad \frac{1}{2}Qpd, \quad (21)$$

причем собственные числа двукратно вырождены. С учетом (20), (21) получаем выражение для энтропии,

$$H(\rho_{XS_AQ_AQS_B}) = 1 + h(p) + h(d) + h(Q). \quad (22)$$

Перейдем к вычислению $H(\rho_{S_AQ_AQS_B})$. Для матрицы плотности $\rho_{S_AQ_AQS_B}$ находим

$$\rho_{S_AQ_AQS_B} = \frac{1}{2}[(1-p)|e_0\rangle_{S_AS_A}\langle e_0| + p|e_1\rangle_{S_AS_A} \times \\ \times \langle e_1|] \otimes |E_0\rangle_{Q_AQ_A}\langle E_0| \otimes [(1-Q)|\Phi_{0^+}\rangle_{QQ} \times \\ \times \langle\Phi_{0^+}| \otimes [(1-d)|d_0\rangle_{S_BS_B}\langle d_0| + d|d_1\rangle_{S_BS_B} \times \\ \times \langle d_1|] + Q|\Theta_{0^+}\rangle_{QQ}\langle\Theta_{0^+}| \otimes [(1-d)|d_1\rangle_{S_BS_B} \times \\ \times \langle d_1| + d|d_0\rangle_{S_BS_B}\langle d_0|]] + \\ + \frac{1}{2}[(1-p)|e_1\rangle_{SS}\langle e_1| + p|e_0\rangle_{SS}\langle e_0|] \otimes |E_1\rangle_{Q_AQ_A} \times \\ \times \langle E_1| \otimes [(1-Q)|\Phi_{1^+}\rangle_{QQ}\,\langle\Phi_{1^+}| \otimes [(1-d)|d_1\rangle_{S_BS_B} \times \\ \times \langle d_1| + d|d_0\rangle_{S_BS_B}\langle d_0|] + Q|\Theta_{1^+}\rangle_{QQ} \times \\ \times \langle\Theta_{1^+}| \otimes [(1-d)|d_0\rangle_{S_BS_B} \times \\ \times \langle d_0| + d|d_1\rangle_{S_BS_B}\langle d_1|]]\,. \quad (23)$$

Собственные числа $\rho_{S_AQ_AQS_B}$ определяются корнями секулярных уравнений

$$\mathrm{Det}\begin{pmatrix} A_i - \lambda & \varepsilon\eta(C_i - \lambda) \\ \varepsilon\eta(C_i - \lambda) & B_i - \lambda \end{pmatrix} = 0, \quad (24)$$

где

$$A_1 = (1-p)(1-d) + pd\varepsilon^2\eta^2, \\ B_1 = (1-p)(1-d)\varepsilon^2\eta^2 + pd, \quad (25) \\ C_1 = (1-p)(1-d) + pd,$$

$$A_2 = (1-p)\,d + p(1-d)\varepsilon^2\eta^2, \\ B_2 = (1-p)\,d\varepsilon^2\eta^2 + p(1-d), \quad (26) \\ C_1 = (1-p)\,d + p(1-d),$$

$$A_3 = p(1-d) + (1-p)\,d\varepsilon^2\eta^2, \\ B_3 = p(1-d)\varepsilon^2\eta^2 + (1-p)\,d, \quad (27) \\ C_3 = p(1-d) + (1-p)\,d,$$

$$A_4 = pd + (1-p)(1-d)\varepsilon^2\eta^2, \\ B_4 = pd\varepsilon^2\eta^2 + (1-p)(1-d), \quad (28) \\ C_4 = pd + (1-p)(1-d).$$

Корни

$$\lambda_{i\pm} = \frac{1}{2(1-\varepsilon^2\eta^2)}\Big[A_i + B_i - 2\varepsilon^2\eta^2C_i \pm \\ \pm \big([A_i + B_i - 2\varepsilon^2\eta^2C_i]^2 - \\ - 4[A_iB_i - \varepsilon^2\eta^2C_i^2](1-\varepsilon^2\eta^2)\big)^{1/2}\Big]. \quad (29)$$

Корни

$$\frac{1}{2}(1-Q)\lambda_{i\pm}, \quad \frac{1}{2}Q\lambda_{i\pm},, \quad I=1,2,3,4, \tag{30}$$

двукратно вырождены. Введем обозначение

$$\chi_i(p,d,\eta,Q) = -\lambda_{i+}\log(\lambda_{i+}) - \lambda_{i-}\log(\lambda_{i-}),$$
$$\chi(p,d,\eta,Q) = \sum_{i=1}^{4}\chi_i(p,d,\eta,Q). \tag{31}$$

В итоге

$$H(\rho_{XS_AQ_AQS_B}|\rho_{S_AQ_AQS_B}) = \\ = h(p) + h(d) - \chi(p,d,\eta,Q). \tag{32}$$

Для оценки длины секретного ключа в строго однофотонном случае с учетом (16), (32) получаем

$$\ell = \lim_{n\to\infty}\frac{\ell_n}{n} = h(p)+h(d)-\chi(p,d,\eta,Q)-h(Q), \tag{33}$$

где утечка информации при коррекции ошибок взята в шенноновском пределе. При коррекции конструктивными кодами последнее слагаемое в правой части (33) нужно заменить $h(Q) \to \text{leak}$ — на реальное число битов в пересчете на одну позицию, раскрытое при коррекции ошибок.

Отметим во избежание недоразумений следующее. В формуле (33), на первый взгляд, первые два слагаемых при значениях параметров $p = d = 0.5$ (полная неразличимость состояний в побочных каналах) дают значение $h(p) + h(d) = 2$, однако выражение для $\chi(p,d,\eta,Q)$ в (31) и величины в (33) определены таким образом, что величина (33) никогда не превышает одного бита.

10. ПРЕДЕЛЬНЫЕ СЛУЧАИ, ФИЗИЧЕСКАЯ ИНТЕРПРЕТАЦИЯ

Прежде чем перейти к оценке доли однофотонной компоненты в информационных состояниях при помощи модифицированного Decoy State-метода, полезно рассмотреть предельные случаи и дать простую и интуитивную интерпретацию полученных результатов.

Первый случай — когда имеется один побочный канал утечки информации, связанный с излучением передающей аппаратуры Алисы, состояние в котором детектируется совместно с информационными квантовыми состояниями. В этом случае собственные числа в (30) становятся равными

$$\frac{1}{2}(1-Q)\lambda_+, \quad \frac{1}{2}(1-Q)\lambda_-, \quad \frac{1}{2}Q\lambda_+, \quad \frac{1}{2}Q\lambda_-,$$

где

$$\lambda_\pm = \frac{1}{2}\left(1 \pm \sqrt{1-4\Lambda(p,\epsilon)}\right), \tag{34}$$

$$\Lambda(p,\epsilon) = \frac{1}{1-\epsilon^2}\left\{[(1-p)+p\epsilon^2][(1-p)\epsilon^2+p]-\epsilon^2\right\},$$

$$\epsilon = {}_Q\langle\Phi_{0^+}|\Phi_{1^+}\rangle_Q = {}_Q\langle\Theta_{0^+}|\Theta_{1^+}\rangle_Q = 1-2Q$$

(см. детали в [14])[1)]. Вместо (32) для энтропии имеем

$$H(\rho_{QS}) = 1 + \chi(p,\epsilon) + h(Q),$$
$$H(\rho_{XQS}|\rho_{QS}) = h(p) - \chi(p,\epsilon), \tag{35}$$

где

$$\chi(p,\epsilon) = -\lambda_+\log(\lambda_+) - \lambda_-\log(\lambda_-).$$

Принимая во внимание (35), для длины секретного ключа получаем

$$\ell = \frac{\ell_n}{n} = h(p) - \chi(p,\epsilon) - h(Q). \tag{36}$$

Данный результат имеет ясную интуитивную интерпретацию. Если Ева не вторгается в квантовый канал, а получает информацию о ключе, только регистрируя побочное излучение от аппаратуры, то фактически Ева и Алиса находятся в ситуации бинарного канала с информационными состояниями для Евы (9), (10). В этом случае нехватка информации Евы о битовой строке Алисы определяется условной энтропией бинарного канала с вероятностью ошибки различения p и условной энтропией $h(p)$. Длина секретного ключа определяется нехваткой информации Евы из побочного канала $h(p)$, которая равна классической условной энтропии бинарного классического канала с ошибкой p [32], за вычетом информации, потраченной на коррекцию ошибок $h(Q)$. При этом ошибка Q не связана с побочным излучением и не зависит от него. Примеры расчетов для данного предельного случая приведены на рис. 2. Из рис. 2*a* видно, что наблюдаемая критическая ошибка на приемной стороне, до которой можно распределять секретные ключи при наличии побочного канала, уменьшается с ростом различимости состояний побочного излучения передающей станции. Величина $p = 1/2$ отвечает полной неразличимости состояний побочного излучения. В этом случае критическая ошибка совпадает с классическим результатом для протокола BB84 в однофотонном случае и равна $Q_c \approx 11\,\%$ (дается корнем уравнения $1 = 2h(Q_c)$). С увеличением p растет информация,

[1)] Отметим, что для того, чтобы получить предел в формуле (34) при $Q \to 0$, нужно воспользоваться правилом Лопиталя до второго порядка малости при разложении знаменателя $1-\varepsilon^2$ и числителя до второго порядка малости по $1-2Q$.

получаемая из побочного канала. В принятых нами обозначениях величина $p = 1.0$ (см. формулу (36)) отвечает достоверной различимости состояний побочного излучения. В этом случае $h(p = 1.0) = 0$, Ева получает достоверную информацию о каждом передаваемом бите ключа из побочного канала. Второе слагаемое в правой части формулы (36) отвечает за информацию Евы, полученную от совместного коллективного измерения квантового состояния побочного излучения и информационных квантовых состояний.

На рис. 2*б* приведены зависимости длины секретного ключа при заданной наблюдаемой ошибке на приемной стороне при различных значениях вероятности p — ошибки различения состояний в побочном канале утечки. Поведение зависимости от значения p аналогично рис. 2*а* — увеличение различимости состояний в побочном канале ведет к уменьшению длины секретного ключа. Принципиально важно отметить, что в формуле (36) Ева использует коллективные измерения как над квантовым состоянием побочного излучения, так и над информационными состояниями в канале (см. замечание выше). Фактически величина χ в (36) является величиной Холево [33, 34] для совместного квантового состояния: побочное излучение + информационное состояние, это подчеркивает важность рассмотрения побочного излучения как квантового сигнала. Граница Холево является достижимой при коллективных измерениях [33, 34].

Нехватка информации Евы о строке Алисы X при одновременной атаке на квантовые состояния и детектировании побочного излучения становится равной (см. (4) и (36)) $h(p) - \chi(p, \epsilon)$, что меньше значения без побочного излучения, $1 - h(Q)$. При этом величина $\chi(p, \epsilon)$, по сути, есть информация Холево [33, 34], которая достигается на коллективных совместных измерениях состояния побочного излучения и информационных квантовых состояний.

Отметим, что без вмешательства Евы в квантовый канал (атаки на квантовые состояния) результат выглядит тривиальным. Канал между Алисой и Бобом в совпадающем базисе (без искажения состояний в канале) дается фактически классическим бинарным каналом с вероятностью ошибки Q, это наблюдаемая ошибка. Нехватка информации Боба о битовой строке Алисы есть $h(Q)$, нехватка информации Евы о строке Алисы — $h(p)$. Разность нехватки информации Евы и нехватки информации Боба о строке Алисы есть длина секретного ключа. При учете совместной атаки на побочное излучение и квантовые состояния результат (36) перестает быть тривиальным и содержит за кадром совместные коллективные измерения.

Чем хуже различимы состояния побочного излучения для 0 и 1, тем параметр p ближе к $1/2$ — полная неразличимость состояний побочного излучения для 0 и 1. При этом $h(p = 1/2) = 1$ и результат переходит в длину секретного ключа для протокола BB84 без учета побочного излучения. При $p > 1/2$ величина $h(p) < 1$, поэтому побочное излучение эффективно уменьшает длину секретного ключа (см. (4), (36)). Напомним, что параметр p определяется экранировкой данной реализации аппаратуры и, в принципе, может быть определен экспериментально.

Рассмотрим атаку с активным зондированием состояния фазового модулятора. В этом случае для собственных чисел матрицы плотности ρ_{QS} вместо (20), (21) находим

$$(1-Q)\left(\frac{1+\epsilon\cdot\eta}{2}\right), \quad (1-Q)\left(\frac{1-\epsilon\cdot\eta}{2}\right),$$

$$Q\left(\frac{1+\epsilon\cdot\eta}{2}\right), \quad Q\left(\frac{1-\epsilon\cdot\eta}{2}\right).$$

Для энтропии получаем

$$H(\rho_{QS}) = \chi(\epsilon\eta) + h(Q), \quad \chi(\epsilon\eta) = -\frac{1+\epsilon\cdot\eta}{2} \times$$
$$\times \log\left(\frac{1+\epsilon\cdot\eta}{2}\right) - \frac{1-\epsilon\cdot\eta}{2}\log\left(\frac{1-\epsilon\cdot\eta}{2}\right). \quad (37)$$

Окончательно, с учетом (37) для условной энтропии Алиса–Ева находим

$$H(\rho_{XQS}|\rho_{QS}) = 1 - \chi(\epsilon\eta). \quad (38)$$

Принимая во внимание (38), в шенноновском пределе [26] коррекции ошибок для длины секретного ключа получаем

$$\ell = \frac{\ell_n}{n} = H(\rho_{XQS}|\rho_{QS}) - H(X|Y) =$$
$$= 1 - \chi(\epsilon\eta) - h(Q), \quad (39)$$

где $\epsilon = 1 - 2Q$ и $\eta = |_{Q_A}\langle E_0|E_1\rangle_{Q_A}|$.

Обсудим интерпретацию результата. Зондирование состояния фазового модулятора эффективно увеличивает различимость информационных квантовых состояний, не приводя при этом к дополнительным ошибкам на приемной стороне.

Фазы отраженных когерентных состояний «привязаны» к состоянию фазового модулятора — приготавливаемому информационному состоянию. В пользу Евы можно считать, что фазы когерентных

состояний соответствуют фазам информационных состояний $|0^+\rangle_X$, $|1^+\rangle_X$, $|0^\times\rangle_X$, $|1^\times\rangle_X$, и отраженные состояния имеют вид $|\sqrt{\mu_s}\rangle_S$, $|-\sqrt{\mu_s}\rangle_S$, $|i\sqrt{\mu_s}\rangle_S$, $|-i\sqrt{\mu_s}\rangle_S$, где μ_s — среднее число фотонов в отраженных состояниях. Если в качестве зондирующего излучения используются когерентные состояния, то для η получаем $\eta = |_S\langle\sqrt{\mu_S}| - \sqrt{\mu_s}\rangle_S| = \exp(-2\mu_S)$, μ_S — среднее число фотонов в отраженном зондирующем состоянии. При малых $\mu_s \ll 1$ для величины $\chi(\epsilon\eta)$ в (29) находим $\chi(\epsilon\eta) \approx h(Q(\mu_S))$, $Q(\mu_S) = Q + \mu_S$. Без совместных коллективных измерений зондирующего излучения и квантовых состояний в канале связи длина секретного ключа при наблюдаемой ошибке Q на приемной стороне (см. (4)) равна $1-2h(Q)$. С учетом зондирующего излучения длина секретного ключа равна $1 - h(Q+\mu_S) - h(Q) < 1 - 2h(Q)$ и, естественно, оказывается меньше (напомним, что $Q < 1/2$).

Принципиально важно отметить, что в формуле (38) для длины секретного ключа учтены совместные коллективные измерения отраженных квантовых зондирующих состояний и информационных квантовых состояний, что выражается в появлении в (38) фундаментальной верхней границы утечки информации — границы Холево [33,34], которая достигается на совместных коллективных измерениях отраженных и информационных состояний. Данная граница в нашем случае есть классическая пропускная способность квантово-классического канала связи Алиса–Ева, где информационными состояниями для Евы являются как информационные квантовые состояния (точнее, искаженные состояния ancilla для Евы, коррелированные с информационными состояниями, см. формулы (5), (6)), так и квантовые состояния отраженного зондирующего излучения.

На рис. 2*в* приведены иллюстрирующие расчеты длины секретного ключа для атаки с совместным измерением квантовых состояний и отраженного зондирующего излучения от фазового модулятора. Степень различимости отраженных состояний определяется скалярным произведением состояний — параметром η. Значение $\eta = 1.0$ отвечает ситуации полной неразличимости для подслушивателя отраженных состояний — полное «слипание» отраженных состояний. В этом случае критическая ошибка совпадает со случаем без активного зондирования и равна $Q_c \approx 11\,\%$. Значение $\eta = 0$ отвечает достоверной с вероятностью единица различимости отраженных состояний — отраженные состояния ортогональны между собой. Уменьшение η ведет к уменьшению длины секретного ключа при одном и том же значении наблюдаемой ошибки на приемной стороне.

11. МОДИФИКАЦИЯ DECOY STATE-МЕТОДА С УЧЕТОМ ПОБОЧНЫХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Decoy State-метод был изначально разработан для детектирования PNS-атаки [24]. Данный метод позволяет оценить регистрируемую долю однофотонной компоненты квантовых информационных состояний на приемной стороне. Секретный ключ набирается из однофотонной компоненты, поскольку для однофотонной компоненты можно получить оценку верхней границы утечки информации к подслушивателю. Данная оценка базируется на фундаментальных законах квантовой механики — энтропийных соотношениях неопределенностей. Многофотонные компоненты состояний не фигурируют в секретном ключе и консервативно считаются полностью известными подслушивателю. Как упоминалось выше, стандартный Decoy State-метод неприменим при наличии побочных каналов утечки информации и требует модификации. Поскольку данный момент является важным, для того, чтобы явно обозначить на формальном уровне ту причину, по которой метод требует модификации, изложим кратко исходную стандартную версию Decoy State-метода.

Исходный Decoy State-метод исходит из следующих посылок. Информационными состояниями являются когерентные состояния. Используется несколько когерентных состояний с разным средним числом фотонов. Часть состояний являются информационными, часть — состояниями «ловушками», которые используются для оценки доли однофотонной компоненты регистрируемых состояний и вероятности ошибки в однофотонной компоненте информационных состояний. Фаза когерентных состояний считается полностью рандомизированной — равнораспределенной на отрезке $[0, 2\pi]$. Поскольку фаза когерентных состояний в каждой посылке подслушивателю неизвестна, подслушиватель «видит» в канале не чистые когерентные состояния, а статистическую смесь фоковских состояний с разным числом фотонов. Статистика состояний по числу фотонов является пуассоновской.

Далее для определенности будем рассматривать Decoy State-метод с тремя состояниями (одно информационное, два состояния «ловушки»), соответ-

ственно, со средним числом фотонов $\xi \in \mathcal{I} = \{\mu, \nu_1, \nu_2\}$. Для матрицы плотности состояний в канале имеем

$$\rho^x(\xi) = e^{-2\xi}\sum_{k=0}^{\infty}\frac{(2\xi)^k}{k!}|\Psi_k^x\rangle_{BB}\langle\Psi_k^x| = \sum_{k=0}^{\infty}P^{(k)}(\mu)\times$$
$$\times\,|\Psi_k^x\rangle_{BB}\langle\Psi_k^x|, \quad P_k(\xi) = e^{-2\xi}\frac{(2\xi)^k}{k!}. \quad (40)$$

$$|\Psi_k^x\rangle_B = \sqrt{\frac{k!}{2^k}}\sum_{m=0}^{k}e^{i\varphi_x m}\frac{|m\rangle_1\otimes|k-m\rangle_2}{\sqrt{m!(k-m)!}}, \quad (41)$$

где φ_x — относительная фаза состояний, локализованных во временных окнах 1 и 2, в которую кодируется информация о битах ключа; состояния $|m\rangle_1\otimes$ $\otimes\,|k-m\rangle_2$ — фоковские состояния при фазовом кодировании во временных окнах 1 и 2 (нижние индексы).

Стандартная квантово-механическая интерпретация матрицы плотности — квантового ансамбля — сводится к тому, что в канале присутствуют состояния $|\Psi_k^x\rangle_{BB}\langle\Psi_k^x|$ с разным числом фотонов с вероятностями $P_k(\xi) = e^{-2\xi}(2\xi)^k/k!$.

Основная идея метода состоит в том, что подслушиватель, не имея дополнительной информации и обнаружив в канале связи компоненту состояний с данным числом фотонов k, не знает, из какого состояния и с каким средним числом фотонов данная компонента возникла. Основное предположение стандартного Decoy State-метода основано на том, что, обнаружив число фотонов k, подслушиватель действует каждый раз одинаково, т. е. действия подслушивателя зависят только от обнаруженного числа фотонов в состоянии (40). На формальном уровне действия подслушивателя после обнаружения состояния с данным числом фотонов описываются действием супероператора — вполне положительного отображения — наиболее общего преобразования квантовых состояний в квантовые состояния. Вид супероператора зависит только от обнаруженного числа фотонов в канале.

Супероператор в самом общем виде может быть представлен как

$$\mathcal{T}_{BE}[|\Psi_k^x\rangle_{BB}\langle\Psi_k^x|] = \rho_{k,BE}^x. \quad (42)$$

В результате возникает запутанное состояние Боб–Ева $\rho_{k,BE}^x$. Явный вид состояния в (42) в стандартном Decoy State-методе не требуется. Для оценки доли однофотонной компоненты и вероятности ошибки в ней достаточно только наблюдаемого темпа отсчетов в посылках, отвечающих состояниям с разным средним числом фотонов.

В итоге Боб на приемной стороне измеряет не исходные состояния (41), а состояния (42). Измерения Боба на приемной стороне описываются разложением единицы, обычно ортогональным. Удобно преобразование входных состояний на стороне Боба перед регистрацией включить в операторно-значные меры, имеем

$$I_B = \sum_{y\in\mathcal{Y}}\mathcal{M}_y, \quad y\in\mathcal{Y} = \{0,1\}. \quad (43)$$

В результате измерений у Боба возникает отсчет, который интерпретируется как логический бит $y = 0$ или $y = 1$.

Пусть Алисой было послано состояние, отвечающее логическому значению бита $x = 0, 1$, тогда условная вероятность того, что Боб зарегистрирует значение y есть

$$P_{X|Y}^{(k)}(y|X=x) = \mathrm{Tr}_{BE}\{\mathcal{M}_y\rho_{k,BE}^x\}. \quad (44)$$

Для Decoy State-метода принципиально важно, что условная вероятность зависит не от ξ — среднего числа фотонов в квантовом состоянии, а только от обнаруженного числа фотонов в данной посылке.

Полный темп отсчетов (вероятность, хотя еще и ненормированная) для посылок, когда посылалось состояние со средним числом фотонов ξ, отвечающее логическому значению бита Алисы x, и когда Боб зарегистрировал логическое значение бита y, с учетом (44) равен

$$Q_\xi(y|X=x) = \sum_{k=0}^{\infty}P^{(k)}(\xi)P_{X|Y}^{(k)}(y|X=x). \quad (45)$$

Полная вероятность по всем значениям логических битов x на передающей и y на приемной стороне для состояния со средним числом фотонов ξ равна

$$Q_\xi^{tot} = \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}}P_X(x)Q_\mu(y|X=x) =$$
$$= \sum_{k=0}^{\infty}P^{(k)}(\xi)\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}}P_X(x)P_{X|Y}^{(k)}(y|X=x). \quad (46)$$

Перейдем к обозначениям, часто используемым в работах по стандартному Decoy State-методу, имеем

$$Y_k = \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}}P_X(x)P_{X|Y}^{(k)}(y|X=x) =$$
$$= P_X(0)[P_{X|Y}^{(k)}(0|0) + P_{X|Y}^{(k)}(1|0)] +$$
$$+ P_X(1)[P_{X|Y}^{(k)}(0|1) + P_{X|Y}^{(k)}(1|1)]. \quad (47)$$

Выражение для полного темпа отсчетов для информационных состояний ($\xi = \mu$) в новых обозначениях принимает вид

$$Q_\mu^{tot} = \sum_{k=0}^{\infty} P^{(k)}(\mu) Y_k. \tag{48}$$

Еще раз подчеркнем, что парциальные темпы отсчетов Y_k (в англоязычной версии Yields) не зависят от среднего числа фотонов в состоянии, в данном случае от μ.

Определим вероятность парциальной ошибки для k-фотонной компоненты состояний:

$$e_k = \frac{P_X(0)P_{X|Y}^{(k)}(1|0) + P_X(1)P_{X|Y}^{(k)}(0|1)}{P_X(0)[P_{X|Y}^{(k)}(0|0) + P_{X|Y}^{(k)}(1|0)] + P_X(1)[P_{X|Y}^{(k)}(0|1) + P_{X|Y}^{(k)}(1|1)]}, \tag{49}$$

где $P_X(0)$ и $P_X(1)$ — априорные вероятности для 0 и 1. Данная ошибка также не зависит от самого состояния — среднего числа фотонов в состоянии.

Полная вероятность ошибочных отсчетов для информационных состояний по всем k-фотонным компонентам состояний равна

$$\mathrm{Err}_\mu^{tot} = \sum_{k=0}^{\infty} P^{(k)}(\mu) e_k Y_k. \tag{50}$$

Перейдем теперь к модификации Decoy State-метода с учетом побочных каналов утечки информации.

12. МОДИФИЦИРОВАННЫЙ DECOY STATE-МЕТОД ПРИ АКТИВНОМ ЗОНДИРОВАНИИ МОДУЛЯТОРА ИНТЕНСИВНОСТИ

Зондирование состояния модулятора интенсивности в отличие от зондирования состояния фазового модулятора не дает прямой информации о передаваемом бите ключа, а дает информацию лишь об интенсивности передаваемого состояния. Доля однофотонной компоненты состояний и вероятность ошибки в ней в посылках, где посылались информационные состояния, оценивается через изменение статистики фотоотсчетов в посылках, где посылались состояния «ловушки». Имея дополнительную информацию о том, какое состояние передается в конкретной посылке — информационное или состояние «ловушка» — подслушиватель может менять свою стратегию при данном обнаруженном числе фотонов k. Например, если известно, что послано состояние «ловушка», то подслушиватель ничего не делает (ведет себя пассивно) и не искажает статистику фотоотсчетов состояний ловушек.

Еще раз напомним, что без побочного канала подслушиватель не может различить состояния с разным средним числом фотонов (информационные либо «ловушки»). При наличии побочного канала стандартный Decoy State-метод перестает работать. Ниже явно покажем, на каком этапе это происходит.

Обозначим отраженное от модулятора интенсивности зондирующее квантовое состояние как $|\psi(\xi)\rangle_{S_M}$. Примем, что данное состояние зависит только от состояния модулятора интенсивности — какое состояние со средним числом фотонов $\xi \in \mathcal{I} = \{\mu, \nu_1, \nu_2\}$ посылается в канал связи. Возможно обобщение на случай, когда данное состояние зависит также от состояния фазового модулятора.

Более формально это означает, что при измерении числа фотонов, которые присутствуют в канале связи, вместо состояний со средним числом фотонов k, т. е. вместо состояния $|\Psi_k^x\rangle_{BB}\langle\Psi_k^x|$ (см. (44)), которое не зависит от среднего числа фотонов ξ, в распоряжении подслушивателя будет состояние $|\Psi_k^x(\xi)\rangle_{BSBS}\langle\Psi_k^x(\xi)|$, которое содержит информацию о среднем числе фотонов, что выражается фактом присутствия отраженного зондирующего состояния $|\psi(\xi)\rangle_{S_M}$, и которое дает Еве дополнительную информацию об интенсивности передаваемого состояния. Передаваемое квантовое состояние с учетом зондирующего отраженного излучения, которое «видит» подслушиватель в канале связи, имеет вид

$$\begin{aligned}\rho^x(\xi) &= e^{-2\xi}\sum_{k=0}^{\infty}\frac{(2\xi)^k}{k!}|\Psi_k^x(\xi)\rangle_{BS_M BS_M}\langle\Psi_k^x(\xi)| = \\ &= \sum_{k=0}^{\infty} P^{(k)}(\xi)|\Psi_k^x(\xi)\rangle_{BS_M BS_M}\langle\Psi_k^x(\xi)|,\end{aligned} \tag{51}$$

$$\begin{gathered}P_k(\xi) = e^{-2\xi}\frac{(2\xi)^k}{k!},\\ |\Psi_k^x(\xi)\rangle_{BS_M} = |\Psi_k^x\rangle_B \otimes |\psi(\xi)\rangle_{S_M},\\ \xi = \mu, \nu_1, \nu_2,\end{gathered} \tag{52}$$

где отраженное от модулятора интенсивности состояние $|\psi(\xi)\rangle_{S_M}$ не зависит от информационного состояния.

Основное предположение стандартного Decoy State-метода, основанное на том, что, обнаружив число фотонов k, подслушиватель действует каждый раз одинаково, т. е. действия подслушивателя зависят только от обнаруженного числа фотонов в (40), нарушается, поскольку Ева имеет в своем распоряжении отраженное от модулятора интенсивности квантовое состояние. На формальном уровне это означает, что действия подслушивателя после обнаружения состояния с данным числом фотонов зависят еще от дополнительной информации, которую подслушиватель может получить из отраженного состояния. Цель измерений — узнать, из состояния с каким средним числом фотонов ξ произошла компонента с данным числом фотонов k. Фактически цель подслушивателя состоит в различении одного из состояний $|\psi(\mu)\rangle_{S_M}$, $|\psi(\nu_1)\rangle_{S_M}$, $|\psi(\nu_2)\rangle_{S_M}$.

Полное измерение Евы и Боба ($\mathcal{I} = \{\mu, \nu_1, \nu_2\}$) дается разложением единицы:

$$I_{BS_M} = I_B \otimes I_{S_M} = \left(\sum_{\xi' \in \mathcal{I}} \mathcal{F}_{\xi'}\right) \otimes \otimes \left(\sum_{y \in \mathcal{Y}} \mathcal{M}_y\right), \quad \xi' \in \{\mu, \nu_1, \nu_2\}. \quad (53)$$

Измерение подслушивателя над отраженным состоянием дается положительно-значными мерами $\mathcal{F}_{\xi'}$. Естественно, подслушиватель выбирает оптимальное измерение, которое минимизирует ошибку различения отраженных состояний, отвечающих состояниям с разным средним числом фотонов. Для конструирования оптимального измерения необходимо знать структуру отраженного состояния — в идеале иметь квантовую томографию такого состояния.

Далее нам не потребуются явно сами отраженные состояния, нужно лишь знать вероятности различения разных состояний, которые считаем известными. Получаем

$$P_{J|I}(\xi'|I = \xi) = \mathrm{Tr}_S\{\mathcal{F}_{\xi'}|\psi(\xi)\rangle_{SS}\langle\psi(\xi)|\}, \quad \mathcal{J} = \{\mu, \nu_1, \nu_2\}, \quad (54)$$

где $P_{J|I}(\xi'|I = \xi)$ — условная вероятность того, что в канал было послано состояние со средним числом фотонов ξ, а подслушиватель в результате измерений (53) получил исход ξ', т. е. посчитал, что в канале имеет место состояние со средним числом фотонов ξ'.

С учетом сказанного действие супероператора подслушивателя может быть представлено в виде

$$\mathcal{T}_{BS_M}[|\Psi_k^x\rangle_B \otimes |\psi(\xi)\rangle_{S_M S_M}\langle\psi(\xi)| \otimes {}_B\langle\Psi_k^x|] = \sum_{\xi' \in \mathcal{J}} P_{J|I}(\xi'|I = \xi)\rho^x_{k,\xi',B}. \quad (55)$$

Формула (55) имеет простую и интуитивно ясную интерпретацию. После обнаружения в канале числа фотонов k Ева, в зависимости от исхода измерений над отраженным от модулятора интенсивности квантовым состоянием, осуществляет преобразование фоковского состояния. На формальном языке это означает, что преобразованная матрица плотности $\rho^x_{k,\xi',B}$, в отличие от ситуации без побочного канала (см. формулу (42)), зависит от исходного состояния — от среднего числа фотонов ξ в нем. Эта зависимость выражается через переходные вероятности $P_{J|I}(\xi'|I = \xi)$, которые определяются различимостью отраженных состояний.

Вероятность исходов измерений на приемной стороне Боба выражается через матрицу плотности в (51), с учетом (54) и (55) находим

$$P^{(k)}_{X|Y}(y, \xi'|X = x) = \mathrm{Tr}_B\{\mathcal{M}_y\rho^x_{k,\xi',B}\}. \quad (56)$$

Для парциального темпа отсчетов на приемной стороне вместо (46) получаем

$$Q_\xi(y|X = x) = \sum_{k=0}^{\infty} P^{(k)}(\xi) \times \times \sum_{\xi' \in \mathcal{J}} P_{J|I}(\xi'|I = \xi)P^{(k)}_{X|Y}(y, \xi'|X = x). \quad (57)$$

Для полного темпа отсчетов в посылках с информационными состояниями ($\xi = \mu$) с учетом (57) находим

$$Q^{tot}_\mu = \sum_{k=0}^{\infty} P^{(k)}(\mu) \sum_{\xi' \in \mathcal{J}} P_{J|I}(\xi'|I = \mu) \times \times \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} P_X(x)P^{(k)}_{X|Y}(y, \xi'|X = x). \quad (58)$$

Перейдя к более компактным обозначениям, получаем

$$Y_k(\xi') = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} P_X(x)P^{(k)}_{X|Y}(y, \xi'|X = x) =$$

$$= P_X(0)[P^{(k)}_{X|Y}(0, \xi'|X = 0) + P^{(k)}_{X|Y}(1, \xi'|X = 0)] +$$

$$+ P_X(1)[P^{(k)}_{X|Y}(0, \xi'|X = 1) + P^{(k)}_{X|Y}(1, \xi'|X = 1)]. \quad (59)$$

Далее, обозначая для краткости $P(\xi'|\mu) = P_{J|I}(\xi'|I = \mu)$ для (58), имеем

$$Q_\mu^{tot} = \sum_{k=0}^{\infty} P^{(k)}(\mu) \sum_{\xi' \in \mathcal{J}} P(\xi'|\mu) Y_k(\xi') = \\ = \sum_{k=0}^{\infty} P^{(k)}(\mu)[P(\mu|\mu)Y_k(\mu) + P(\nu_1|\mu)Y_k(\nu_1) + \\ + P(\nu_2|\mu)Y_k(\nu_2)]. \quad (60)$$

Аналогично (60), получаем выражение для парциальной ошибки в информационных состояниях:

$$e_k(\xi') = \frac{P_X(0)P^{(k)}_{X|Y}(1,\xi'|X=0) + P_X(1)P^{(k)}_{X|Y}(0,\xi'|X=1)}{P_X(0)[P^{(k)}_{X|Y}(0,\xi'|X=0) + P^{(k)}_{X|Y}(1,\xi'|X=0)] + P_X(1)[P^{(k)}_{X|Y}(0,\xi|X=1) + P^{(k)}_{X|Y}(1,\xi'|X=1)]}. \quad (61)$$

Используя (57), находим выражение для полной ошибки в информационных состояниях:

$$Err_\mu^{tot} = \sum_{k=0}^{\infty} P^{(k)}(\mu) \sum_{\xi' \in \mathcal{J}} P_{J|I}(\xi'|I=\mu) e_k(\xi') Y_k(\xi') = \\ = \sum_{k=0}^{\infty} P^{(k)}(\mu)[P(\mu|\mu)e_k(\mu)Y_k(\mu) + \\ + P(\nu_1|\mu)e_k(\nu_1)Y_k(\nu_1) + P(\nu_2|\mu)e_k(\nu_2)Y_k(\nu_2)]. \quad (62)$$

13. ОЦЕНКА ПАРАМЕТРОВ МОДИФИЦИРОВАННЫМ DECOY STATE-МЕТОДОМ

Нашей дальнейшей целью будет оценка доли однофотонной компоненты и ошибки в однофотонной компоненте для определения длины секретного ключа. Для вычисления длины секретного ключа необходимо знать по отдельности величины $Y_1(\mu)$, $Y_1(\nu_1)$, $Y_1(\nu_2)$, аналогично для вероятности ошибки нужны отдельные значения $e_1(\mu)$, $e_1(\nu_1)$, $e_1(\nu_2)$. Для того чтобы пояснить суть проблемы, приведем формулу для длины секретного ключа в случае, когда есть только активное зондирование модулятора интенсивности. Нехватка информации Евы с учетом зондирующего излучения в доле однофотонной компоненты есть

$$\sum_\xi \left\{ \frac{P(\xi|\mu)Y_1(\xi)}{\sum_{\xi'} P(\xi'|\mu)Y_1(\xi')}[1 - h(e_1(\xi))] \right\}. \quad (63)$$

Decoy State-метод не позволяет получить выражения для отдельных долей однофотонных компонент и ошибок. Decoy State-метод позволяет получить лишь их комбинации (сумму всех величин, см. ниже). Тем не менее можно будет получить оценку длины ключа, используя только сумму величин.

Перейдем к получению необходимых комбинаций однофотонных компонент. Для дальнейшего введем новые обозначения

$$\overline{Q}_\mu^{tot} = e^{2\mu} Q_\mu^{tot} = \sum_{k=0}^{\infty} \frac{(2\mu)^k}{k!}[P(\mu|\mu)Y_k(\mu) + \\ + P(\nu_1|\mu)Y_k(\nu_1) + P(\nu_2|\mu)Y_k(\nu_2)], \quad (64)$$

$$\overline{Q}_{\nu_1}^{tot} = e^{2\nu_1} Q_{\nu_1}^{tot} = \sum_{k=0}^{\infty} \frac{(2\nu_1)^k}{k!}[P(\mu|\nu_1)Y_k(\mu) + \\ + P(\nu_1|\nu_1)Y_k(\nu_1) + P(\nu_2|\nu_1)Y_k(\nu_2)], \quad (65)$$

$$\overline{Q}_{\nu_2}^{tot} = e^{2\nu_2} Q_{\nu_2}^{tot} = \sum_{k=0}^{\infty} \frac{(2\nu_2)^k}{k!}[P(\mu|\nu_2)Y_k(\mu) + \\ + P(\nu_1|\nu_2)Y_k(\nu_1) + P(\nu_2|\nu_2)Y_k(\nu_2)]. \quad (66)$$

Отметим, что в отличие от стандартного Decoy State-метода в выражения для темпа отсчетов состояний с разным средним числом фотонов входят различные величины Y_k и с разными весовыми коэффициентами — условными вероятностями, зависящими от отраженных состояний от модулятора интенсивности.

Введем новые более удобные обозначения для вероятности ошибки:

$$\overline{\mathrm{Err}}_\mu^{tot} = e^{2\mu} \mathrm{Err}_\mu^{tot} = \sum_{k=0}^{\infty} \frac{(2\mu)^k}{k!}[P(\mu|\mu)e_k(\mu)Y_k(\mu) + \\ + P(\nu_1|\mu)e_k(\nu_1)Y_k(\nu_1) + P(\nu_2|\mu)e_k(\nu_2)Y_k(\nu_2)], \quad (67)$$

$$\overline{\mathrm{Err}}_{\nu_1}^{tot} = e^{2\nu_1} \mathrm{Err}_{\nu_1}^{tot} = \sum_{k=0}^{\infty} \frac{(2\nu_1)^k}{k!} \times \\ \times [P(\mu|\nu_1)e_k(\mu)Y_k(\mu) + P(\nu_1|\nu_1)e_k(\nu_1)Y_k(\nu_1) + \\ + P(\nu_2|\nu_1)e_k(\nu_2)Y_k(\nu_2)], \quad (68)$$

$$\overline{\mathrm{Err}}_{\nu_2}^{tot} = e^{2\nu_2}\mathrm{Err}_{\nu_2}^{tot} = \sum_{k=0}^{\infty}\frac{(2\nu_2)^k}{k!}\times$$
$$\times\left[P(\mu|\nu_2)e_k(\mu)Y_k(\mu) + P(\nu_1|\nu_2)e_k(\nu_1)Y_k(\nu_1) + \right.$$
$$\left. + P(\nu_2|nu_2)e_k(\nu_2)Y_k(\nu_2)\right]. \quad (69)$$

Далее обозначим

$$\begin{aligned} p^{min}(\xi) &= \min_{\xi'\in\{\mu,\nu_1,\nu_2\}} P(\xi'|\xi), \\ p^{max}(\xi) &= \max_{\xi'\in\{\mu,\nu_1,\nu_2\}} P(\xi'|\xi). \end{aligned} \quad (70)$$

С использованием (64)–(70) получаем следующую цепочку неравенств:

$$\overline{Q}_{\mu}^{tot} \geq p^{min}(\mu)Y_0^{\Sigma} + $$
$$+ p^{min}(\mu)\left[2\mu Y_1^{\Sigma} + \sum_{k=2}^{\infty}\frac{(2\mu)^k}{k!}Y_k^{\Sigma}\right], \quad (71)$$

$$\begin{aligned} Y_k^{\Sigma} &= Y_k(\mu) + Y_k(\nu_1) + Y_k(\nu_2), \\ Y_0^{\Sigma} &= \sum_{\xi\in\{\mu,\nu_1,\nu_2\}} Y_0(\xi). \end{aligned} \quad (72)$$

Далее

$$\overline{Q}_{\nu_1}^{tot} \leq p^{max}(\nu_1)Y_0^{\Sigma} + $$
$$+ p^{max}(\nu_1)\left[2\nu_1 Y_1^{\Sigma} + \sum_{k=2}^{\infty}\frac{(2\nu_1)^k}{k!}Y_k^{\Sigma}\right], \quad (73)$$

$$\overline{Q}_{\nu_2}^{tot} \geq p^{min}(\nu_2)Y_0^{\Sigma} + $$
$$+ p^{min}(\nu_2)\left[2\nu_2 Y_1^{\Sigma} + \sum_{k=2}^{\infty}\frac{(2\nu_2)^k}{k!}Y_k^{\Sigma}\right]. \quad (74)$$

Введены обозначения

$$\overline{Q}_{\mu}^{tot,min} = \frac{Q_{\mu}^{tot}}{p^{min}(\mu)}, \quad \overline{Q}_{\nu_1}^{tot,max} = \frac{Q_{\nu_1}^{tot}}{p^{max}(\nu_1)}. \quad (75)$$

Комбинируя (71)–(74), находим

$$(2\nu_1 - 2\nu_2)Y_1^{\Sigma} \geq \left[\overline{Q}_{\nu_1}^{tot,max} - \overline{Q}_{\nu_2}^{tot,min}\right] -$$
$$- \sum_{k=2}^{\infty}\frac{(2\nu_1)^k - (2\nu_2)^k}{k!}Y_k^{\Sigma}. \quad (76)$$

Учитывая, что

$$\frac{(2\nu_1)^2 - (2\nu_2)^2}{(2\mu)^2}\sum_{k=2}^{\infty}\frac{(2\mu)^k}{k!}Y_k^{\Sigma} \geq$$
$$\geq \sum_{k=2}^{\infty}\frac{(2\nu_1)^k - (2\nu_2)^k}{k!}Y_k^{\Sigma}, \quad (77)$$

с учетом (71)–(74) получаем

$$\overline{Q}_{\mu}^{tot,min} - Y_0^{\Sigma} - 2\mu Y_1^{\Sigma} \geq \sum_{k=2}^{\infty}\frac{(2\mu)^k}{k!}Y_k^{\Sigma}. \quad (78)$$

Окончательно находим

$$Y_1^{\Sigma} \geq \frac{1}{(2\nu_1 - 2\nu_2) - \dfrac{(2\nu_1)^2 - (2\nu_2)^2}{2\mu}}\times$$
$$\times\left\{\left[\overline{Q}_{\nu_1}^{tot,max} - \overline{Q}_{\nu_2}^{tot,min}\right] - \frac{(2\nu_1)^2 - (2\nu_2)^2}{(2\mu)^2}\times\right.$$
$$\left.\times\left[\overline{Q}_{\mu}^{tot,min} - Y_0^{\Sigma}\right]\right\}. \quad (79)$$

Как было упомянуто выше и как видно из (79), удается получить лишь оценку для суммы однофотонных компонент Y_1^{Σ}, а не оценку для отдельных компонент. В то же время в оценку для длины секретного ключа (63) входят значения отдельных компонент. Ниже увидим, что эту проблему удается обойти, используя свойство выпуклости условных энтропий.

Для оценки суммарной доли вакуумной компоненты Y_0^{Σ} с учетом (73), (74) получаем

$$Y_0^{\Sigma} \geq \max\left\{\frac{2\nu_1\overline{Q}_{\nu_2}^{tot,max} - 2\nu_2\overline{Q}_{\nu_1}^{tot,min}}{2\nu_1 - 2\nu_2}, 0\right\}, \quad (80)$$

где

$$\begin{aligned} \overline{Q}_{\nu_{1,2}}^{tot,min} &= \frac{Q_{\nu_{1,2}}^{tot}}{p^{min}(\nu_{1,2})}, \\ \overline{Q}_{\nu_{1,2}}^{tot,max} &= \frac{Q_{\nu_{1,2}}^{tot}}{p^{max}(\nu_{1,2})}. \end{aligned} \quad (81)$$

Получим оценку для вероятности ошибки в однофотонной компоненте состояний:

$$\overline{Err}_{\nu_1}^{tot} \geq p^{min}(\nu_1)\left\{\sum_{k=0}^{\infty}\frac{(2\nu_1)^k}{k!}(eY)_k^{\Sigma}\right\}. \quad (82)$$

Аналогично предыдущему находим

$$\overline{Err}_{\nu_2}^{tot} \leq p^{max}(\nu_2)\left\{\sum_{k=0}^{\infty}\frac{(2\nu_2)^k}{k!}(eY)_k^{\Sigma}\right\}, \quad (83)$$

где введено обозначение

$$(eY)_k^{\Sigma} = e_k(\mu)Y_k(\mu) + e_k(\nu_1)Y_k(\nu_1) +$$
$$+ e_k(\nu_2)Y_k(\nu_2). \quad (84)$$

Комбинируя неравенства (73) и (74), получаем

$$(eY)_1^{\Sigma} \leq \frac{\overline{\mathrm{Err}}_{\nu_1}^{tot,min} - \overline{\mathrm{Err}}_{\nu_2}^{tot,max}}{2\nu_1 - 2\nu_2}, \quad (85)$$

где введены обозначения

$$\overline{\mathrm{Err}}_{\nu_1}^{tot,min} = \frac{\overline{\mathrm{Err}}_{\nu_1}^{tot}}{p^{min}(\nu_1)}, \qquad \overline{\mathrm{Err}}_{\nu_2}^{tot,max} = \frac{\overline{\mathrm{Err}}_{\nu_2}^{tot}}{p^{max}(\nu_2)}. \tag{86}$$

14. ОЦЕНКА ДЛИНЫ СЕКРЕТНОГО КЛЮЧА

В разделах выше были получены оценки длины секретного ключа для строго однофотонной компоненты. При этом параметры, описывающие побочное излучение (p, d, η) следует относить к посылкам, в которых посылались информационные состояния со средним числом фотонов μ. Выражения для длины секретного ключа (см. формулу (33)) имеют следующую структуру:

$$\begin{aligned} &P(\mu|\mu)Y_1(\mu)[f(p,d) - \chi(e_1(\mu),p,d,\eta)] + \\ &\quad + P(\nu_1|\mu)Y_1(\nu_1)[f(p,d) - \chi(e_1(\nu_1),p,d,\eta)] + \\ &\quad + P(\nu_2|\mu)Y_1(\nu_2)[f(p,d) - \chi(e_1(\nu_2),p,d,\eta)], \end{aligned} \tag{87}$$

где $f(p,d)$ — одна из функций в (33); в формулах (36), (39), чтобы перейти к формулам (87), нужно заменить $Q \to e_1(\xi)$. Формула (87) имеет простую интерпретацию. Неформально говоря, после обнаружения в канале состояния с числом фотонов k, Ева проводит измерения отраженного зондирующего состояния с целью выяснить, из какого состояния, информационного или состояния «ловушки», произошло обнаруженное состояние. После измерения, вероятность исхода дается условной вероятностью $P(\xi'|\xi)$, Ева делает вывод о дальнейших действиях. Другими словами, вероятности ошибки $e_1(\xi)$ в (87) и доли однофотонной компоненты $Y_1(\xi)$ зависят от исхода измерений над отраженным состоянием. Условные вероятности $P(\xi'|\xi)$ являются известными.

Функции $\chi(e_1(\xi),p,d,\eta)$ в (33) и (39) являются выпуклыми функциями аргументов. Используя это свойство, получаем следующее неравенство:

$$\begin{aligned} &\frac{P(\mu|\mu)Y_1(\mu)}{\sum_\xi P(\xi|\mu)Y_1(\xi)}\chi(e_1(\mu),p,d,\eta) + \frac{P(\nu_1|\mu)Y_1(\nu_1)}{\sum_\xi P(\xi|\mu)Y_1(\xi)} \times \\ &\times\chi(e_1(\nu_1),p,d,\eta) + \frac{P(\nu_2|\mu)Y_1(\nu_2)}{\sum_\xi P(\xi|\mu)Y_1(\xi)}\chi(e_1(\nu_2),p,d,\eta) \le \\ &\le \frac{p^{max}(\mu)}{p^{min}(\mu)}\left\{\frac{Y_1(\mu)}{Y_1^\Sigma}\chi(e_1(\mu),p,d,\eta) + \right. \\ &\left. + \frac{Y_1(\nu_1)}{Y_1^\Sigma}\chi(e_1(\nu_1),p,d,\eta)\frac{Y_1(\nu_2)}{Y_1^\Sigma}\chi(e_1(\nu_2),p,d,\eta)\right\} \le \\ &\le \frac{p^{max}(\mu)}{p^{min}(\mu)}\chi\left(\frac{(eY)_1^\Sigma}{Y_i^\Sigma},p,d,\eta\right). \end{aligned} \tag{88}$$

В итоге, используя (87) и (88), для доли секретных битов получаем

$$\begin{aligned} \ell = \frac{\ell_n}{n} = f(p,d) - &\left\{\frac{P(\mu|\mu)Y_1(\mu)}{\sum_\xi P(\xi|\mu)Y_1(\xi)}\chi(e_1(\mu),p,d,\eta) + \right. \\ &+ \frac{P(\nu_1|\mu)Y_1(\nu_1)}{\sum_\xi P(\xi|\mu)Y_1(\xi)}\chi(e_1(\nu_1),p,d,\eta) + \\ &\left. + \frac{P(\nu_2|\mu)Y_1(\nu_2)}{\sum_\xi P(\xi|\mu)Y_1(\xi)}\chi(e_1(\nu_2),p,d,\eta)\right\} \ge \\ \ge f(p,d) - &\frac{p^{max}(\mu)}{p^{min}(\mu)}\left\{\frac{Y_1(\mu)}{Y_1^\Sigma}\chi(e_1(\mu),p,d,\eta) + \right. \\ &\left. + \frac{Y_1(\nu_1)}{Y_1^\Sigma}\chi(e_1(\nu_1),p,d,\eta) + \frac{Y_1(\nu_2)}{Y_1^\Sigma}\chi(e_1(\nu_2),p,d,\eta)\right\} \ge \\ \ge f(p,d) - &\frac{p^{max}(\mu)}{p^{min}(\mu)}\chi\left(\frac{(eY)_1^\Sigma}{Y_1^\Sigma},p,d,\eta\right). \end{aligned} \tag{89}$$

В формулу (89) входят интегральная доля однофотонной компоненты Y_1^Σ и интегральная ошибка в однофотонной компоненте состояний $(eY)_1^\Sigma$. Данные величины выражаются в модифицированном Decoy State-методе через наблюдаемые величины — темпы отсчетов на приемной стороне для состояний с разным средним числом фотонов.

Обратим внимание на то, что при получении формулы (89) значения параметров p и d, описывающих различимость, соответственно, состояний побочного излучения аппаратуры передающей станции и различимости состояний при переизлучении лавинных детекторов, считались одинаковыми при разных состояниях модулятора интенсивности — состояний с разным числом фотонов. Тот факт, что данные параметры могут зависеть от состояния модулятора интенсивности, может быть несложно учтен с использованием свойства выпуклости энтропии. В этом случае функцию $f(p,d)$ следует заменить на $\frac{p^{min}(\mu)}{p^{max}(\mu)}f(p^{max},d^{max})$, где $1/2 \le p^{max} \le 1$, $1/2 \le d^{max} \le 1$ в аргументе f отвечают максимальным вероятностям различения побочного излучения передающей станции и переизлучения лавинных детекторов при трех разных состояниях модулятора интенсивности, посылаемых в канал состояний с разным средним числом фотонов $\{\mu,\nu_1,\nu_2\}$. Напомним, что ошибка различения побочного излучения и состояний переизлучения детекторов, а также равенства $p = 1/2$ и $d = 1/2$ отвечают ситуации полной неразличимости состояний в побочных каналах. Учитывая (89), окончательно для длины секретного ключа получаем

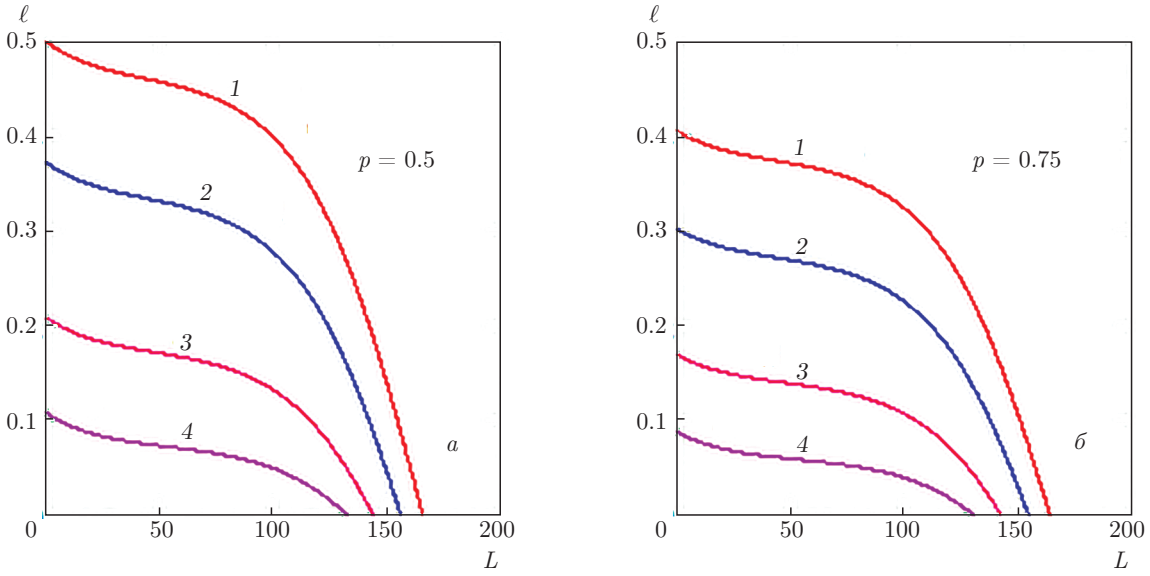

Рис. 3. Зависимости длины секретного ключа в пересчете на одну посылку от длины линии связи L для случая детектирования только побочного излучения передающей станции для $p = 0.5$ ($а$), 0.75 ($б$). Оценка длины секретного ключа проводилась модифицированным Decoy State-методом. Отношения вероятностей различения отраженных состояний от модулятора интенсивности $\frac{p^{max}(\mu)}{p^{min}(\mu)} = 0.9$ (*1*), 0.8 (*2*), 0.7 (*3*), 0.65 (*4*). Остальные значения параметров одинаковы для рис. $а$ и $б$: среднее число фотонов в информационных состояниях $\mu = 0.25$, среднее число в состояниях «ловушках» $\nu_1 = 0.1$ и $\nu_2 = 0.01$, квантовая эффективность детектора на приемной стороне $\eta_d = 0.2$, вероятность темновых отсчетов на строб лавинного детектора $p_d = 10^{-6}$, удельные потери в линии связи $\delta = 0.2$ дБ/км

$$\ell = \frac{\ell_n}{n} \geq \frac{p^{min}(\mu)}{p^{max}(\mu)} f(p^{max}, d^{max}) - \frac{p^{max}(\mu)}{p^{min}(\mu)} \times \\ \times \chi\left(\frac{(eY)_1^{\Sigma}}{Y_1^{\Sigma}}, p^{max}, d^{max}, \eta(\mu_s)\right). \quad (90)$$

В формуле (89) величины $p^{min,max}$, $d^{min,max}$ должны находиться экспериментально посредством измерения состояний, отраженных от модулятора интенсивности. Величины $(eY)_1^{\Sigma}$ и Y_1^{Σ} определяются по экспериментально наблюдаемым ошибкам и темпам отсчетов. Перекрытие отраженных состояний $\eta(\mu_s)$ при активном зондировании фазового модулятора также должно определяться экспериментально для каждой реализации системы КРК. Напомним, что μ_s — среднее число фотонов в отраженных от фазового модулятора зондирующих состояниях.

В качестве иллюстрации на рис. 3 приведены результаты расчетов длины секретного ключа в зависимости от длины линии связи для случая, когда существует побочный канал утечки, связанный с излучением аппаратуры передающей станции, и активное зондирование модулятора интенсивности. Как видно из рис. 3, увеличение вероятности различимости состояний побочного излучения, увеличение параметра p, приводит к уменьшению длины секретного ключа. Значение отношения $\frac{p^{max}(\mu)}{p^{min}(\mu)} = 1$ соответствует полной неразличимости отраженных состояний от модулятора интенсивности. Чем больше отношение $\frac{p^{max}(\mu)}{p^{min}(\mu)}$, тем больше вероятность подслушивателя отличить информационное состояние от состояний «ловушек», тем меньше длина секретного ключа, которую можно получить. Хотя зондирование модулятора интенсивности и не дает прямой информации о передаваемом бите ключа, тем не менее информация из данного побочного канала уменьшает длину секретного ключа.

На рис. 4 приведены результаты расчетов для длины секретного ключа как функции длины линии связи для случая всех побочных каналов утечки информации. Как видно из рис. 4, общая тенденция сводится к тому, что введение дополнительных побочных каналов утечки информации ведет к уменьшению длины секретного ключа.

15. ЗАКЛЮЧЕНИЕ

Системы квантовой криптографии являются физическими системами. Само квантовое распределение секретных ключей представляет собой распределенный физический эксперимент, который сводится к приготовлению и измерению квантовых со-

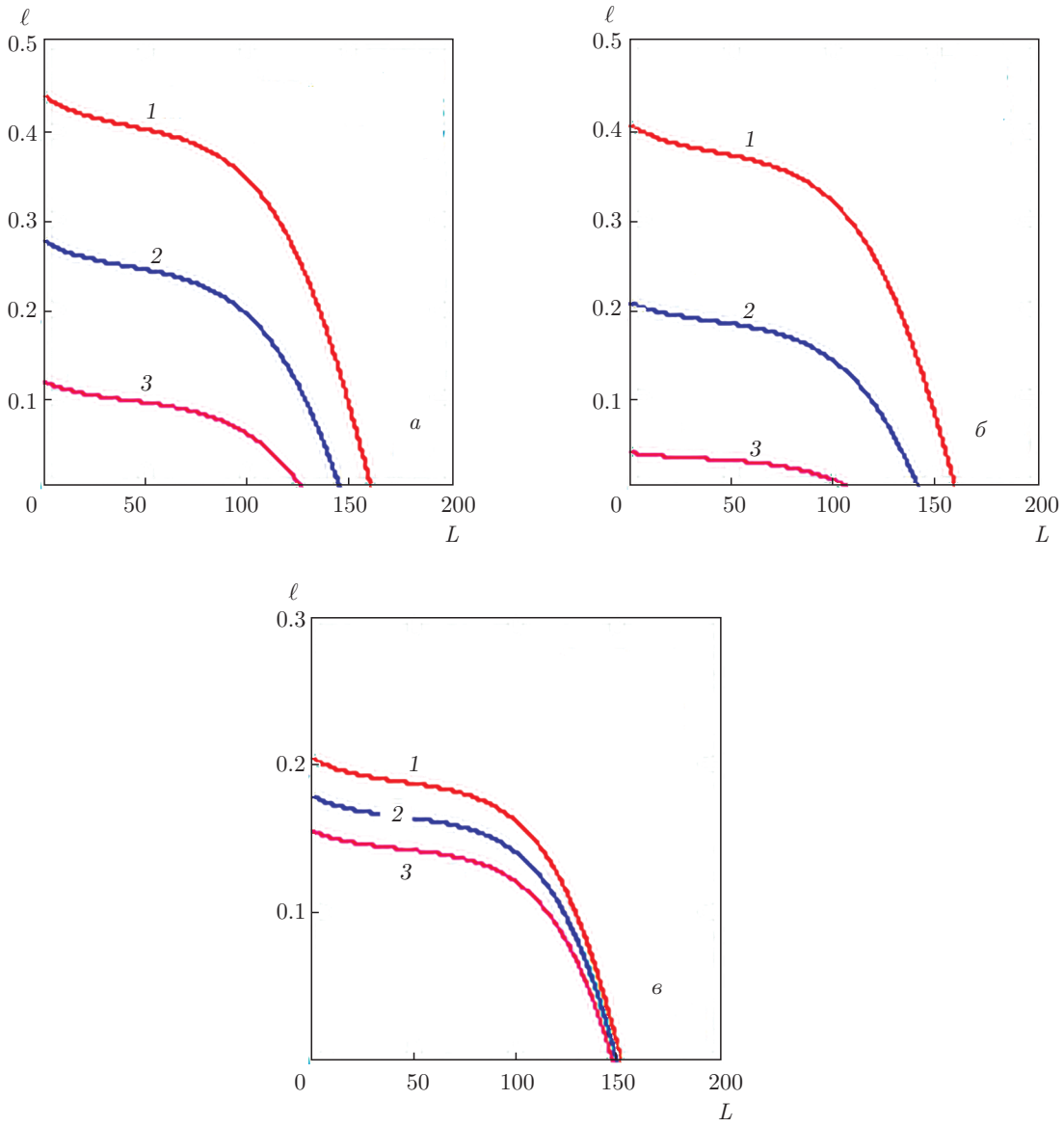

Рис. 4. Зависимости длины секретного ключа в пересчете на одну посылку от длины линии связи L для общего случая: детектирования побочного излучения передающей станции (параметр p — вероятность ошибки различения побочного излучения), активного зондирования фазового модулятора (параметр η — степень перекрытия отраженных зондирующих состояний), детектирования переизлучения от лавинных детекторов на приемной станции (параметр d — вероятность ошибки различения), активного зондирования модулятора интенсивности (вероятности различения $\frac{p^{max}(\mu)}{p^{min}(\mu)}$ отраженных состояний от модулятора интенсивности). Параметры p, d, η имеют следующие значения: *а*) $p = 0.5$, $d = 0.5$, $\eta = 0.999$, $\frac{p^{max}(\mu)}{p^{min}(\mu)} = 0.9$ (*1*), 0.8 (*2*), 0.7 (*3*); *б*) $p = 0.65$ (*1*), 0.75 (*2*), 0.85 (*3*), $d = 0.5$, $\eta = 0.999$; *в*) $p = 0.75$, $d = 0.5$, $\eta = 0.88$ (*1*), 0.85 (*2*), 0.82 (*3*), $\frac{p^{max}(\mu)}{p^{min}(\mu)} = 0.9$. Остальные значения параметров такие же, как на рис. 3

стояний. Как и в любом физическом эксперименте, невозможно целиком изолировать экспериментальную систему от окружающего мира. Любой аккуратный физический эксперимент по исследованию некоторого явления неизбежно включает мероприятия, которые минимизируют влияние нежелательных факторов, влияющих на «чистоту» исследуемого явления. Все сказанное в полной мере относится и к системам квантовой криптографии.

Такими нежелательными факторами в системах квантовой криптографии являются побочные каналы утечки информации. Утечка информации при атаках на квантовые состояния в квантовом канале связи учитывается энтропийными соотношениями неопределенности, которые связывают утечку информации из квантового канала с наблюдае-

мой ошибкой на приемной стороне. Нежелательными факторами, влияющими на «чистоту» квантового распределения ключей, являются утечки по побочным каналам — излучение аппаратуры при приготовлении и детектировании квантовых состояний, измерение отраженного зондирующего излучения от активных элементов системы (фазовых модуляторов и модуляторов интенсивности). Если известна, например, интенсивность и структура квантовых состояний в побочных каналах, то также можно указать верхнюю границу утечки информации, которую может получить подслушиватель при измерениях этих состояний. Данная верхняя граница информации, фактически, дается фундаментальной величиной Холево — информацией, которую может получить подслушиватель из ансамбля квантовых состояний в побочных каналах. Структура и интенсивность квантовых состояний в каждом побочном канале достигаются техническими средствами при реализации системы, например, экранированием передающей аппаратуры. Критические побочные каналы утечки информации известны и определяются конкретной физической реализацией системы. Поэтому правильное конструирование физической экспериментальной системы позволяет учесть утечку информации по побочным каналам и внести соответствующие поправки на длину секретного ключа, причем вычисление поправок также проводится на уровне фундаментальных ограничений квантовой теории на различимость квантовых состояний.

Таким образом, построены различные атаки на систему КРК с учетом побочных каналов утечки информации. Как упоминалось выше, в отличие от атак на однофотонные информационные квантовые состояния, при атаках с учетом побочных каналов, по-видимому, невозможно получить оценки длины секретного ключа без каких-то модельных предположений о структуре квантовых состояний в побочных каналах. Тем не менее, удается получить оценки в достаточно общих предположениях о структуре состояний в побочных каналах. Часто точная структура состояний не требуется, достаточно лишь знать степень перекрытия (степень различимости) данных состояний. При пассивном излучении аппаратуры приемной станции достаточно обойтись вероятностью ошибки p, если побочный канал моделируется дискретным двоичным квантовым каналом связи. В классической криптографии из-за большого числа степеней свободы системы для оценки утечки информации по такому каналу часто используется модель гауссовского канала с шумом. Приготовлению в аппаратуре состояния, отвечающего 0 или 1, отвечает сигнал побочного излучения мощностью P или $-P$ относительно некоторого опорного уровня. При этом данные уровни побочного сигнала могут быть измерены непосредственно вблизи аппаратуры. Вне аппаратуры подслушивателю доступен гауссовский сигнал, искаженный шумом мощностью P_{noise}. Такой гауссовский побочный канал может быть «конвертирован» в бинарный дискретный канал связи с вероятностью ошибки различения двух сигналов равной

$$p = 1-\Phi\left(\sqrt{\frac{P}{P_{noise}}}\right), \quad \Phi(x) = \frac{1}{\sqrt{2\pi}}\int\limits_{-\infty}^{x} e^{-z^2/2}dz.$$

Фактически для оценок длины ключа в формуле (89) нужно заменить значение p на приведенное выше, которое выражается через измеримый уровень мощности побочных сигналов. Побочный гауссовский канал также может быть включен в рассмотрение непосредственно.

Важно также отметить, что при тех или иных модельных предположениях о структуре побочного канала состояния в этом канале должны рассматриваться сразу как квантовые. Невозможно рассматривать информационные состояния как квантовые, а состояния в побочных каналах классическим образом, поскольку при таком подходе выпадают из рассмотрения коллективные измерения и совместные атаки на информационные состояния и состояния в побочных каналах. Параметры квантовых состояний в побочных каналах входят в утечку информации от информационных квантовых состояний.

Используемый метод может применяться не только для протокола BB84, но и для других протоколов.

Сделаем последнее замечание. Как было видно выше, стандартный Decoy State-метод неприменим при учете активного зондирования модулятора интенсивности, поскольку подслушиватель может с определенной вероятностью различать информационные состояния и состояния «ловушки». Кроме измерений отраженных от модулятора интенсивности состояний, которые различают состояния с разным числом фотонов, подслушиватель может делать измерения с определенным исходом (UM-измерения) над отраженными состояниями. Данные измерения дают достоверную информацию о типе состояния — информационное или «ловушка», но с вероятностью меньше единицы. Более того, совместные UM-измерения над информационным состоянием в квантовом канале и отраженным состоянием дают полную информацию о типе состояния и передаваемом би-

те ключа, но с вероятностью меньше единицы. Иначе говоря, в посылках, где произошел определенный исход совместных UM-измерений, подслушиватель знает передаваемый бит ключа и тип состояния. Остальные посылки с неопределенным исходом подслушиватель блокирует. Ситуация принципиально отличается, когда нет отраженных состояний, а UM-измерения проводятся только над информационными состояниями. В этом случае подслушиватель знает передаваемый бит ключа, но не знает, к какому типу состояния относится определенный исход измерения. Блокирование посылок, где был неопределенный исход измерения, нарушает статистику фотоотсчетов для состояний с разным средним числом фотонов, что детектируется стандартным Decoy State-методом.

При совместных UM-измерениях подслушиватель знает передаваемый бит и тип состояния, поэтому может перепосылать нужное число состояний из посылок с определенным исходом измерения, чтобы отсчеты на приемной стороне выглядели для всех состояний с разным числом фотонов, как отсчеты из квантового канала с большими потерями, но одинаковыми потерями для всех состояний, т. е. без изменения пуассоновской статистики для каждого типа состояний. Анализ данной атаки требует отдельного рассмотрения. Для детектирования такой атаки необходимо явно следить за изменением потерь в квантовом канале связи. То есть потери в канале связи становятся параметром протокола. Отметим, что в Decoy State-методе параметр потерь в явном виде не входит в протокол.

Благодарности. Автор выражает благодарность И. М. Арбекову, С. П. Кулику, К. А. Балыгину и А. Н. Климову за интересные и многочисленные обсуждения, а также коллегам по Академии криптографии Российской Федерации за обсуждения и поддержку.

Финансирование. Работа выполнена при поддержке Российского научного фонда (проект № 16-12-00015 (продолжение)).

ЛИТЕРАТУРА

1. W. K. Wooters and W. H. Zurek, Nature **299**, 802 (1982).
2. W. Heisenberg, Zeit. Phys. **43**, 172 (1927).
3. H. P. Robertson, Phys. Rev. **34**, 163 (1929).
4. D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).
5. H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
6. K. Kraus, Phys. Rev. D **35**, 3070 (1987).
7. M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).
8. C. H. Bennett and G. Brassard, in *Proc. of IEEE Int. Conf. on Comp. Sys. and Sign. Process.* (1984), pp. 175–179.
9. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
10. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
11. R. Renner, PhD thesis, ETH Zürich (2005), arXiv: 0512258.
12. J. M. Renes and J.-C. Boileau, Phys. Rev. Lett. **103**, 020402 (2009).
13. M. Tomamichel, Ch. Ci Wen Lim, N. Gisin, and R. Renner, arXiv:1103.4130 v2 (2011); Nature Commun. **3**, 1 (2012).
14. С. Н. Молотков, ЖЭТФ **153**, 895 (2018) [S. N. Molotkov, JETP **126**, 741 (2018)].
15. A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Opt. **48**, 2023 (2001).
16. N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
17. N. Jain, E. Anisimova, I. Khan, V. Makarov, Ch. Marquardt, and G. Leuchs, *Talk presented at the Central European Workshop on Quantum Optics*, Brussels, June 2327 (2014).
18. L. Lydersen, C. Wiechers, Ch. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photon. **4**, 686 (2011).
19. A. Vakhitov, V. Makarov, and Dag R. Hjelme, J. Mod. Opt. **48**, 2023 (2001).
20. V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).
21. K. A. Balygin, A. N. Klimov, I. B. Bobrov, K. S. Kravtsov, S. P. Kulik, and S. N. Molotkov, Laser Phys. Lett. **15**, 095203 (2018) .
22. K. A. Balygin, A. N. Klimov, I. B. Bobrov, K. S. Kravtsov, S. P. Kulik, and S. N. Molotkov, Laser Phys. Lett. **16**, 019402 (2019).
23. Won-Young Hwang, arXiv[quant-ph]:0211153.
24. Xiang-Bin Wang, Phys. Rev. Lett. **94**, 230503 (2005).

25. Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, Phys. Rev. Lett. **94**, 230504 (2005); Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo, arXiv[quant-ph]: 0503005.

26. K. Tamaki, M. Curty, and M. Lucamarini, New J. Phys. **18**, 065008 (2016).

27. W. Wang, K. Tamaki, and M. Curty, New J. Phys. **20**, 083027 (2018).

28. M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Phys. Rev. X **5**, 031030 (2015); arXiv:1506.01989.

29. S. W. Allison, G. T. Gillies, D. W. Magnuson, and T. S. Pagano, Appl. Opt. **24**, 1 (1985).

30. L. W. Tutt and T. F. Boggess, Progr. Quant. Electron. **17**, 299 (1993).

31. R. M. Wood, *Laser-Induced Damage of Optical Materials*, Taylor & Francis (2003).

32. C. E. Shannon, Bell System Techn. J. **XXVII**, 379 (1948).

33. A. S. Holevo, Russ. Math. Surveys **53**, 1295 (1998).

34. А. С. Холево, *Квантовые системы, каналы, информация*, МЦНМО, Москва (2010).