ЖЭТФ, 2021, том 160, вып. 3 (9), стр. 327–365

ПОБОЧНЫЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ В КВАНТОВОЙ КРИПТОГРАФИИ: НЕ СТРОГО ОДНОФОТОННЫЕ СОСТОЯНИЯ, РАЗНЫЕ КВАНТОВЫЕ ЭФФЕКТИВНОСТИ ДЕТЕКТОРОВ, КОНЕЧНЫЕ ПЕРЕДАВАЕМЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ

С. Н. Молотков*

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

Академия криптографии Российской Федерации
121552, Москва, Россия

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

Поступила в редакцию 20 апреля 2021 г.,
после переработки 20 апреля 2021 г.
Принята к публикации 25 апреля 2021 г.

Реализации систем квантовой криптографии существенно отличаются от идеализированных моделей, которые используются для доказательства секретности распределяемых ключей. Без учета неидеальностей реальных систем невозможно всерьез говорить о криптографической стойкости. Для практического использования систем квантовой криптографии необходимо учитывать все реальные факторы, влияющие на секретность распределяемых ключей. В работе предложен, по сути, аналитический метод, учитывающий нестрогую однофотонность информационных состояний, различные квантовые эффективности детекторов, флуктуации параметров за счет конечных передаваемых последовательностей, утечку информации через побочные каналы как при пассивном детектировании побочного излучения, так и при активном зондировании элементов системы. Состояния в побочных каналах могут иметь предельно низкую интенсивность, поэтому рассматриваются квантовым образом. Максимально возможная полная утечка информации к подслушивателю по всем каналам достигается на совместных коллективных измерениях как квантовых информационных состояний, так и квантовых состояний в побочных каналах. Метод применим при любом спектральном распределении числа фотонов в побочных каналах.

DOI: 10.31857/S0044451021090029

1. ВВЕДЕНИЕ

Квантовая криптография [1] — квантовое распределение ключей — один из разделов квантовых технологий, который доведен до практических применений. Квантовая криптография, по сути, является процедурой согласования двух независимых случайных последовательностей на передающей и приемной сторонах путем передачи и регистрации квантовых состояний через открытый квантовый канал связи. При этом квантовый канал связи доступен не только для прослушивания, но и для произвольных модификаций третьей нелегитимной стороной. Для согласования результатов измерений, коррекции ошибок в первичных ключах на приемной стороне и сжатия очищенных ключей используется вспомогательный классический открытый аутентичный канал связи.

Секретность ключей в квантовой криптографии базируется на фундаментальном свойстве квантовых состояний — вторжение в квантовый канал связи неизбежно приводит к возмущению передаваемых квантовых состояний и ошибкам измерений на приемной стороне.

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

Анализ криптостойкости квантовой криптографии прошел длинный путь. Первоначально рассматривались «идеальные» системы квантовой криптографии и отдельные атаки на передаваемые квантовые состояния. На первом этапе предполагалось, что квантовые состояния являются строго однофотонными, что не отвечает реальной ситуации.

В реальной ситуации в качестве информационных квантовых состояний используются сильно ослабленные когерентные состояния, которые являются квазиоднофотонными — имеют пуассоновскую статистику по числу фотонов, что приводит к возникновению новых атак, которые отсутствуют в случае строго однофотонных состояний.

Предполагалось, что передающая и приемная станции изолированы от внешнего мира, т. е. подслушиватель не имеет ни прямого, ни косвенного доступа к аппаратуре. В реальности системы квантовой криптографии являются открытыми системами в том смысле, что подслушиватель может иметь опосредованный доступ через линию связи к приемной и передающей аппаратуре. Кроме того, подслушиватель может детектировать побочное излучение самой аппаратуры [2, 3].

Для практического использования систем квантовой криптографии необходимо учитывать все реальные факторы, влияющие на секретность распределяемых ключей, а именно:

1) разную и неидеальную квантовую эффективность однофотонных детекторов;

2) нестрогую однофотонность информационных состояний;

3) побочные каналы утечки информации;

4) атаки активного зондирования;

5) конечную длину передаваемых последовательностей.

Доказательство секретности ключей должно учитывать все упомянутые выше факторы. До сих пор комплексный учет всех факторов, влияющих на секретность распределяемых ключей, не сделан.

В случае строго однофотонных информационных состояний и идеальных детекторов фундаментальные энтропийные соотношения неопределенностей позволяют связать утечку информации к подслушивателю с наблюдаемой ошибкой на приемной стороне. Энтропийные соотношения неопределенностей позволяют не перебирать и не строить явно всевозможные атаки, а выразить утечку только через наблюдаемую ошибку на приемной стороне. Данный метод применим также и для конечных передаваемых последовательностей [4, 5]. При этом считалось, что измерения на приемной стороне являются идеальными — детекторы имеют идеальную и одинаковую квантовую эффективность, что также не отвечает реальной ситуации. Метод не позволяет перенести доказательство на случай неидеальных детекторов с разными квантовыми эффективностями.

Обычно в системах квантовой криптографии используется пара детекторов. В одном из базисов отсчеты в одном детекторе D_1 отвечают за регистрацию 0, в другом детекторе D_2 — за регистрацию 1. В сопряженном базисе, наоборот, отсчеты в детекторе D_2 отвечают за регистрацию 0, в детекторе D_1 — за регистрацию 1. Базисы передающей и приемной сторон раскрываются через открытый аутентичный канал связи. Информация о том, в каком базисе была регистрация, известна подслушивателю.

Интуитивно ясно, что в случае, когда квантовая эффективность одного из детекторов стремится к нулю (отсчеты имеют место только в одном из детекторов), невозможно гарантировать секретность ключей. Базис подслушивателю известен, и срабатывает только один детектор. В такой ситуации подслушиватель знает весь ключ даже без вторжения в квантовый канал связи. При этом подслушиватель не производит ошибок на приемной стороне и не обнаруживается, а система квантовой криптографии оказывается несекретной.

Как видно из приведенного простого примера, учет различных квантовых эффективностей детекторов играет принципиальную роль в обеспечении секретности ключей в квантовой криптографии даже в случае строго однофотонных состояний. В этом направлении имеются лишь частичные результаты [6].

В рамках энтропийных соотношений неопределенностей также невозможно учесть утечку информации к подслушивателю по побочным каналам. Интуитивно данный факт имеет простое объяснение. Энтропийные соотношения неопределенностей связывают утечку информации с возмущением квантовых состояний — ошибкой на приемной стороне. Утечка информации по побочным каналам, например детектирование побочного излучения передающей и приемной аппаратуры, не приводит к возмущению подслушивателем информационных состояний и ошибкам на приемной стороне. По этой причине утечка информации по побочным каналам лежит за рамками энтропийных соотношений неопределенностей.

Неоднофотонность информационных состояний приводит к атаке с расщеплением по числу фотонов (PNS-атака, Photon Number Splitting). В канале с потерями, при уровне потерь больше некоторой кри-

тической величины, данная атака приводит к тому, что подслушиватель знает весь передаваемый ключ и не производит ошибок на приемной стороне — не детектируется. Для детектирования PNS-атаки используется Decoy State-метод. Данный метод в исходном виде перестает работать при атаках активного зондирования — атаках с зондированием модулятора интенсивности, и требует обобщения. Такое обобщение было сделано в работах [7, 8].

Анализ криптостойкости систем квантовой криптографии с полным учетом неидеальностей 1)–5) до сих пор не сделан.

Цель данной работы — учесть упомянутые выше неидеальности систем квантовой криптографии в доказательстве секретности ключей.

Логика доказательства будет состоять в следующем. Секретный ключ формируется из однофотонной компоненты информационных состояний, достигающей приемной стороны. Информация, содержащаяся в многофотонных компонентах состояний в пользу подслушивателя, считается ему известной и не фигурирует в секретном ключе. Оценка доли однофотонной компоненты проводится обобщенным Decoy State-методом. Учет побочных каналов утечки информации требует построения явной атаки на состояния в квантовом канале связи. Кроме того, учет разной и неидеальной квантовой эффективности детекторов также требует явного вида однофотонной компоненты информационных состояний. Состояния в побочных каналах также необходимо рассматривать квантовым образом. Неформально говоря, данные квантовые состояния «подцепляются» явно к однофотонной компоненте состояний.

Предложен также простой метод учета флуктуаций наблюдаемых параметров, которые имеют место при конечных длинах передаваемых последовательностей.

Ниже будем последовательно включать в рассмотрение неидеальности системы, чтобы продемонстрировать, как зависит оценка длины секретного ключа от каждого из факторов.

2. СЛЕДОВОЕ РАССТОЯНИЕ, СГЛАЖЕННЫЕ min- И max-ЭНТРОПИИ

Выше была описана на неформальном уровне причина секретности ключей, которая гарантируется фундаментальными законами Природы. На формальном уровне секретность ключей в квантовой криптографии выражается в довольно абстрактных терминах, и доказательства секретности являются «многоходовыми» [4]. Для самодостаточности изложения приведем определения величин, которые используются в доказательстве секретности.

Секретность ключей в квантовой криптографии дается в терминах следовой метрики — расстояния между двумя квантовыми состояниями, описывающими реальную ситуацию после квантового распределения ключей и идеальную ситуацию, когда ключи строго равновероятны и полностью некоррелированы с квантовыми состояниями подслушивателя.

Данный критерий вызывал споры даже среди специалистов [9, 10]. Абстрактность критерия секретности ключей на основе следовой метрики не содержит интуитивно прозрачных соображений, которые были выработаны применительно к использованию ключей в классической криптографии, например, таких как переборная сложность по поиску истинного ключа, число шифр-сообщений до их первого дешифрования при условии, что шифрование происходит на ключах, полученных в результате квантового распределения.

Явная связь следового критерия секретности ключей в квантовой криптографии с переборными критериями секретности в классической криптографии была установлена в работе [11].

В задачах квантовой криптографии после передачи и измерения квантовых состояний возникает матрица плотности ρ_{XE} Алиса–Ева, которая имеет классически-квантовую структуру. Алиса имеет в своем распоряжении случайную эталонную битовую строку, к которой Ева не имеет доступа. Ева имеет в своем распоряжении квантовое состояние, которое возникает из-за вторжения в квантовый канал связи. Матрица плотности имеет вид

$$\rho_{XE}^{(n)} = \sum_{x\in\{0,1\}^n} |x\rangle_X\langle x| \otimes \rho_E^x, \qquad |x\rangle_X = |x_1\rangle_X \otimes |x_2\rangle_X \otimes \ldots \otimes |x_n\rangle_X. \tag{1}$$

Удобно классической битовой строке x длиной n сопоставить регистр ортогональных квантовых состояний $|x\rangle_X$, отвечающих состоянию классического регистра с последовательностью битов $(x_1, x_2, \ldots, x_n)$, ρ_E^x — квантовое состояние Евы, коррелированное с битовой строкой Алисы.

Для дальнейшего потребуются сглаженные min- и max-квантовые энтропии, которые мажорируют следовое расстояние. По определению имеем (см. детали в [4])

$$H_{min}^{\varepsilon}(\rho_{XE}^{(n)}|\rho_E^{(n)}) = \sup_{\overline{\rho}_{XE}^{(n)}\in\mathcal{B}^{\varepsilon}(\rho_{XE}^{(n)})} H_{min}(\overline{\rho}_{XE}^{(n)}|\overline{\rho}_E^{(n)}), \tag{2}$$

$$H^{\varepsilon}_{max}(\rho^{(n)}_{XE}|\rho^{(n)}_{E}) = \inf_{\overline{\rho}^{(n)}_{XE}\in\mathcal{B}^{\varepsilon}(\rho^{(n)}_{XE})} H_{max}(\overline{\rho}^{(n)}_{XE}|\overline{\rho}^{(n)}_{E}), \quad (3)$$

далее, пусть λ — минимальное число, такое что

$$\lambda I_X \otimes \overline{\rho}^{(n)}_{E} - \overline{\rho}^{(n)}_{XE} \geq 0,$$

тогда по определению

$$H_{min}(\overline{\rho}^{(n)}_{XE}|\overline{\rho}^{(n)}_{E}) = -\log(\lambda), \quad (4)$$

где $\log \equiv \log_2$. Матрицы плотности, по которым определяются inf и sup, лежат внутри шара $\mathcal{B}^{\varepsilon}(\rho_{XE})$,

$$\mathrm{Tr}\{|\rho^{(n)}_{XE} - \overline{\rho}^{(n)}_{XE}|\} = ||\rho^{(n)}_{XE} - \overline{\rho}^{(n)}_{XE}||_1 \leq \varepsilon. \quad (5)$$

Для дальнейшего будет полезно эквивалентное определение, которое следует из (4):

$$H_{min}(\overline{\rho}^{(n)}_{XE}|\overline{\rho}^{(n)}_{E}) = -\log(\lambda_{max}((I_X \otimes (\overline{\rho}^{(n)}_{E})^{-1/2}) \times \times \overline{\rho}^{(n)}_{XE}(I_X \otimes (\overline{\rho}^{(n)}_{E})^{-1/2}))), \quad (6)$$

где

$$\lambda_{max}((I_X \otimes (\overline{\rho}^{(n)}_{E})^{-1/2})\overline{\rho}^{(n)}_{XE}(I_X \otimes (\overline{\rho}^{(n)}_{E})^{-1/2}))$$

— максимальное собственное число оператора в скобках (6). Далее

$$H_{max}(\overline{\rho}^{(n)}_{XE}|\overline{\rho}^{(n)}_{E}) = \log(\mathrm{Tr}\{I_X \otimes \overline{\rho}^{(n)}_{E}\mathcal{P}(\overline{\rho}^{(n)}_{XE})\}), \quad (7)$$

где $\mathcal{P}(\overline{\rho}^{(n)}_{XE})$ — проектор на носитель матрицы плотности $\overline{\rho}^{(n)}_{XE}$.

Данные определения предполагают минимизацию/максимизацию по матрицам плотности, лежащим в некоторой области пространства состояний. При конкретных практических вычислениях такая минимизация/максимизация вряд ли возможна. Кроме того, данные определения предполагают, что матрица плотности $\rho^{(n)}_{XE}$ (центр шара) известна точно. В реальной ситуации матрица плотности $\rho^{(n)}_{XE}$ точно не известна по двум причинам. Первая — передаваемые последовательности имеют конечную длину, поэтому можно получить лишь оценку самой $\rho^{(n)}_{XE}$. Вторая причина состоит в том, что даже если матрица плотности всей последовательности точно известна и имеет структуру тензорного произведения, $\rho^{(n)}_{XE} = \rho^{\otimes n}_{XE}$, то вычислить сглаженные энтропии точно не удается, можно лишь получить верхнюю/нижнюю оценку для сглаженных энтропий.

По этим причинам приходится делать двойное усечение матрицы плотности — вычисление сглаженных энтропий в два этапа (см. подробности ниже). На первом этапе оценивается матрица плотности $\rho^{(n)}_{XE}$ — центр шара. На втором этапе получается верхняя/нижняя оценка для сглаженных энтропий.

3. СЛЕДОВОЕ РАССТОЯНИЕ И КРИТЕРИЙ СЕКРЕТНОСТИ КЛЮЧЕЙ

Секретность ключей в квантовой криптографии формулируется в терминах следового расстояния [4]. После передачи и регистрации квантовых состояний, но до коррекции ошибок у Боба, квантовое состояние Алиса–Ева описывается матрицей плотности $\rho^{(n)}_{XE}$ (1), которая содержит корреляции между эталонной битовой строкой Алисы и квантовой системой Евы. После коррекции ошибок через открытый аутентичный канал связи Ева получает дополнительную информацию о битовой строке Алисы. При коррекции ошибок через открытый канал между Алисой и Бобом передается множество битовых строк $\mathcal{C}$.

После коррекции ошибок Алиса и Боб проводят усиление секретности очищенного ключа при помощи универсальных хеш-функций второго порядка, которое сводится к сжатию очищенной битовой строки $f : x = \{0,1\}^n \to \ell = \{0,1\}^{\ell}$. Хеш-функция сама является случайной величиной, которая равновероятно выбирается из множества хеш-функций $\mathcal{F}$. Выбор хеш-функции проводится через открытый канал связи и известен Еве.

Универсальные хеш-функции второго порядка обладают свойством [12]

$$\Pr_{f\in\mathcal{F}}\{f(x) = f(x')\} < \frac{1}{2^{\ell}} \quad \forall \quad x \neq x'. \quad (8)$$

После усиления секретности матрица плотности Алиса–Ева и матрица плотности Евы, коррелированная с битовой строкой x, переходит в новую матрицу плотности $\rho^{(n)}_{XE} \to \rho^{(\ell)}_{\mathcal{F}(X)\mathcal{F}(E)}$.

После сжатия следовое расстояние мажорируется условной min-энтропией (см. детали в [4]):

$$||\rho^{(\ell)}_{\mathcal{F}(X)\mathcal{F}(E)} - \rho_{\mathcal{F}(U_X)} \otimes \rho^{(\ell)}_{\mathcal{F}(E)}||_1 < < 2^{-(1/2)(H_{min}(\rho^{(n)}_{XEC}|\rho^{(n)}_{EC})-\ell)} = = 2^{-(1/2)(H_{min}(\rho^{(n)}_{XE}|\rho^{(n)}_{E})-\log|\mathcal{C}|-\ell)}. \quad (9)$$

Отметим, что в правой части (9) фигурируют матрицы плотности после передачи и регистрации квантовых состояний в согласованных базисах, но до усиления секретности и коррекции ошибок. В (9), (11) $U = \mathcal{F}(U_X)$, $\mathcal{C}$ — множество битовых строк (синдрома ошибок и др.), передаваемых через открытый канал между Алисой и Бобом при коррекции ошибок, $\log|\mathcal{C}|$ — количество информации в битах, содержащееся в этих строках,

$$\log|\mathcal{C}| = \mathrm{leak}. \quad (10)$$

Далее, $\rho_{\mathcal{F}(X)\mathcal{F}(E)}$ — матрица плотности после сжатия битовой строки $f : x = \{0,1\}^n \to \ell = \{0,1\}^\ell$,

$$\rho_{U_X} = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} |x\rangle_{X\,X}\langle x|,$$
$$\rho_U = \frac{1}{2^\ell} \sum_{x\in\{0,1\}^\ell} |x\rangle_{X\,X}\langle x|, \qquad (11)$$
$$\rho^{(\ell)}_{\mathcal{F}(E)} = \mathrm{Tr}_{\mathcal{F}(X)}\{\rho^{(\ell)}_{\mathcal{F}(X)\mathcal{F}(E)}\}.$$

Матрица плотности $\rho^{(\ell)}_{\mathcal{F}(X)\mathcal{F}(E)}$ описывает реальную ситуацию после усиления секретности — остаточные корреляции между новой битовой строкой Алисы и новой квантовой системой Евы.

Матрица плотности $\rho_{\mathcal{F}(U_X)} \otimes \rho^{(\ell)}_{\mathcal{F}(E)}$ описывает идеальную ситуацию, когда ключи равновероятно распределены и никак не коррелированы с квантовыми состояниями Евы $\rho^{(\ell)}_{\mathcal{F}(E)}$.

4. ПЕРЕХОД К min-ЭНТРОПИИ

По «техническим математическим» причинам удобно перейти от условной min-энтропии в (9) к сглаженной условной min-энтропии. Почему возникает min-энтропия?

Умозрительно можно было бы вычислить условную min-энтропию в (2)–(4), (9), если матрица плотности $\rho^{(n)}_{XE}$ в (2)–(4) была бы точно известна и ее можно было бы вычислить. Однако это невозможно. В лучшем случае можно получить оценку матрицы плотности. Определения (2)–(7) с математической точки зрения очень удобны при доказательстве различных неравенств. Однако при практических вычислениях ими невозможно напрямую воспользоваться.

Пусть матрица плотности $\rho^{(n)}_{XE}$ лежит в шаре $\rho^{(n)}_{XE} \in \mathcal{B}_\varepsilon(\rho^{(n)}_{XE})$, тогда

$$\begin{aligned}
||\rho^{(\ell)}_{\mathcal{F}(X)\mathcal{F}(E)} - \rho^{(\ell)}_{\mathcal{F}(U_X)} \otimes \rho^{(\ell)}_{\mathcal{F}(E)}||_1 \le \\
\le ||\rho^{(\ell)}_{\mathcal{F}(X)\mathcal{F}(E)} - \overline{\rho}^{(\ell)}_{\mathcal{F}(X)\mathcal{F}(E)}||_1 + \\
+ ||\overline{\rho}^{(\ell)}_{\mathcal{F}(X)\mathcal{F}(E)} - \overline{\rho}_U \otimes \rho^{(\ell)}_{\mathcal{F}(E)}||_1 + ||\overline{\rho}^{(\ell)}_{\mathcal{F}(E)} - \rho^{(\ell)}_{\mathcal{F}(E)}||_1 \le \\
\le 2\varepsilon + 2^{-(1/2)(H_{min}(\rho^{(n)}_{XE}|\rho^{(n)}_E) - \log|\mathcal{C}| - \ell)} \le \\
\le 2\varepsilon + 2^{-(1/2)(H^\varepsilon_{min}(\rho^{(n)}_{XE}|\rho^{(n)}_E) - \log|\mathcal{C}| - \ell)}. \qquad (12)
\end{aligned}$$

В (12) дважды использовано неравенство треугольника для следового расстояния, а также тот факт, что следовое расстояние не возрастает при взятии частичного следа. Последнее неравенство следует из определения (2) условной min-энтропии.

Напомним, что в правую часть (12) входит матрица плотности до стадии усиления секретности.

Если величина сжатия (длина секретного ключа ℓ) выбрана такой, что

$$2\varepsilon + 2^{-(1/2)(H^\varepsilon_{min}(\rho^{(n)}_{XE}|\rho^{(n)}_E) - \log|\mathcal{C}| - \ell)} \le \varepsilon', \qquad (13)$$

то ключ называется ε'-секретным в смысле следового расстояния (9), (12). После усиления секретности следовое расстояние оказывается меньше ε' — параметра секретности ключей, который выбирается легитимными пользователями и достигается соответствующим сжатием (выбором хеш-функций) очищенных ключей.

Таким образом, доказательство секретности сводится к вычислению условной сглаженной min-энтропии после передачи и измерения квантовых состояний до коррекции ошибок и усиления секретности.

Для конструктивного вычисления сглаженной min-энтропии требуется получить оценку для матрицы плотности $\rho^{(n)}_{XE}$ — центра шара.

5. КВАНТОВАЯ КРИПТОГРАФИЯ КАК РАСПРЕДЕЛЕННЫЙ СТАТИСТИЧЕСКИЙ ЭКСПЕРИМЕНТ СО ЗЛОУМЫШЛЕННИКОМ

Квантовое распределение ключей представляет собой статистический эксперимент в следующем смысле. Легитимные пользователи Алиса и Боб связаны между собой через «черный ящик» — квантовый канал связи, в который вторгается Ева. Алиса контролирует информационные состояния на входе, Боб на приемной стороне видит результаты измерений при условии, что были посланы конкретные квантовые состояния. Это осуществляется на стадии оценки параметров путем раскрытия части передаваемой последовательности.

Целью этой стадии протокола является оценка частичной матрицы плотности $\rho^{(n)}_{XE} = \mathrm{Tr}_B\{\rho^{(n)}_{XBE}\}$ при условии, что Боб получает результаты измерений на частичной матрице плотности $\rho^{(n)}_{XB} = \mathrm{Tr}_E\{\rho^{(n)}_{XBE}\}$.

Если бы матрица плотности $\rho^{(n)}_{XE}$ была бы точно известна, то задача вычисления длины секретного ключа сводилась бы к вычислению $H_{min}(\rho^{(n)}_{XE}|\rho^{(n)}_E)$ в (2).

В реальной ситуации матрица плотности $\rho^{(n)}_{XE}$ точно не известна. Вопрос об оценке матрицы плот-

ности должен решаться в терминах теории вероятностей и математической статистики. Матрица плотности Алиса–Ева зависит от действий Евы — от параметров (ошибки на приемной стороне, доли однофотонной компоненты и пр.), которые управляются Евой и которые в явном виде недоступны легитимным пользователям. Легитимные пользователи имеют косвенную информацию об этих параметрах из результатов измерений. Точнее говоря, они имеют лишь оценку параметров (например, оценку вероятности ошибки), которая зависит от длины последовательности и истинной вероятности ошибки.

Обозначим набор параметров, от которых зависит матрица плотности, как $\{\mathcal{Q}\}$. Данные параметры известны Еве точно, поскольку ей и определяются. Для легитимных пользователей данные параметры «скрыты».

Ниже увидим, что имеются два типа скрытых параметров: 1) наблюдаемые скрытые параметры, которые могут быть определены из измерений на приемной стороне Боба, иначе говоря, вероятности фотоотсчетов на приемной стороне напрямую зависят от данных параметров; 2) ненаблюдаемые скрытые параметры, от которых не зависят вероятности результатов измерений на приемной стороне, но от них зависит утечка информации к подслушивателю.

Нет другого способа, кроме как рассматривать скрытый набор параметров для легитимных пользователей как случайные величины, которые имеют свое распределение вероятностей, определяемое Евой, но явно неизвестное легитимным пользователям. В этом смысле квантовое распределение ключей представляет собой статистический эксперимент, когда истинное совместное распределение параметров и величин легитимных пользователей неизвестно, но требуется получить оценку данного совместного распределения (оценку совместной матрицы плотности) по маргинальному распределению (частичной матрице плотности). Оценка частичной матрицы плотности в реальной ситуации должна быть получена по конечному, а не асимптотическому (бесконечному) набору наблюдаемых данных.

Сказанное означает, что недоступные параметры должны рассматриваться легитимными пользователями как случайные величины, которые подчиняются некоторому, также неизвестному для них, распределению вероятностей. Данные параметры должны быть включены в матрицу плотности, которая может быть записана в виде

$$\rho_{XEQ}^{(n)} = \sum_{x\in(\mathcal{X})} P_X(x)|x\rangle_X\langle x| \otimes \sum_{Q\in\mathcal{Q}} P_Q(Q)|Q\rangle\langle Q| \otimes \rho_{E|Q}^{x(n)} = \sum_{x\in(\mathcal{X})} P_X(x)|x\rangle_X\langle x| \otimes \rho_{EQ}^{x(n)}, \quad (14)$$

здесь $P_X(x)$ — вероятность распределения битовых строк у Алисы,

$$\sum_{x\in(\mathcal{X})} P_X(x) = 1. \quad (15)$$

В (14) введено обозначение

$$\rho_{EQ}^{x(n)} = \sum_{Q\in\mathcal{Q}} P_Q(Q)|Q\rangle\langle Q| \otimes \rho_{XE|Q}^{x(n)}, \qquad \mathrm{Tr}_E\{\rho_{E|Q}^{x(n)}\} = 1. \quad (16)$$

Каждому набору параметров Q удобно сопоставить соответствующие ортогональные (различимые) квантовые состояния $|Q\rangle_Q$. Набор параметров Q имеет распределение вероятностей $P_Q(Q)$, которое известно Еве, более того, Еве известен в каждом акте распределения ключей сам набор параметров. Неформально ситуацию можно интерпретировать следующим образом. Ева «случайно генерирует» в соответствии с распределением $P_Q(Q)$ набор параметров атаки Q. После «генерации» параметры самой Еве точно известны, но не известны Алисе и Бобу. В результате атаки Ева имеет условную матрицу плотности $\rho_{E|Q}^{x(n)}$, зависящую от атаки, которая параметризуется набором сгенерированных параметров.

Матрица плотности параметров и функция распределения параметров имеют вид

$$\rho_Q(\mathcal{Q}) = P_Q(Q)|Q\rangle_{QQ}\langle Q|, \quad \sum_{Q\in\mathcal{Q}} P_Q(Q) = 1. \quad (17)$$

Поскольку сами параметры и их распределение Алисе неизвестны, статистический ансамбль по всевозможным наборам параметров дается матрицей плотности Алиса–Ева:

$$\rho_{XE}^{(n)} = \sum_{Q\in\mathcal{Q}} P_Q(Q)\rho_{XE|Q}^{(n)}, \qquad \rho_{XE|Q}^{(n)} = \sum_{x\in(\mathcal{X})} P_X(x)|x\rangle_X\langle x| \otimes \rho_{E|Q}^{x(n)}. \quad (18)$$

Набор скрытых от легитимных пользователей параметров параметризует атаку Евы и определяет вероятности результатов измерений на приемной стороне Боба. Например, таким параметром в строго

однофотонном случае и при идеальных детекторах является один параметр Q — вероятность ошибочных отсчетов на приемной стороне.

По этой причине, если имеется оценка параметра Q по результатам измерений, то можно оценить матрицу плотности $\rho_{XE|Q}^{x(n)}$, которая приводит к таким результатам измерений. Более точно, попадание параметров в доверительный интервал с определенной вероятностью позволяет оценить следовое расстояние.

Разобьем все множество параметров на две области:

$$\rho_{XE}^{(n)} = \sum_{Q\in\delta_Q} P_Q(Q)\rho_{XE|Q}^{(n)} + \sum_{Q\notin\delta_Q} P_Q(Q)\rho_{XE|Q}^{(n)}, \quad (19)$$

где

$$\mathrm{Tr}_{XE}\{\rho_{XE|Q}^{(n)}\} = 1. \quad (20)$$

Введем символические обозначения

$$Q\in\delta_Q = Q\in\delta\mathcal{Q}, \quad Q\notin\delta_Q = Q\notin\delta\mathcal{Q}, \quad (21)$$

параметры попадают в доверительнный интервал или лежат вне его. Далее, используя (14)–(21), получаем

$$\begin{aligned}\rho_{XE}^{(n)} = \Pr\{Q\in\delta_Q\}\sum_{Q\in\delta_Q}\frac{P_Q(Q)\rho_{XE|Q}^{(n)}}{\Pr\{Q\in\delta_Q\}} + \\ + \Pr\{Q\notin\delta_Q\}\sum_{Q\notin\delta_Q}\frac{P_Q(Q)\rho_{XE|Q}^{(n)}}{\Pr\{Q\notin\delta_Q\}} = \\ = \Pr\{Q\in\delta_Q\}\rho_{XE|Q\in\delta_Q}^{(n)} + \\ + \Pr\{Q\notin\delta_Q\}\rho_{XE|Q\notin\delta_Q}^{(n)}, \quad (22)\end{aligned}$$

где

$$\begin{aligned}\Pr\{Q\in\delta_Q\} = \sum_{Q\in\delta_Q} P_Q(Q), \\ \Pr\{Q\notin\delta_Q\} = \sum_{Q\notin\delta_Q} P_Q(Q).\end{aligned} \quad (23)$$

При этом условные матрицы плотности в (22) нормированы:

$$\mathrm{Tr}_{XE}\{\rho_{XE|Q\in\delta_Q}^{(n)}\} = 1, \quad \mathrm{Tr}_{XE}\{\rho_{XE|Q\notin\delta_Q}^{(n)}\} = 1. \quad (24)$$

6. ДВОЙНОЕ УСЕЧЕНИЕ МАТРИЦ ПЛОТНОСТИ

Матрица плотности $\rho_{XE}^{(n)}$ является истинной и зависит от скрытых параметров. В дальнейшем придется иметь дело с усеченными матрицами плотности, которые близки к истинной матрице плотности в смысле следового расстояния. Усечение матриц плотности приходится делать дважды.

Введем события.

Первое событие Ω_1 — параметры матрицы плотности попадают в доверительный интервал (23). Второе событие Ω_2 — собственные числа матрицы плотности попадают в типичное множество последовательностей при условии, что ее параметры уже лежат в доверительном интервале (23). Совместная вероятность двух событий есть

$$\Pr\{\Omega_1\cap\Omega_2\} = \Pr\{\Omega_2|\Omega_1\}\Pr\{\Omega_1\}, \quad (25)$$

здесь $\Pr\{\Omega_2|\Omega_1\}$ — условная вероятность того, что матрица плотности попадает в типичное пространство при условии, что параметры матрицы плотности лежат в доверительном интервале.

6.1. Первое усечение матриц плотности

Пусть событие Ω_1 такое, что параметры попадают в доверительный интервал, пусть вероятность данного события

$$\Pr\{\Omega_1\} = \Pr\{Q\in\delta_Q\} > 1-\varepsilon_1. \quad (26)$$

Матрица плотности после первого усечения истинной матрицы плотности, с учетом (18), (19), имеет вид

$$\overline{\rho}_{XE}^{(n)} = \sum_{Q\in\delta_Q} P_Q(Q)\rho_{XE|Q}^{(n)}. \quad (27)$$

Усеченная матрица плотности $\overline{\rho}_{XE}^{(n)}$ является ε_1-близкой в смысле следового расстояния к истинной матрице плотности $\rho_{XE}^{(n)}$. Действительно,

$$\begin{aligned}||\rho_{XE}^{(n)} - \overline{\rho}_{XE}^{(n)}||_1 = ||\sum_{Q\notin\delta_Q} P_Q(Q)\rho_{XE|Q}^{(n)}||_1 \le \\ \le \sum_{Q\notin\delta_Q} P_Q(Q)||\rho_{XE|Q}^{(n)}||_1 \le \sum_{Q\notin\delta_Q} P_Q(Q) \le \varepsilon_1. \quad (28)\end{aligned}$$

В (28) использовано неравенство треугольника для следового расстояния.

Тот факт, что параметры усеченной матрицы плотности (событие Ω_1) лежат в доверительном интервале с вероятностью

$$\Pr\{\Omega_1\} = \Pr\{Q\in\delta_Q\} > 1-\varepsilon_1,$$

гарантирует, что наблюдаемые параметры на приемной стороне (например, ошибка Q) также лежат в доверительном интервале с той же вероятностью.

6.2. Второе усечение матриц плотности

Второе усечение матрицы плотности $\overline{\rho}_{XE}^{(n)}$ в (27), в отличие от первого усечения, связано, скорее, с техническими вычислительными причинами, чем с принципиальными причинами, диктуемыми статистикой.

Пусть параметры матрицы плотности уже лежат в доверительном интервале.

При вычислении min-энтропии необходимо выбирать значения параметров на нужной границе (правой или левой) доверительного интервала, которые в пользу подслушивателя приводят к минимальному значению условной min-энтропии. Минимальное значение условной min-энтропии для параметров на нужной границе доверительного интервала означает (в пользу подслушивателя) выбор минимальной нехватки информации подслушивателя о битовой строке Алисы.

Обозначим символически это значение как Q_{max}.

Обсудим теперь технические подробности вычисления min-энтропии на усеченной матрице плотности $\overline{\rho}_{XE}^{(n)}$.

Реально вычислить сглаженную энтропию можно, если матрица плотности имеет структуру тензорного произведения $\overline{\rho}_{XE|Q}^{(n)} = \overline{\rho}_{XE|Q}^{\otimes n}$. Второе усечение связано с тем, что даже, если матрица плотности имеет структуру тензорного произведения, то для конечной последовательности большой длины и при заданном значении параметров Q_{max} не удается точно вычислить условную сглаженную min-энтропию. Можно лишь получить оценку верхней границы для нее.

Матрица плотности после второго усечения $\hat{\rho}_{XE|Q_{max}}^{\otimes n}$ это матрица плотности, полученная из $\overline{\rho}_{XE|Q_{max}}^{\otimes n}$ оставлением только тех слагаемых, чьи собственные числа реализуются с вероятностью не менее $1-\varepsilon_2$ — попадают в множество ε_2-типичных последовательностей,

$$\Omega_2 = \left\{ \lambda \left(\left(I_X \otimes \left(\overline{\rho}_{E|Q_{max}}^{\otimes n} \right)^{-1/2} \right) \times \right.\right.$$

$$\left.\left. \times \ \overline{\rho}_{XE|Q_{max}}^{\otimes n} \left(I_X \otimes \left(\overline{\rho}_{E|Q_{max}}^{\otimes n} \right)^{-1/2} \right) \right) \in \mathrm{Typ}_{\varepsilon_2} \right\}, \quad (29)$$

при условии, что параметры уже лежат в доверительном интервале.

Вероятность попадания собственных чисел в множество ε_2-типичных последовательностей

$$\Pr\{\Omega_2|\Omega_1\} \geq 1-\varepsilon_2. \quad (30)$$

В итоге вероятность события, при котором параметры лежат в доверительном интервале и собственные числа попадают в множество ε_2-типичных последовательностей, равна

$$\Pr\{\Omega_1 \cap \Omega_2\} \geq (1-\varepsilon_1)(1-\varepsilon_2) \geq 1-\varepsilon_1-\varepsilon_2. \quad (31)$$

Матрица плотности $\hat{\rho}_{XE}^{\otimes n}$ после двойного усечения является $\varepsilon_1+\varepsilon_2$-близкой, в смысле следового расстояния, к истинной матрице плотности:

$$||\rho_{XE}^{\otimes n} - \hat{\rho}_{XE}^{\otimes n}||_1 = ||\rho_{XE}^{\otimes n} - \sum_{Q\in\delta} P_Q(Q)\rho_{XE|Q}^{\otimes n} +$$

$$+ \sum_{Q\in\delta} P_Q(Q)(\rho_{XE|Q}^{\otimes n} - \hat{\rho}_{XE|Q}^{\otimes n})||_1 \leq$$

$$\leq \varepsilon_1 + \sum_{Q\in\delta} P_Q(Q)||\rho_{XE|Q}^{\otimes n} - \hat{\rho}_{XE|Q}^{\otimes n}||_1 \leq$$

$$\leq \varepsilon_1 + (1-\varepsilon_1)\varepsilon_2 \leq \varepsilon_1+\varepsilon_2, \quad (32)$$

здесь $\hat{\rho}_{XE|Q}^{\otimes n}$ — усеченная матрица плотности ($Q\in\delta$), которая отличается от не усеченной $\overline{\rho}_{XE|Q}^{\otimes n}$ тем, что в ней присутствуют слагаемые с собственными числами, которые попадают в ε_2-типичное множество (см. следующий раздел).

6.3. Иллюстративный пример вычисления условной сглаженной min-энтропии

Для интуитивного подкрепления сказанного в предыдущем разделе приведем краткое эвристическое вычисление условной энтропии на усеченной матрице плотности. Более аккуратный вывод см. в [4]. Результат вычислений, естественно, будет одинаковым при нашем выводе и точном выводе [4]. При вычислении воспользуемся определением (6). Приведем матрицу плотности $\rho_{XE|Q_{max}}$ к диагональному виду, имеем

$$(\rho_{XE|Q_{max}})^{\otimes n} = \left(\sum_i \Lambda_i |\Lambda_i\rangle\langle\Lambda_i| \right)^{\otimes n} =$$

$$= \sum_{i_1}\sum_{i_2}\dots\sum_{i_n} \Lambda_{i_1}\Lambda_{i_2}\dots\Lambda_{i_n} |\Lambda_{i_1}\rangle\langle\Lambda_{i_1}| \otimes$$

$$\otimes |\Lambda_{i_2}\rangle\langle\Lambda_{i_2}| \otimes \dots |\Lambda_{i_n}\rangle\langle\Lambda_{i_n}|, \quad (33)$$

здесь Λ_i — собственные числа, $|\Lambda_i\rangle$ — собственные векторы, отвечающие собственным числам, матрицы плотности $\rho_{XE|Q_{max}}$.

Усеченная матрица плотности содержит слагаемые, которые попадают в множество ε_2-типичных последовательностей. Это такие последовательности, вероятности которых удовлетворяют неравенствам

$$P(i_1, i_2, \dots, i_n) = \Lambda_{i_1}\Lambda_{i_2}\dots\Lambda_{i_n}, \quad (34)$$

$$2^{-n(H(\rho_{XE|Q_{max}})+\delta(\varepsilon_2))} \le P(i_1, i_2, \ldots, i_n) \le$$
$$\le 2^{-n(H(\rho_{XE|Q_{max}})-\delta(\varepsilon_2))}. \quad (35)$$

Аналогично предыдущему приведем к диагональному виду матрицу плотности $\rho_{E|Q_{max}}$, находим

$$(\rho_{E|Q_{max}})^{\otimes n} = \left(\sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i|\right)^{\otimes n} =$$
$$= \sum_{i_1}\sum_{i_2}\ldots\sum_{i_n} \lambda_{i_1}\lambda_{i_2}\ldots\lambda_{i_n} |\lambda_{i_1}\rangle \times$$
$$\times \langle\lambda_{i_1}| \otimes |\lambda_{i_2}\rangle\langle\lambda_{i_2}| \otimes \ldots |\lambda_{i_n}\rangle\langle\lambda_{i_n}|, \quad (36)$$

где λ_i — собственные числа, $|\lambda_i\rangle$ — отвечающие им собственные векторы матрицы плотности $\rho_{E|Q_{max}}$. Усеченная матрица плотности содержит слагаемые, вероятности которых попадают в множество ε_2-типичных последовательностей. Это такие слагаемые, вероятности которых удовлетворяют условиям

$$p(i_1, i_2, \ldots, i_n) = \lambda_{i_1}\lambda_{i_2}\ldots\lambda_{i_n}, \quad (37)$$

$$2^{-n(H(\rho_{E|Q_{max}})+\delta(\varepsilon_2))} \le p(i_1, i_2, \ldots, i_n) \le$$
$$\le 2^{-n(H(\rho_{E|Q_{max}})-\delta(\varepsilon_2))}. \quad (38)$$

Оценка вероятности $\Pr\{\Omega_2|\Omega_1\}$ того, что собственные числа лежат в интервале при условии, что параметры атаки Евы $\mathcal{Q}$ лежат в доверительном интервале, есть

$$2^{-n(H(\rho_{XE|Q_{max}}|\rho_{E|Q_{max}})+\delta(\varepsilon_2))} \le$$
$$\le \lambda\left(\left(I_X \otimes \left(\rho_{E|Q_{max}}^{\otimes n}\right)^{-1/2}\right) \times\right.$$
$$\left.\times\ \rho_{XE|Q_{max}}^{\otimes n}\left(I_X \otimes \left(\rho_{E|Q_{max}}^{\otimes n}\right)^{-1/2}\right)\right) =$$
$$= \frac{P(i_1, i_2, \ldots, i_n)}{p(i_1, i_2, \ldots, i_n)} \le$$
$$\le 2^{-n(H(\rho_{XE|Q_{max}}|\rho_{E|Q_{max}})-\delta(\varepsilon_2))}, \quad (39)$$

где собственные числа лежат в множестве $\mathrm{Typ}_{\varepsilon_2}$ (29).

Вычисление min-энтропии через максимальное собственное число матрицы плотности после второго усечения, с учетом (6) и (29), дает

$$H_{min}^{\varepsilon_1+\varepsilon_2}(\rho_{XE|Q\in\delta_Q}^{(n)}|\rho_{E|Q\in\delta_Q}^{(n)}) \ge$$
$$\ge H_{min}^{\varepsilon_1+\varepsilon_2}(\rho_{XE|Q_{max}}^{(n)}|\rho_{E|Q_{max}}^{(n)}). \quad (40)$$

Смысл данного неравенства интуитивно понятен. Неформально, условная энтропия есть нехватка информации Евы о битовой строке Алисы при условии, что ошибка на приемной стороне из-за вторжения в квантовый канал есть Q_{max}. Соответственно, чем меньше ошибка, тем больше нехватка информации Евы.

С учетом (6), (29) получаем

$$H_{min}^{\varepsilon_1+\varepsilon_2}(\rho_{XE|Q_{max}}^{(n)}|\rho_{E|Q_{max}}^{(n)}) =$$
$$= -\log\left(\lambda\left(\left(I_X \otimes \left(\rho_{E|Q_{max}}^{\otimes n}\right)^{-1/2}\right) \times\right.\right.$$
$$\left.\left.\times\ \rho_{XE|Q_{max}}^{\otimes n}\left(I_X \otimes \left(\rho_{E|Q_{max}}^{\otimes n}\right)^{-1/2}\right)\right)\right) =$$
$$= n(H(\rho_{XE|Q_{max}}|\rho_{E|Q_{max}}) - \delta(\varepsilon_2)), \quad (41)$$

здесь $H(\rho) = -\mathrm{Tr}\{\rho\log(\rho)\}$ — энтропия фон Неймана. Таким образом, вычисление условной сглаженной min-энтропии при неизвестных скрытых параметрах сводится к вычислению условной (не сглаженной) энтропии для параметров — вероятности ошибки Q, лежащей на правой границе доверительного интервала $Q = Q_{max}$.

7. ПОСТРОЕНИЕ ЯВНОЙ АТАКИ НА ОДНОФОТОННУЮ КОМПОНЕНТУ СОСТОЯНИЙ

Для вычисления условной min-энтропии в (9), а также учета побочных каналов утечки информации, разных квантовых эффективностей детекторов, как было отмечено выше, требуется явное построение атаки на однофотонную компоненту состояний.

При побочных каналах утечки фундаментальная связь между ошибкой и утечкой к Еве расцепляется. По этой причине, чтобы «подцепить» побочные квантовые состояния к информационным состояниям, требуется явное знание состояний и, соответственно, явное построение атаки.

В следующих разделах будет построена явная атака на однофотонные состояния, затем будут приведены оценки для длины секретного ключа.

Атака Евы на однофотонные информационные состояния в квантовом канале связи определяется унитарным оператором, который определяется и параметризуется набором параметров, контролируемых Евой. Атака Евы приводит к преобразованию входных квантовых состояний в новые квантовые состояния. Самое общее преобразование квантовых состояний (матриц плотности) в матрицы плотности

задается линейным вполне положительным отображением — супероператором [13]. Любой супероператор согласно [14] унитарно представим. Неформально, супероператор может быть реализован как совместная унитарная эволюция исходного состояния вместе со вспомогательным состоянием. В результате возникает совместное запутанное состояние. Взятие частичного следа по вспомогательной системе дает преобразованную матрицу плотности исходного состояния.

Построение супероператора сводится к построению унитарного оператора, который параметризуется набором параметров, которые находятся в руках подслушивателя.

Естественно, подслушиватель должен выбирать унитарный оператор оптимальным образом. Оптимальность понимается в смысле максимизации информации подслушивателя о передаваемых битах ключа при заданной наблюдаемой ошибке на приемной стороне.

При идеальных детекторах и без учета побочных каналов утечки информации можно явно не строить атаку, а воспользоваться энтропийными соотношениями неопределенностей. Оптимальная унитарная атака, достигающая нижнюю границу энтропийных соотношений неопределенностей [5], может быть построена явно [15].

Для дальнейшего потребуется построение явной атаки с учетом разных и неидеальных квантовых эффективностей детекторов. Для определенности будем иметь в виду протокол BB84, который является базовым. Предлагаемый метод применим и к другим протоколам.

Унитарная атака на информационные состояния в базисе + имеет вид

$$|0^+\rangle_X\otimes|0^+\rangle_Y\to|0^+\rangle_X\otimes U_{BE}(|0^+\rangle_Y\otimes|E\rangle_Q)=$$
$$=|0^+\rangle_X\otimes[\sqrt{1-Q^+}|0^+\rangle_Y\otimes|\Phi_{0^+}\rangle_Q+$$
$$+\sqrt{Q^+}|1^+\rangle_Y\otimes|\Theta_{0^+}\rangle_Q], \quad (42)$$

$$|1^+\rangle_X\otimes|1^+\rangle_Y\to|1^+\rangle_X\otimes U_{BE}(|1^+\rangle_Y\otimes|E\rangle_Q)=$$
$$=|1^+\rangle_X\otimes[\sqrt{1-Q^+}|1^+\rangle_Y\otimes|\Phi_{1^+}\rangle_Q+$$
$$+\sqrt{Q^+}|0^+\rangle_Y\otimes|\Theta_{1^+}\rangle_Q], \quad (43)$$

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

Формулы (42), (43) представляют собой разложение Шмидта, параметр Q^+ пока является свободным. Ниже увидим, что Q^+ является наблюдаемой ошибкой на приемной стороне, к которой приводит атака на квантовые состояния в канале связи.

Индекс «Q» для состояний Евы символизирует атаку на квантовые информационные состояния. Аналогичные (42), (43) выражения имеют место, когда в канал посылаются состояния в базисе $\times$, $|0^\times\rangle_Y$, $|1^\times\rangle_Y$. Имеем

$$|0^\times\rangle_X\otimes|0^\times\rangle_Y\to|0^\times\rangle_X\otimes U_{BE}(|0^\times\rangle_Y\otimes|E\rangle_Q)=$$
$$=|0^\times\rangle_X\otimes[\sqrt{1-Q^\times}|0^+\rangle_Y\otimes|\Phi_{0^\times}\rangle_Q+$$
$$+\sqrt{Q^\times}|1^+\rangle_Y\otimes|\Theta_{0^\times}\rangle_Q], \quad (44)$$

$$|1^\times\rangle_X\otimes|1^\times\rangle_Y\to|1^\times\rangle_X\otimes U_{BE}(|1^\times\rangle_Y\otimes|E\rangle_Q)=$$
$$=|1^\times\rangle_X\otimes[\sqrt{1-Q^\times}|1^\times\rangle_Y\otimes|\Phi_{1^\times}\rangle_Q+$$
$$+\sqrt{Q^\times}|0^\times\rangle_Y\otimes|\Theta_{1^\times}\rangle_Q]. \quad (45)$$

Связь между информационными состояниями в разных базисах дается соотношениями

$$|0^\times\rangle=\frac{1}{\sqrt{2}}\left(|0^+\rangle+|1^+\rangle\right),$$
$$|1^\times\rangle=\frac{1}{\sqrt{2}}\left(|0^+\rangle-|1^+\rangle\right). \quad (46)$$

Связь между состояниями Евы в разных базисах следует из линейности унитарного оператора. С учетом (42)–(46) получаем

$$|\Phi_\pm\rangle_E=|\Phi_{0^+}\rangle_E\pm|\Phi_{1^+}\rangle_E,$$
$$|\Theta_\pm\rangle_E=|\Theta_{0^+}\rangle_E\pm|\Theta_{1^+}\rangle_E, \quad (47)$$

где

$${}_E\langle\Phi_{0^\times}|\Phi_{0^\times}\rangle_E+{}_E\langle\Theta_{0^\times}|\Theta_{0^\times}\rangle_E=1,$$
$${}_E\langle\Phi_{1^\times}|\Phi_{1^\times}\rangle_E+{}_E\langle\Theta_{1^\times}|\Theta_{1^\times}\rangle_E=1,$$

$$|\Phi_{0^\times}\rangle_E=\frac{|\Phi_+\rangle_E+|\Theta_+\rangle_E}{2},$$
$$|\Theta_{0^\times}\rangle_E=\frac{|\Phi_-\rangle_E-|\Theta_-\rangle_E}{2}, \quad (48)$$
$$|\Phi_{1^\times}\rangle_E=\frac{|\Phi_+\rangle_E-|\Theta_+\rangle_E}{2},$$
$$|\Theta_{1^\times}\rangle_E=\frac{|\Phi_-\rangle_E+|\Theta_-\rangle_E}{2}. \quad (49)$$

Таким образом, атака Евы параметризуется величинами Q^+, $Q^\times$, имеющими смысл вероятностей ошибок в базисах $+$ и $\times$.

Отметим, что, как было показано в [16], векторы $\{|\Phi_{0^+}\rangle_Q, |\Phi_{1^+}\rangle_Q\}$ и $\{|\Theta_{0^+}\rangle_Q, |\Theta_{1^+}\rangle_Q\}$ лежат в ортогональных подпространствах. Аналогично для состояний $\{|\Phi_{0^\times}\rangle_Q, |\Phi_{1^\times}\rangle_Q\}$ и $\{|\Theta_{0^\times}\rangle_Q, |\Theta_{1^\times}\rangle_Q\}$. Этот факт будет использован в дальнейшем.

Ниже будет видно, что не все параметры, которыми параметризуется унитарная атака, являются наблюдаемыми при измерениях на приемной стороне. Существуют параметры, от которых зависит утечка информации к Еве, но которые явно не проявляются в измерениях Боба. Такими параметрами являются скалярные произведения между различными состояниями Евы.

7.1. Идеальные и реальные измерения

Для дальнейшего нам потребуются описания измерений для случаев идеальных и реальных детекторов. С формальной точки зрения любое измерение задается разложением единицы.

Идеальные измерения Боба в базисах $+$ и $\times$ даются разложением единицы I_Y (I_Y — единичный оператор в пространстве состояний Боба):

$$I_Y = |0^+\rangle_{YY}\langle 0^+| + |1^+\rangle_{YY}\langle 1^+| = \\ = |0^\times\rangle_{YY}\langle 0^\times| + |1^\times\rangle_{YY}\langle 1^\times|. \quad (50)$$

Ситуацию с не равной единице квантовой эффективностью детекторов можно описывать следующим образом. Пусть квантовые эффективности детекторов равны η_0 и η_1. Отсутствие отсчета в обоих детекторах можно считать отсчетом в фиктивном состоянии $\perp$. В этом случае измерения в базисах $+$ и $\times$ даются разложением единицы:

$$I_Y = \\ = \eta_0|0^+\rangle_{YY}\langle 0^+| + \eta_1|1^+\rangle_{YY}\langle 1^+| + \eta_\perp^+|\perp^+\rangle_{\perp\perp}\langle\perp^+| = \\ = \eta_1|0^\times\rangle_{YY}\langle 0^\times| + \eta_0|1^\times\rangle_{YY}\langle 1^\times| + \\ + \eta_\perp^\times|\perp^\times\rangle_{\perp\perp}\langle\perp^\times|. \quad (51)$$

Исходы измерений, при которых отсутствуют отсчеты в детекторах, отбрасываются.

Необходимо отметить важный факт (см. расстановку квантовых эффективностей в формуле (51)). Поскольку квантовые эффективности детекторов различаются, число регистрируемых 0 и 1 внутри каждого базиса не равно друг другу. Для выравнивания суммарного количества регистрируемых 0 и 1 в двух базисах, на приемной стороне при фазовом кодировании разность фаз в плечах интерферометра в разных базисах выбирается таким образом, чтобы 0 в одном базисе регистрировался в детекторе $D0$, а единица — в детекторе $D1$. В сопряженном базисе, наоборот, 0 регистрируется в детекторе $D1$, а 1 — в детекторе $D0$.

7.2. Матрицы плотности после идеальных измерений

Измерения (50) фактически сводятся к проектированию на набор ортогональных состояний. С учетом (42)–(46), после идеальных измерений Боба матрица плотности Алиса–Боб–Ева принимает вид

$$\rho^+_{XYE} = \frac{1}{2}|0^+\rangle_{XX}\langle 0^+| \otimes [(1-Q^+)|0^+\rangle_{YY}\langle 0^+| \otimes |\Phi_{0^+}\rangle_{QQ}\langle\Phi_{0^+}| + Q^+|1^+\rangle_Y \times \\ \times {}_Y\langle 1^+| \otimes |\Theta_{0^+}\rangle_{QQ}\langle\Theta_{0^+}|] + \frac{1}{2}|1^+\rangle_{XX}\langle 1^+| \otimes [(1-Q^+)|1^+\rangle_{YY}\langle 1^+| \otimes |\Phi_{1^+}\rangle_Q \times \\ \times {}_Q\langle\Phi_{1^+}| + Q^+|0^+\rangle_{YY}\langle 0^+| \otimes |\Theta_{1^+}\rangle_{QQ}\langle\Theta_{1^+}|]. \quad (52)$$

Частичная матрица плотности Алиса–Ева

$$\rho^+_{XE} = \frac{1}{2}|0^+\rangle_{XX}\langle 0^+| \otimes [(1-Q^+)|\Phi_{0^+}\rangle_{QQ}\langle\Phi_{0^+}| + Q^+|\Theta_{0^+}\rangle_{QQ}\langle\Theta_{0^+}|] + \frac{1}{2}|1^+\rangle_{XX}\langle 1^+| \otimes \\ \otimes[(1-Q^+)|\Phi_{1^+}\rangle_{QQ}\langle\Phi_{1^+}| + Q^+|\Theta_{1^+}\rangle_{QQ}\langle\Theta_{1^+}|]. \quad (53)$$

Частичная матрица плотности Евы

$$\rho^+_E = \frac{1}{2}(1-Q^+)[|\Phi_{0^+}\rangle_{QQ}\langle\Phi_{0^+}| + |\Phi_{1^+}\rangle_{QQ}\langle\Phi_{1^+}|] + Q^+\frac{1}{2}[|\Theta_{0^+}\rangle_{QQ}\langle\Theta_{0^+}| + |\Theta_{1^+}\rangle_{QQ}\langle\Theta_{1^+}|]. \quad (54)$$

В базисе $\times$ с учетом (42)–(46) и (50) находим

$$\rho^{\times}_{XYE}=\frac{1}{2}|0^{\times}\rangle_{XX}\langle 0^{\times}|\otimes[(1-Q^{\times})|0^{\times}\rangle_{YY}\langle 0^{\times}|\otimes|\Phi_{0\times}\rangle_{QQ}\langle\Phi_{0\times}|+Q^{\times}|1^{\times}\rangle_{YY}\langle 1^{\times}|\otimes|\Theta_{0\times}\rangle_{QQ}\langle\Theta_{0\times}|]+$$

$$+\frac{1}{2}|1^{\times}\rangle_{XX}\langle 1^{\times}|\otimes[(1-Q^{\times})|1^{\times}\rangle_{YY}\langle 1^{\times}|\otimes|\Phi_{1\times}\rangle_{QQ}\langle\Phi_{1\times}|+Q^{\times}|0^{\times}\rangle_{YY}\langle 0^{\times}|\otimes|\Theta_{1\times}\rangle_{QQ}\langle\Theta_{1\times}|]. \quad (55)$$

Частичная матрица плотности Алиса–Ева

$$\rho^{\times}_{XE}=\frac{1}{2}|0^{\times}\rangle_{XX}\langle 0^{\times}|\otimes[(1-Q^{\times})|\Phi_{0\times}\rangle_{QQ}\langle\Phi_{0\times}|+Q^{\times}|\Theta_{0\times}\rangle_{QQ}\langle\Theta_{0\times}|]+\frac{1}{2}|1^{\times}\rangle_{XX}\langle 1^{\times}|\otimes$$

$$\otimes[(1-Q^{\times})|\Phi_{1\times}\rangle_{QQ}\langle\Phi_{1\times}|+Q^{\times}|\Theta_{1\times}\rangle_{QQ}\langle\Theta_{1\times}|]. \quad (56)$$

Частичная матрица плотности Евы

$$\rho^{\times}_{E}=\frac{1}{2}(1-Q^{\times})[|\Phi_{0\times}\rangle_{QQ}\langle\Phi_{0\times}|+|\Phi_{1\times}\rangle_{QQ}\langle\Phi_{1\times}|]+Q^{\times}\frac{1}{2}[|\Theta_{0\times}\rangle_{QQ}\langle\Theta_{0\times}|+|\Theta_{1\times}\rangle_{QQ}\langle\Theta_{1\times}|]. \quad (57)$$

7.3. Матрицы плотности после реальных измерений

После реальных измерений и отбрасывания холостных исходов матрица плотности Алиса–Боб–Ева в базисе $+$, нормированная на полную вероятность отсчетов $\eta_0+\eta_1$ в детекторах, принимает вид

$$\rho^{+}_{XYE}=|0^{+}\rangle_{XX}\langle 0^{+}|\otimes[\xi_0(1-Q^{+})|0^{+}\rangle_{YY}\langle 0^{+}|\otimes|\Phi_{0+}\rangle_{QQ}\langle\Phi_{0+}|+\xi_1Q^{+}|1^{+}\rangle_{Y}\times$$

$$\times{}_{Y}\langle 1^{+}|\otimes|\Theta_{0+}\rangle_{QQ}\langle\Theta_{0+}|]+|1^{+}\rangle_{XX}\langle 1^{+}|\otimes[\xi_1(1-Q^{+})|1^{+}\rangle_{YY}\langle 1^{+}|\otimes|\Phi_{1+}\rangle_{Q}\times$$

$$\times{}_{Q}\langle\Phi_{1+}|+\xi_0Q^{+}|0^{+}\rangle_{YY}\langle 0^{+}|\otimes|\Theta_{1+}\rangle_{QQ}\langle\Theta_{1+}|]. \quad (58)$$

Частичная матрица плотности Алиса–Ева

$$\rho^{+}_{XE}=|0^{+}\rangle_{XX}\langle 0^{+}|\otimes[\xi_0(1-Q^{+})|\Phi_{0+}\rangle_{QQ}\langle\Phi_{0+}|+\xi_1Q^{+}|\Theta_{0+}\rangle_{QQ}\langle\Theta_{0+}|]+|1^{+}\rangle_{XX}\langle 1^{+}|\otimes$$

$$\otimes[\xi_1(1-Q^{+})|\Phi_{1+}\rangle_{QQ}\langle\Phi_{1+}|+\xi_0Q^{+}|\Theta_{1+}\rangle_{QQ}\langle\Theta_{1+}|]. \quad (59)$$

Частичная матрица плотности Евы

$$\rho^{+}_{E}=(1-Q^{+})[\xi_0|\Phi_{0+}\rangle_{QQ}\langle\Phi_{0+}|+\xi_1|\Phi_{1+}\rangle_{QQ}\langle\Phi_{1+}|]+Q^{+}[\xi_1|\Theta_{0+}\rangle_{QQ}\langle\Theta_{0+}|+\xi_0|\Theta_{1+}\rangle_{QQ}\langle\Theta_{1+}|]. \quad (60)$$

В базисе $\times$ получаем

$$\rho^{\times}_{XYE}=|0^{\times}\rangle_{XX}\langle 0^{\times}|\otimes[\xi_1(1-Q^{\times})|0^{\times}\rangle_{YY}\langle 0^{\times}|\otimes|\Phi_{0\times}\rangle_{QQ}\langle\Phi_{0\times}|+\xi_0Q^{\times}|1^{\times}\rangle_{YY}\langle 1^{\times}|\otimes|\Theta_{0\times}\rangle_{Q}\times$$

$$\times{}_{Q}\langle\Theta_{0\times}|]+|1^{\times}\rangle_{XX}\langle 1^{\times}|\otimes[\xi_0(1-Q^{\times})|1^{\times}\rangle_{YY}\langle 1^{\times}|\otimes|\Phi_{1\times}\rangle_{QQ}\langle\Phi_{1\times}|+\xi_1Q^{\times}|0^{\times}\rangle_{YY}\langle 0^{\times}|\otimes|\Theta_{1\times}\rangle_{QQ}\langle\Theta_{1\times}|]. \quad (61)$$

Частичная матрица плотности Алиса–Ева

$$\rho^{\times}_{XE}=|0^{\times}\rangle_{XX}\langle 0^{\times}|\otimes[\xi_1(1-Q^{\times})|\Phi_{0\times}\rangle_{QQ}\langle\Phi_{0\times}|+\xi_0Q^{\times}|\Theta_{0\times}\rangle_{QQ}\langle\Theta_{0\times}|]+|1^{\times}\rangle_{XX}\langle 1^{\times}|\otimes[\xi_0(1-Q^{\times})\times$$

$$\times|\Phi_{1\times}\rangle_{QQ}\langle\Phi_{1\times}|+\xi_1Q^{\times}|\Theta_{1\times}\rangle_{QQ}\langle\Theta_{1\times}|]. \quad (62)$$

Частичная матрица плотности Евы

$$\rho^{\times}_{E}=(1-Q^{\times})[\xi_1|\Phi_{0\times}\rangle_{QQ}\langle\Phi_{0\times}|+\xi_0|\Phi_{1\times}\rangle_{QQ}\langle\Phi_{1\times}|]+Q^{\times}\frac{1}{2}[\xi_0|\Theta_{0\times}\rangle_{QQ}\langle\Theta_{0\times}|+\xi_1|\Theta_{1\times}\rangle_{QQ}\langle\Theta_{1\times}|]. \quad (63)$$

В (58)–(63) для удобства введены обозначения

$$\xi_0=\frac{\eta_0}{\eta_0+\eta_1},\quad \xi_1=\frac{\eta_1}{\eta_0+\eta_1}. \quad (64)$$

7.4. Скрытые ненаблюдаемые параметры — скалярные произведения между состояниями подслушивателя

Измерения на приемной стороне не являются информационно полными, поскольку не позволяют однозначно восстановить искаженное информационное квантовое состояние на входе в приемную станцию. Этот факт приводит к тому, что утечка информации, которая выражается через условную энтропию, зависит от ненаблюдаемых скрытых для легитимных пользователей параметров атаки Евы. Точнее говоря, при одних и тех же вероятностях исходов измерений на приемной стороне значения ненаблюдаемых скрытых параметров будут разными. Исходы измерений не чувствительны к данным параметрам, но в то же время условная энтропия — утечка информации к Еве — зависит от данных параметров.

Такими ненаблюдаемыми скрытыми для Алисы и Боба параметрами являются скалярные произведения между состояниями подслушивателя, $\langle\Phi_{0^+}|\Phi_{1^+}\rangle$ и $\langle\Theta_{0^+}|\Theta_{1^+}\rangle$.

Фундаментальное требование унитарности оператора в (42)–(49) приводит к тому, что скалярные произведения между квантовыми состояниями подслушивателя в разных базисах связаны определенными соотношениями.

С учетом выражений (42)–(49), следующих из унитарности оператора Евы, получаем соотношения между скалярными произведениями в разных базисах:

$$\begin{aligned}(1-Q^+)\varepsilon(\Phi^+) &= |\langle\Phi_{0^+}|\Phi_{1^+}\rangle|,\\ Q^+\varepsilon(\Theta^+) &= |\langle\Theta_{0^+}|\Theta_{1^+}\rangle|,\end{aligned} \tag{65}$$

$$\begin{aligned}(1-Q^\times)\varepsilon(\Phi^\times) &= |\langle\Phi_{0^\times}|\Phi_{1^\times}\rangle|,\\ Q^\times\varepsilon(\Theta^\times) &= |\langle\Theta_{0^\times}|\Theta_{1^\times}\rangle|,\end{aligned} \tag{66}$$

$$(1-Q^+)\varepsilon(\Phi^+) = \frac{1}{2}[1-2Q^+ + \\ + (1-Q^+)\,\mathrm{Re}(\varepsilon(\Phi^+)) - Q^+\,\mathrm{Re}(\varepsilon(\Theta^+))], \tag{67}$$

$$Q^\times\varepsilon(\Theta^\times) = \frac{1}{2}[1-2Q^+ - \\ - (1-Q^+)\,\mathrm{Re}(\varepsilon(\Phi^+)) + Q^+\,\mathrm{Re}(\varepsilon(\Theta^+))]. \tag{68}$$

Параметры Q^+ и $Q^\times$ являются экспериментально наблюдаемыми параметрами и имеют смысл вероятностей ошибок в прямом $+$ и сопряженном $\times$ базисах. Результаты измерений на стороне Боба не зависят от скалярных произведений (65)–(68), но от них зависит утечка информации к Еве.

По этой причине при определенных из измерений параметрах Q^+ и $Q^\times$, по ненаблюдаемым скрытым параметрам необходимо проводить максимизацию утечки информации к Еве при данных наблюдаемых Q^+ и $Q^\times$.

7.5. Область допустимых значений ненаблюдаемых скрытых параметров

Покажем, что независимым является только один параметр $\varepsilon_+(\Phi)$, остальные выражаются через него. Кроме того, поскольку состояния $|\Phi_{0^{+,\times},0^{+,\times}}\rangle$ и $|\Theta_{0^{+,\times},0^{+,\times}}\rangle$ ортогональны, в утечку информации, которая выражается через собственные числа матрицы плотности Евы (см. ниже), входят только модули скалярных произведений. Это означает, что утечка информации к Еве не зависит от фаз, вообще говоря, комплексных скалярных произведений. Из-за такой нечувствительности к фазе можно считать скалярные произведения вещественными.

Из наблюдаемых величин (вероятностей исходов измерений) можно определить не все скалярные произведения, от которых зависит утечка информации к подслушивателю. Из четырех скалярных произведений $\varepsilon_+(\Phi)$, $\varepsilon_+(\Theta)$, $\varepsilon_\times(\Phi)$ и $\varepsilon_\times(\Theta)$ остается неопределенным $\varepsilon_+(\Phi)$. Остальные три могут быть выражены через него.

С учетом уравнений (65)–(68) получаем следующие соотношения:

$$\varepsilon_+(\Theta) = \frac{1-2Q^\times-(1-Q^+)\varepsilon_+(\Phi)}{Q^+}, \tag{69}$$

$$\varepsilon_\times(\Phi) = \frac{1}{2(1-Q^\times)}\times \\ \times\left((1-2Q^+)-(1-2Q^\times)+2(1-Q^+)\varepsilon_+(\Phi)\right), \tag{70}$$

$$\varepsilon_\times(\Theta) = \frac{1}{2Q^\times}\times \\ \times\left((1-2Q^+)+(1-2Q^\times)-2(1-Q^+)\varepsilon_+(\Phi)\right). \tag{71}$$

Скалярные произведения между квантовыми состояниями по модулю не должны превышать единицы, с учетом (65)–(71) это приводит к следующим неравенствам:

$$L_1(Q^+,Q^\times) = \frac{1-2Q^\times-Q^+}{1-Q^+} \le \varepsilon_+(\Phi) \le \\ \le \frac{1-2Q^\times+Q^+}{1-Q^+} = R_1(Q^+,Q^\times), \tag{72}$$

$$L_2(Q^+,Q^\times)=\frac{1}{2(1-Q^+)}\times$$
$$\times\left(-2(1-Q^\times)-[(1-2Q^+)-(1-2Q^\times)]\right)\le$$
$$\le\varepsilon_+(\Phi)\le\frac{1}{2(1-Q^+)}\left(2(1-Q^\times)-\right.$$
$$\left.-[(1-2Q^+)-(1-2Q^+)]\right)=R_2(Q^+,Q^\times),\quad(73)$$

$$L_3(Q^+,Q^\times)=\frac{1}{2(1-Q^+)}\times$$
$$\times\left((1-2Q^+)+(1-2Q^\times)-2Q^\times\right)\le\varepsilon_+(\Phi)\le$$
$$\le\frac{1}{2(1-Q^+)}\left((1-2Q^+)+(1-2Q^\times)+2Q^\times\right)=$$
$$=R_3(Q^+,Q^\times).\quad(74)$$

Таким образом, максимизацию утечки информации к подслушивателю достаточно проводить по одному параметру $\varepsilon_+(\Phi)$, который с учетом (72)–(74) меняется на отрезке

$$R(Q^+,Q^\times)=\min\left\{R_1(Q^+,Q^\times),\right.$$
$$\left.R_2(Q^+,Q^\times),R_3(Q^+,Q^\times)\right\},\quad(75)$$

$$L(Q^+,Q^\times)=\max\left\{L_1(Q^+,Q^\times),\right.$$
$$\left.L_2(Q^+,Q^\times),L_3(Q^+,Q^\times)\right\},\quad(76)$$

$$V(Q^+,Q^\times)=R(Q^+,Q^\times)-L(Q^+,Q^\times).\quad(77)$$

Удобно параметризовать $\varepsilon_+(\Phi)$ следующим образом:

$$\varepsilon_+(\Phi)=L(Q^+,Q^\times)+xV(Q^+,Q^\times),\quad x\in[0,1].\quad(78)$$

Остальные параметры выражаются по формулам (62)–(71).

В итоге максимизацию утечки информации к Еве при данных наблюдаемых параметрах Q^+ и $Q^\times$ можно проводить только по одной переменной x.

7.6. Собственные числа матрицы плотности подслушивателя

Для вычисления условных энтропий нужны собственные числа матриц плотности. Для собственных чисел матрицы плотности ρ^+_{XE} в базисе + находим

$$\xi_0(1-Q^+),\quad\xi_1Q^+,\quad\xi_1(1-Q^+),\quad\xi_0Q^+.\quad(79)$$

Аналогично для матрицы плотности $\rho^\times_{XE}$:

$$\xi_1(1-Q^\times),\quad\xi_0Q^\times,\quad\xi_0(1-Q^\times),\quad\xi_1Q^\times.\quad(80)$$

Собственные числа матрицы плотности ρ^+_E в базисе + равны

$$\Lambda_\pm(\Phi^+)=(1-Q^+)\lambda_\pm(\Phi^+),$$
$$\Lambda_\pm(\Theta^+)=Q^+\lambda_\pm(\Theta^+),\quad(81)$$

где

$$\lambda_\pm(\Phi^+)=$$
$$=\frac{1}{2}\left\{1\pm\sqrt{1-\frac{4(A(\Phi^+)B(\Phi^+)-|\varepsilon(\Phi^+)|^2)}{1-|\varepsilon(\Phi^+)|^2}}\right\},\quad(82)$$

$$A(\Phi^+)=\xi_0+\xi_1|\varepsilon(\Phi^+)|^2,$$
$$B(\Phi^+)=\xi_0|\varepsilon(\Phi^+)|^2+\xi_1,\quad(83)$$

$$\lambda_\pm(\Theta^+)=$$
$$=\frac{1}{2}\left\{1\pm\sqrt{1-\frac{4(A(\Theta^+)B(\Theta^+)-|\varepsilon(\Theta^+)|^2)}{1-|\varepsilon(\Theta^+)|^2}}\right\},\quad(84)$$

$$A(\Theta^+)=\xi_0+\xi_1|\varepsilon(\Theta^+)|^2,$$
$$B(\Theta^+)=\xi_0|\varepsilon(\Theta^+)|^2+\xi_1,\quad(85)$$

Аналогично (79)–(85) для собственных чисел матрицы плотности $\rho^\times_E$ в базисе $\times$ получаем

$$\Lambda_\pm(\Phi^\times)=(1-Q^\times)\lambda_\pm(\Phi^\times),$$
$$\Lambda_\pm(\Theta^\times)=Q^\times\lambda_\pm(\Theta^\times),\quad(86)$$

где

$$\lambda_\pm(\Phi^\times)=$$
$$=\frac{1}{2}\left\{1\pm\sqrt{1-\frac{4(A(\Phi^\times)B(\Phi^\times)-|\varepsilon(\Phi^\times)|^2)}{1-|\varepsilon(\Phi^\times)|^2}}\right\},\quad(87)$$

$$A(\Phi^\times)=\xi_1+\xi_0|\varepsilon(\Phi^\times)|^2,$$
$$B(\Phi^\times)=\xi_1|\varepsilon(\Phi^\times)|^2+\xi_0,\quad(88)$$

$$\lambda_\pm(\Theta^\times)=$$
$$=\frac{1}{2}\left\{1\pm\sqrt{1-\frac{4(A(\Theta^\times)B(\Theta^\times)-|\varepsilon(\Theta^\times)|^2)}{1-|\varepsilon(\Theta^\times)|^2}}\right\},\quad(89)$$

$$A(\Theta^\times)=\xi_0+\xi_1|\varepsilon(\Theta^\times)|^2,$$
$$B(\Theta^\times)=\xi_0|\varepsilon(\Theta^\times)|^2+\xi_1.\quad(90)$$

8. ОЦЕНКА ДЛИНЫ СЕКРЕТНОГО КЛЮЧА: ОДНОФОТОННЫЙ СЛУЧАЙ, ИДЕАЛЬНЫЕ ДЕТЕКТОРЫ, АСИМПТОТИЧЕСКИЙ ПРЕДЕЛ

Для того чтобы показать, как изменяется оценка длины секретного ключа по мере включения в рассмотрение различных реальных каналов утечки информации, сначала приведем такие оценки для строго однофотонного источника, когда параметры атаки Евы известны точно. Затем учтем тот факт, что имеется только оценка параметров атаки — ошибки на приемной стороне при конечной длине переданных последовательностей.

Сначала рассмотрим асимптотический случай длинных последовательностей. При стремлении длины передаваемой последовательности к бесконечности оценка вероятности ошибки становится самой вероятностью, т. е. параметр ошибки известен точно.

В случае идеальных детекторов нижняя граница энтропийных соотношений неопределенностей достигается на симметричной атаке [15], $Q^{+} = Q^{\times} = Q$. Ненаблюдаемые скрытые параметры — скалярные произведения в этом случае равны

$$\varepsilon(\Phi^{+,\times}) = \varepsilon(\Theta^{+,\times}) = 1 - 2Q.$$

Оценки параметров и первого усечения матриц плотности, связанного с оценкой наблюдаемых параметров, не требуется. Достаточно только второго усечения при вычислении условной сглаженной энтропии матрицы плотности в виде тензорного произведения $\rho_{XE}^{(n)} = \rho_{XE}^{\otimes n}$. Сглаженная условная min-энтропия, вычисленная на усеченной матрице плотности $\overline{\rho}_{XE}^{\otimes n}$, удовлетворяющей условию ε-близости в смысле следового расстояния, имеет вид

$$\begin{aligned} H_{min}^{\varepsilon}(\overline{\rho}_{XE}^{\otimes n}|\overline{\rho}_{E}^{\otimes n}) = \\ = \max_{||\rho_{XE}^{\otimes n} - \overline{\rho}_{XE}^{\otimes n}||_1 \le \varepsilon} H_{min}(\rho_{XE}^{\otimes n}|\rho_{E}^{\otimes n}) = \\ = H(\rho_{XE}^{\otimes n}) - H(\rho_{E}^{\otimes n}) - \delta(\varepsilon) = \\ = n\left(1 - h(Q) - (2H_{max}(\rho_X) + 1)\sqrt{\frac{1}{n}\log\left(\frac{1}{\varepsilon}\right)}\right), \quad (91) \end{aligned}$$

где Q — истинная вероятность ошибки, матрица плотности в (91) берется из соотношений (52)–(57),

$$\text{const} = 2H_{max}(\rho_X) + 1,$$

$$H_{max}(\rho_X) = \text{rank}(\rho_X) = 2$$

[4], n — длина зарегистрированной последовательности.

Утечка информации при коррекции ошибок в асимптотическом шенноновском пределе с учетом (52)–(71) имеет вид

$$\begin{aligned} H_{max}^{\varepsilon}(\rho_{XY}^{\otimes n}|\rho_{Y}^{\otimes n}) = H(\rho_{XY}^{\otimes n}) - H(\rho_{Y}^{\otimes n}) + \delta(\varepsilon) = \\ = n\left(h(Q) + \text{const}\sqrt{\frac{1}{n}\log\left(\frac{1}{\varepsilon}\right)}\right). \quad (92) \end{aligned}$$

Оценка длины ε-секретного ключа принимает вид

$$\begin{aligned} \ell^{\varepsilon} = H_{min}^{\varepsilon}(\rho_{XE}^{\otimes n}|\rho_{E}^{\otimes n}) - H_{max}^{\varepsilon}(\rho_{XY}^{\otimes n}|\rho_{Y}^{\otimes n}) = \\ = n\left(1 - 2h(Q) - 2\text{const}\sqrt{\frac{1}{n}\log\left(\frac{1}{\varepsilon}\right)}\right). \quad (93) \end{aligned}$$

В асимптотическом пределе $n \to \infty$, $\varepsilon \to 0$ последнее слагаемое в (93) стремится к нулю, и мы приходим к знаменитой формуле для длины секретного ключа протокола BB84 [4, 17] $\ell^{\varepsilon \to 0} = n(1 - 2h(Q))$. Длина секретного ключа обращается в нуль при ошибке выше критической $Q_c \approx 11\,\%$.

9. ОЦЕНКА ПАРАМЕТРОВ ПО РЕЗУЛЬТАТАМ ИЗМЕРЕНИЙ

В реальной ситуации истинная вероятность ошибки $\overline{Q}$ точно не известна, имеется лишь оценка данной вероятности. Есть различные способы оценки данной вероятности. Первый способ состоит в раскрытии и сравнении части последовательности, посланной Алисой, и последовательности, измеренной Бобом. Пусть оценка вероятности ошибки — доля неправильных отсчетов n_{incorr}, зарегистрированных Бобом из последовательности длины n_1, есть $Q = n_{incorr}/n_1$. Из-за конечной длины последовательности число (частота) неправильных отсчетов флуктуирует.

Второй способ оценки вероятности состоит в следующем. Существующие процедуры коррекции ошибок позволяют сразу проводить коррекцию ошибок без предварительной оценки вероятности ошибки. Пусть проведена чистка ошибок, после коррекции известна оценка вероятности ошибки — известно число исправленных битов. Однако это не означает, что такое число и есть истинное число ошибок в последовательности n_1. Для определенности будем иметь в виду первый способ. При этом для экономии обозначений будем считать, что длина n_1 раскрываемой последовательности для оценки вероятности ошибки совпадает с длиной не раскрываемой последовательности n для получения ключа.

При оценке вероятности ошибки фактически мы имеем дело с бернуллиевской схемой испытаний. Для бернуллиевской схемы испытаний вероятность того, что частота ошибок Q в последовательности длины n отличается от вероятности $\overline{Q}$, есть (см., например, [18])

$$\Pr\{\Omega_1\} = \Pr\{|\overline{Q} - Q| \le \delta(\varepsilon_1)\} \ge \\ \ge 1 - 2\exp\{-2\delta(\varepsilon_1)^2 n_1\} = 1 - \varepsilon_1. \quad (94)$$

Важно отметить, что данная оценка является однородной в том смысле, что вероятность отклонения частоты $\overline{Q}$ от истинной вероятности $\overline{Q}$ не зависит от величины вероятности $\overline{Q}$. По этой причине формулу (94) можно интерпретировать следующим образом: вероятность события, что наблюдаемая величина ошибки попадает в δ-окрестность истинной вероятности $\overline{Q}$ $(Q - \delta(\varepsilon_1), Q + \delta(\varepsilon_1))$, реализуется с вероятностью не менее $1 - \varepsilon_1$.

10. ОЦЕНКА ДЛИНЫ СЕКРЕТНОГО КЛЮЧА: ОДНОФОТОННЫЙ СЛУЧАЙ, ИДЕАЛЬНЫЕ ДЕТЕКТОРЫ, КОНЕЧНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ

При конечной длине последовательности, когда вероятность ошибки точно не известна, для вычисления сглаженной min-энтропии нужно использовать формулы (52)–(57) для матриц плотности, в которых вместо Q должно быть подставлено $Q_{max} = \\ = Q + \delta(\varepsilon_1)$ — чем больше ошибка, тем меньше условная энтропия, тем меньше нехватка информации Евы о ключе. Значение берется на правой границе доверительного интервала в (94). При этом вероятность события Ω_1 не менее $1 - \varepsilon_1$. С учетом сказанного для тензорного произведения

$$\rho^{(n)}_{XE|Q_{max}} = \rho^{\otimes n}_{XE|Q_{max}}$$

для сглаженной энтропии с учетом (52)–(57) получаем

$$H^{\varepsilon_1+\varepsilon_2}_{min}(\rho^{(n)}_{XE|Q\in\delta_Q}|\rho^{(n)}_{E|Q\in\delta_Q}) \ge \\ \ge n\left(H(\rho_{XE|Q_{max}}|\rho_{E|Q_{max}}) - \right. \\ \left. - \text{const}\sqrt{\frac{1}{n}\log\left(\frac{1}{\varepsilon_2}\right)}\right), \quad Q_{max} = Q + \delta(\varepsilon_1), \quad (95)$$

где Q — наблюдаемая ошибка на приемной стороне, Q_{max} — оценка вероятности ошибки — значение на правой границе доверительного интервала.

В итоге вычисление условной сглаженной энтропии проводится на матрицах плотности $\varepsilon = \varepsilon_1 + \varepsilon_2$, близких в смысле следового расстояния к истинной матрице плотности, находим

$$H^{\varepsilon_1+\varepsilon_2}_{min}(\rho^{(n)}_{XE|Q\in\delta_Q}|\rho^{(n)}_{E|Q\in\delta_Q}) \ge \\ \ge n\left(1-h(Q+\delta(\varepsilon_1))-\text{const}\sqrt{\frac{1}{n}\log\left(\frac{1}{\varepsilon_2}\right)}\right). \quad (96)$$

Для оценки длины секретного ключа нужно учесть информацию, выдаваемую при коррекции ошибок. В шенноновском пределе аналогично (91)–(93) получаем

$$H^{\varepsilon_1+\varepsilon_2}_{max}(\rho^{(n)}_{XE|Q\in\delta_Q}|\rho^{(n)}_{E|Q\in\delta_Q}) \le \\ \le n\left(h(Q+\delta(\varepsilon_1)) + \text{const}\sqrt{\frac{1}{n}\log\left(\frac{1}{\varepsilon_2}\right)}\right). \quad (97)$$

После этого проверяется факт исправления ошибок. Алиса генерирует открыто случайную битовую строку длиной n и вычисляет бит четности данной строки со своим ключом. Боб поступает аналогично. Биты четности Алисы и Боба открыто сравниваются. Процедура проводится M раз. Если все M сравнений успешны, то вероятность того, что все ошибки действительно исправлены и очищенный ключ Боба X_B совпадает с ключом Алисы X_A, есть

$$\Pr[X_A = X_B] \ge 1 - \varepsilon_{corr}, \quad \varepsilon_{corr} = 1/2^M. \quad (98)$$

Поскольку при такой проверке через открытый канал связи выдается $M = \log(1/\varepsilon_{corr})$ битов информации, длина финального секретного ключа должна быть уменьшена на M битов. Окончательно для оценки длины $\varepsilon = \varepsilon_1 + \varepsilon_2$-секретного ключа получаем

$$\ell^{\varepsilon} = n\left(1 - 2h\left(Q + \delta(\varepsilon_1)\right)\right) - \\ - 2\text{const}\sqrt{n\log\left(\frac{1}{\varepsilon_2}\right)} - \log\left(\frac{1}{\varepsilon_{corr}}\right). \quad (99)$$

Связь между $\delta(\varepsilon_1)$ и ε_1 дается формулой (94).

Формула (99) означает, что если n-битовая строка первичного ключа до коррекции ошибок сжимается при помощи универсальных хеш-функций второго порядка до длины, определяемой (99), то сжатая строка — финальный ключ — будет ε-секретным в смысле следового расстояния.

Из сравнения (93) и (99) видно, что при конечной длине передаваемой последовательности эффективная ошибка Q_{max}, входящая в формулу для длины

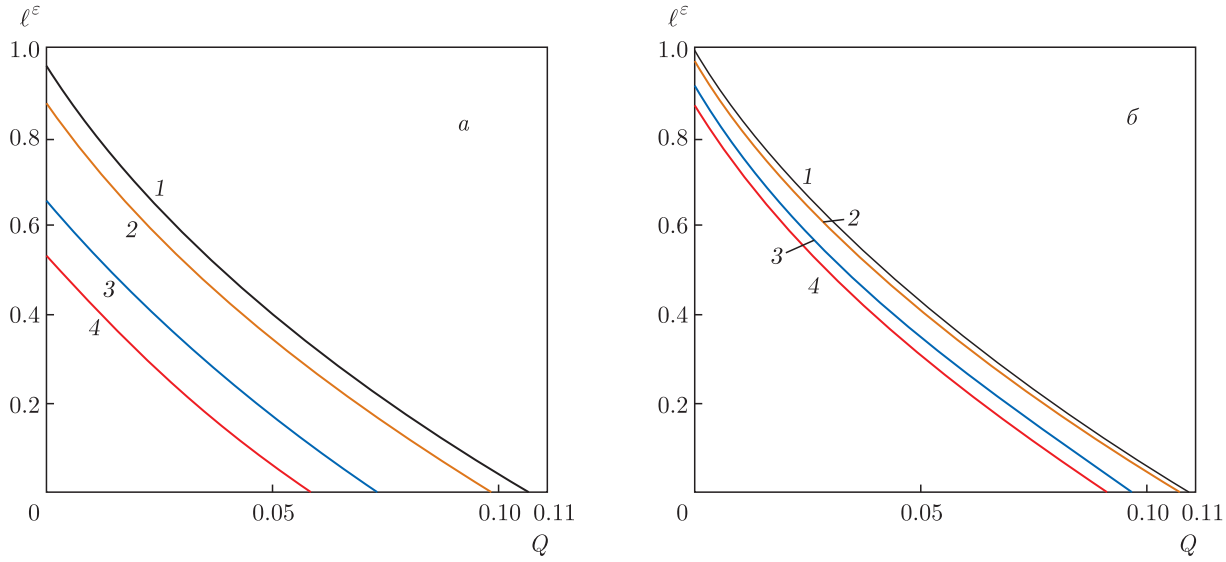

Рис. 1. Зависимости длины секретного ключа в пересчете на одну посылку от наблюдаемой величины ошибки Q: a) предел конечных последовательностей, имеется оценка вероятности ошибки, $б$) вероятность ошибки точно известна. Параметр секретности $\varepsilon_1 = \varepsilon_2 = 10^{-9}$ для всех кривых. Длина последовательности n для оценки параметров и длина последовательности для получения ключа приняты одинаковыми и равными $n = 10^7$ (*1*), 10^6 (*2*), 10^5 (*3*), 10^4 (*4*)

секретного ключа, оказывается большей, чем реальная ошибка Q.

Результат, аналогичный выражению (99), был получен ранее в [5] с использованием энтропийных соотношений неопределенностей. В нашем случае результат получается явным построением атаки Евы на передаваемый ключ, что требуется для последующего вычисления длины ключа в случае неидеальных детекторов с различными квантовыми эффективностями, а также для учета побочных каналов утечки информации к Еве.

11. РЕЗУЛЬТАТЫ РАСЧЕТОВ В ОДНОФОТОННОМ СЛУЧАЕ

Для иллюстрации эволюции длины секретного ключа по мере последовательного включения в рассмотрение различных факторов приведем результаты численных расчетов.

Однофотонный случай, предел конечных последовательностей, равные квантовые эффективности детекторов.

На рис. 1 приведены зависимости от Q длины секретного ключа для строго однофотонных информационных состояний в пределе конечных последовательностей (рис. 1a) в случае, когда истинная вероятность ошибки неизвестна, а делается ее оценка через наблюдаемую величину ошибки Q. Рисунок 1$б$ относится к случаю, когда истинная вероятность ошибки $\overline{Q}$ точно известна.

Как видно из рис. 1, с ростом длины последовательности n, используемой для оценки величины ошибки, критическая наблюдаемая ошибка Q, до которой возможно секретное распределение ключей, увеличивается и принимает асимптотическое значение $Q \approx 11\,\%$. Таким образом, при заданном параметре секретности $\varepsilon_{1,2}$ для достижения большей величины критической ошибки требуется более длинная последовательность для оценки истинной вероятности ошибки.

Однофотонный случай, разные квантовые эффективности детекторов, конечные последовательности.

Отметим, что поиск минимума по одной переменной x проводился с учетом флуктуаций параметра ошибки (см. формулу (78)). Как видно на рис. 2, длина ключа обнаруживает минимум как функция параметра минимизации x. Кроме того, скалярные произведения между состояниями Евы в симметричном случае — одинаковые наблюдаемые ошибки в прямом и сопряженном базисах, $\xi_0 = \xi_1 = 0.5$ — равные квантовые эффективности детекторов, оказываются одинаковыми в минимуме длины секретного ключа. В симметричном случае скалярные произведения $\varepsilon_+(\Phi)$ и $\varepsilon_\times(\Phi)$, $\varepsilon_+(\Theta)$ и $\varepsilon_\times(\Theta)$ оказываются равными $1 - 2\overline{Q}$ ($\overline{Q}$ — ошибка с учетом флук-

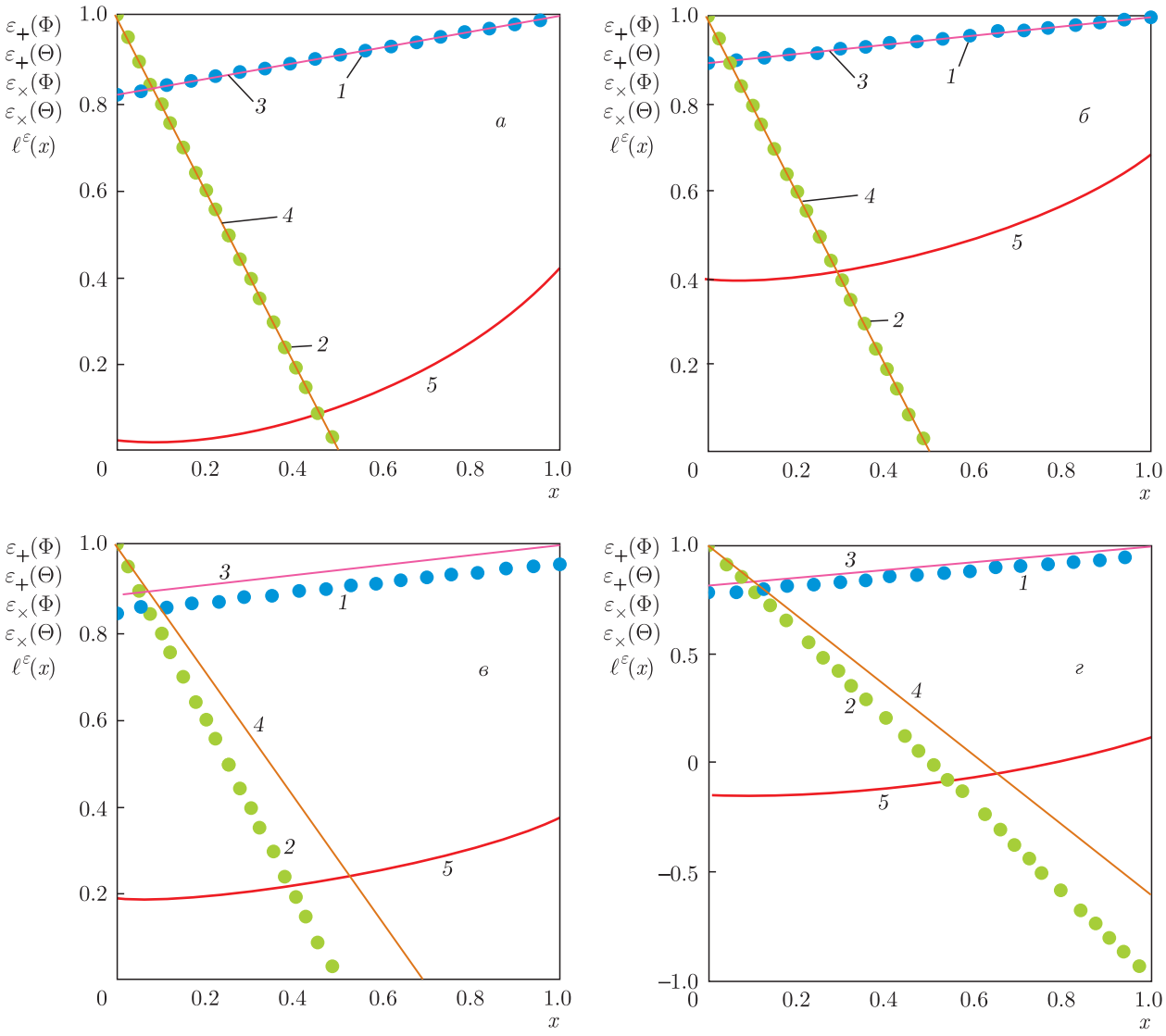

Рис. 2. Зависимости ненаблюдаемых скрытых параметров — скалярных произведений между состояниями Евы в разных базисах (кривые *1*–*4*), кривые *5* — зависимости длины секретного ключа от параметра оптимизации x (формула (78)). Кривым *1* отвечает зависимость $\varepsilon_+(\Phi)$, *2* — $\varepsilon_+(\Theta)$, *3* — $\varepsilon_\times(\Phi)$, *4* — $\varepsilon_\times(\Theta)$ как функция параметра x. Значения параметров: $\xi_0 = 0.5$, $\xi_1 = 0.5$ для всех кривых рис. *а, б*. Вероятность наблюдаемой ошибки $Q^+ = Q^\times = 0.05$ для всех кривых рис. *а, б*. Длина последовательности $n = 10^4$ для кривых рис. *а*, $n = 10^6$ для кривых рис. *б*. Значения параметров: $\xi_0 = 0.25$, $\xi_1 = 0.75$ для всех кривых рис. *в, г*. Вероятность наблюдаемой ошибки $Q^+ = 0.05$, $Q^\times = 0.07$ для всех кривых рис. *в, г*. Длина последовательности $n = 10^4$ для кривых рис. *г*, $n = 10^6$ для кривых рис. *в*. Параметр секретности для всех кривых $\varepsilon_1 = \varepsilon_2 = 10^{-9}$

туаций) в разных базисах. Как видно из сравнения рис. 2*а* и *б*, а также рис. 2*г* и *в*, с уменьшением длины последовательности n, используемой для оценки параметров, длина секретного ключа уменьшается из-за большего доверительного интервала при заданном параметре секретности ε. Кроме того, с увеличением разницы квантовых эффективностей детекторов длина секретного ключа уменьшается. Например, из рис. 2*г* видно, что при достаточно большой разности квантовых эффективностей детекторов ($\xi_0 = 0.25$, $\xi_1 = 0.75$) длина ключа в минимуме оказывается отрицательной, что означает невозможность получить секретный ключ при таких параметрах. При длине последовательности

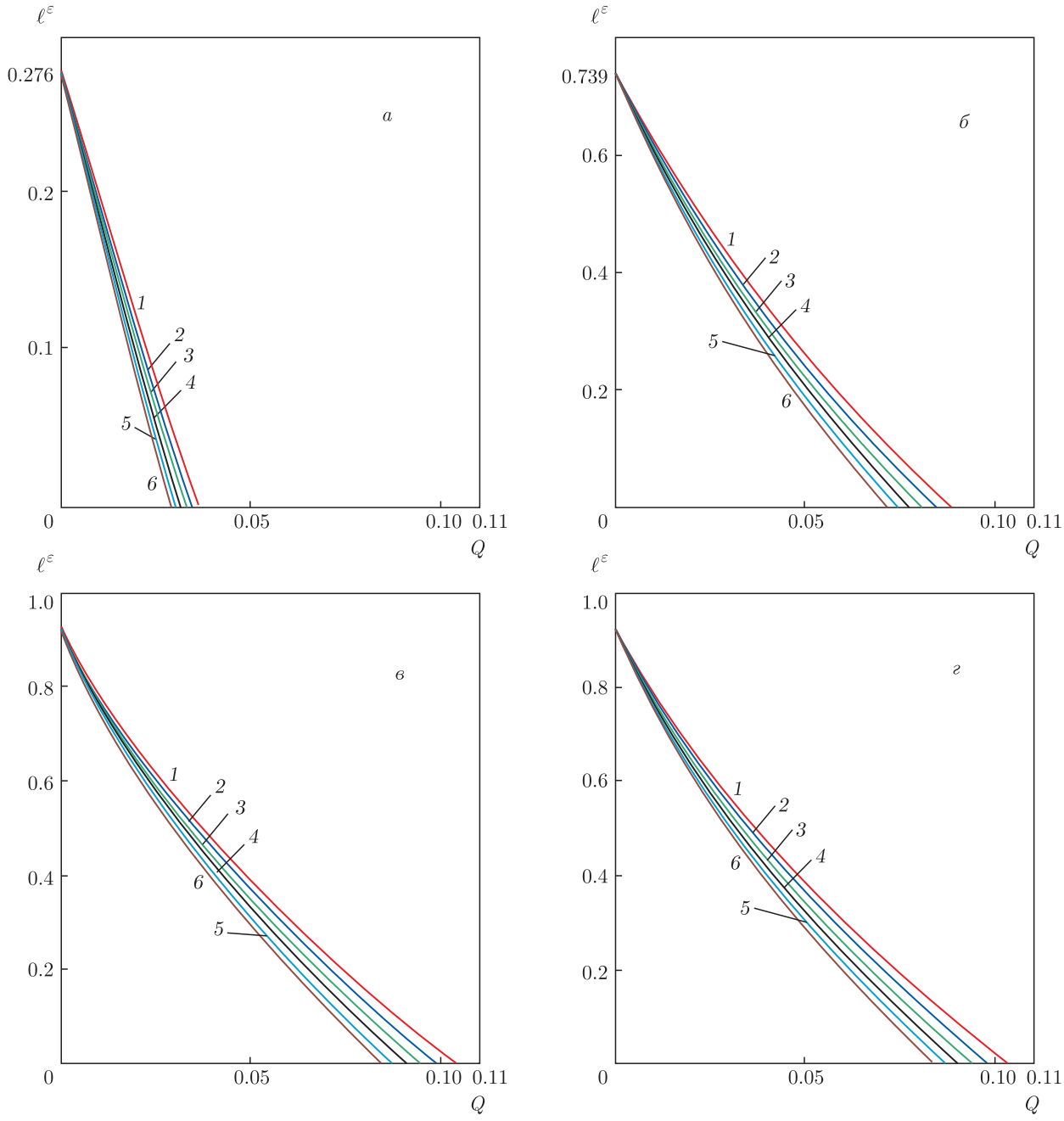

Рис. 3. Зависимости длины секретного ключа от наблюдаемой ошибки Q в базисе $+$ в случае конечной длины последовательности. Параметры для рис. *а, б*: квантовые эффективности детекторов $\xi_0 = 0.25$, $\xi_1 = 0.75$ для всех кривых; наблюдаемая ошибка в базисе $Q^\times = Q$, $1.1Q$, $1.2Q$, $1.3Q$, $1.4Q$, $1.5Q$ соответственно для кривых *1–6*; длина последовательности для оценки параметров $n = 10^4$ (*а*), $n = 10^6$ (*б*). Параметры для рис. *в, г*: *в*) квантовые эффективности детекторов $\xi_0 = 0.5$, $\xi_1 = 0.5$ для всех кривых; *г*) квантовые эффективности детекторов $\xi_0 = 0.45$, $\xi_1 = 0.55$ для всех кривых; наблюдаемая ошибка в базисе $Q^\times = Q$, $1.1Q$, $1.2Q$, $1.3Q$, $1.4Q$, $1.5Q$ соответственно для кривых *1–6*; длина последовательности для оценки параметров рис. *в, г* $n = 10^6$. Параметр секретности для всех рисунков $\varepsilon_1 = \varepsilon_2 = 10^{-9}$

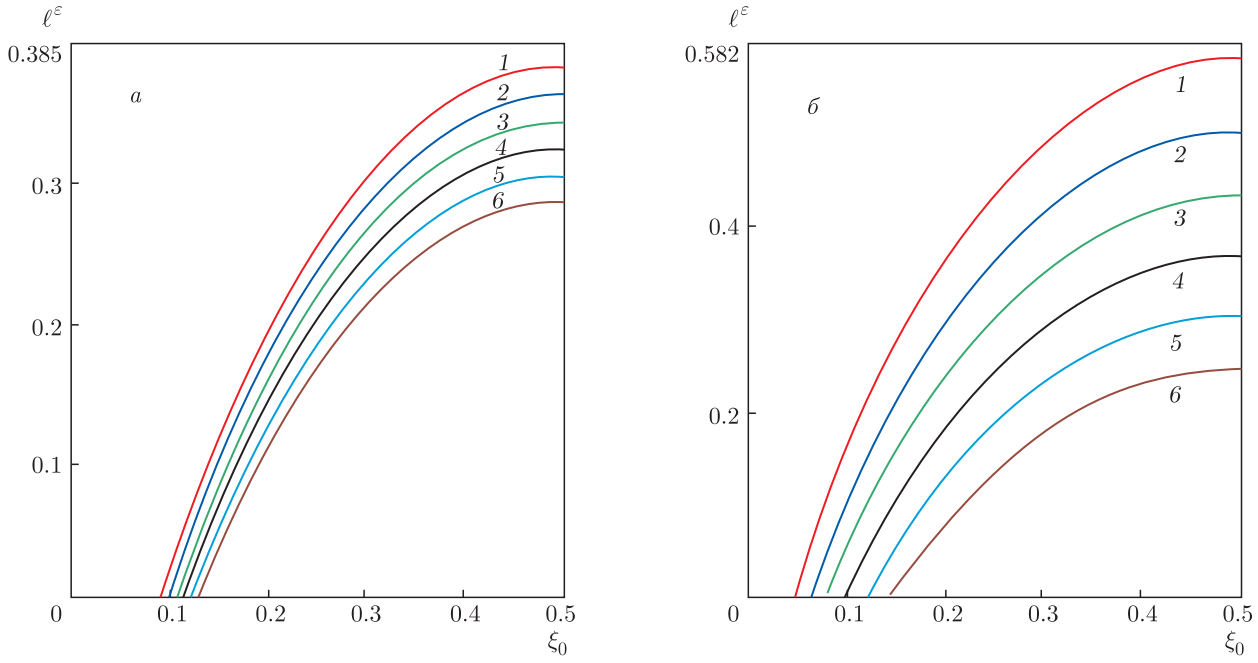

Рис. 4. Зависимости длины секретного ключа от квантовой эффективности детекторов $\xi_0 = \eta_0/(\eta_0+\eta_1)$ при различных значениях наблюдаемой ошибки в разных базисах. Значения используемых параметров: *а*) $Q^{+} = 0.05$ для всех кривых, $Q^{\times} = 0.05,\ 1.1\cdot 0.05,\ 1.2\cdot 0.05,\ 1.3\cdot 0.05,\ 1.4\cdot 0.05, 1.5\cdot 0.05$ соответственно для кривых *1–6*; *б*) $Q^{+} = 0.01,\ 0.02,\ 0.03,\ 0.04,\ 0.05,\ 0.06$, $Q^{\times} = 0.05,\ 1.1\cdot 0.05,\ 1.2\cdot 0.05,\ 1.3\cdot 0.05,\ 1.4\cdot 0.05,\ 1.5\cdot 0.05$ соответственно для кривых *1–6*. Длина последовательности для всех кривых $n = 10^6$, параметр секретности $\varepsilon_1 = \varepsilon_2 = 10^{-9}$

$n = 10^4$ для оценки параметров доверительный интервал оказывается широким и оценка истинной вероятности ошибки завышенной (ср. рис. 2*в* и 2*г*).

Зависимости длины секретного ключа от наблюдаемой ошибки в однофотонном случае при конечных длинах последовательностей приведены на рис. 3. Однородная оценка параметров по наблюдаемой ошибке проводилась по формуле (94). После этого проводилась минимизация длины ключа по параметру x. Основной вывод из рис. 3 сводится к тому, что критическая наблюдаемая ошибка и длина секретного ключа уменьшаются по мере несимметричности по наблюдаемой ошибке в разных базисах и при разных квантовых эффективностях детекторов. Выход длины секретного ключа на асимптотический режим происходит при длинах n, используемых для оценки истинной вероятности ошибки, т. е. при значениях $n \approx 10^6$ (см. рис. 3*а,б* и рис. 3*в,г*).

Представляет интерес поведение длины секретного ключа в широком диапазоне квантовых эффективностей детекторов. На рис. 4 приведены зависимости от ξ_0 длины секретного ключа в строго однофотонном случае при конечных длинах последовательностей.

Как следует из рис. 4, при данной наблюдаемой вероятности ошибки существует критическое значение разности квантовых эффективностей, при которой еще возможно распределение секретных ключей. При стремлении квантовой эффективности одного из детекторов к нулю длина секретного ключа обращается в нуль при сколь угодно малой ошибке.

12. УЧЕТ НЕОДНОФОТОННОСТИ ИНФОРМАЦИОННЫХ СОСТОЯНИЙ, DECOY STATE-МЕТОД ПРИ РАЗНЫХ КВАНТОВЫХ ЭФФЕКТИВНОСТЯХ ДЕТЕКТОРОВ

Как упоминалось выше, секретный ключ набирается из однофотонной компоненты состояний, достигающей приемной стороны. В этом разделе получим оценки для вероятности однофотонной компоненты состояний, когда параметры атаки Евы известны точно. В следующем разделе учтем тот факт, что параметры точно не известны, а имеется лишь оценка параметров. Затем будут учтены поправки, связанные с конечной длиной передаваемых последовательностей.

Исходный Decoy State-метод исходит из следующих посылок [19–22]. Информационными состояниями являются когерентные состояния. Используется несколько когерентных состояний с разными средними числами 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») соответственно со средним числом фотонов $\xi \in \mathcal{I} = \{\mu, \nu_1, \nu_2\}$. Для матрицы плотности состояний в канале имеем

$$\rho^x(\xi) = e^{-2\xi} \sum_{k=0}^{\infty} \frac{(2\xi)^k}{k!} |\Psi_k^x\rangle_{BB}\langle\Psi_k^x| =$$

$$= \sum_{k=0}^{\infty} P^{(k)}(\mu) |\Psi_k^x\rangle_{BB}\langle\Psi_k^x|, \qquad (100)$$

$$P_k(\xi) = e^{-2\xi} \frac{(2\xi)^k}{k!},$$

$$|\Psi_k^x\rangle_B = \sqrt{\frac{k!}{2^k}} \sum_{m=0}^{k} e^{i\varphi_x m} \frac{|m\rangle_1 \otimes |k-m\rangle_2}{\sqrt{m!(k-m)!}}, \qquad (101)$$

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

Нужно отметить следующее. Состояния в (100), (101) после рандомизации фаз в среднем имеют такой вид в канале связи. При фазовом кодировании число фотонов в двух временных окнах равно 2ξ. Перед регистрацией данные (см., например, [8]) состояния преобразуются на интерферометре Маха–Цандера, затем регистрируются в определенном временном окне, поэтому вероятность регистрации пропорциональна ξ, а не 2ξ. Этот факт учитывается при численных расчетах ниже.

Стандартная квантовомеханическая интерпретация матрицы плотности — квантового ансамбля, сводится к тому, что в канале присутствуют состояния $|\Psi_k^x\rangle_{BB}\langle\Psi_k^x|$ с разными числами фотонов с вероятностями

$$P_k(\xi) = e^{-2\xi} \frac{(2\xi)^k}{k!}.$$

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. 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

$$\mathcal{T}_{BE}[|\Psi_k^x\rangle_{BB}\langle\Psi_k^x|] = \rho_{k,BE}^x. \qquad (102)$$

В результате возникает запутанное состояние Боб–Ева $\rho_{k,BE}^x$. Явный вид состояния в (102) 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 различными средними числами фотонов.

В итоге Боб на приемной стороне измеряет не исходные состояния, а состояния (102).

Измерения Боба на приемной стороне описываются разложением единицы, обычно ортогональным (50), (51). 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

$$P_{Y|X}^{(k)}(y|X = x) = \mathrm{Tr}_{BE}\{M_y \rho_{k,BE}^x\}. \qquad (103)$$

Для Decoy State-метода принципиально важно, что условная вероятность не зависит от ξ — среднего

числа фотонов в квантовом состоянии, а только от обнаруженного числа фотонов в данной посылке. Полный темп отсчетов (условная вероятность пока не нормирована) 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 (100), (103) равен

$$P_\xi(y^\alpha|X=x^\alpha) = \\ = \sum_{k=0}^{\infty} P^{(k)}(\xi) P^{(k)}_{Y|X}(y^\alpha|X=x^\alpha). \quad (104)$$

Темп отсчетов (104) зависит от базиса $\alpha = +, \times$ из-за разных квантовых эффективностей детекторов, но не зависит от ξ.

Для дальнейшего рассмотрения будут нужны парциальные темпы отсчетов, а именно, посылались 0 и 1, отсчеты были 0, аналогично, посылались 1 и 0, отсчеты были 1 (как правильные, так и неправильные). Соответствующие условные вероятности в базисе + имеют вид

$$Y_k^\alpha(00) = P^{(k)}_{Y|X}(0^+|X=0^+), \quad (105)$$

$$Y_k^\alpha(10) = P^{(k)}_{Y|X}(1^+|X=0^+), \quad (106)$$

$$Y_k^\alpha(11) = P^{(k)}_{Y|X}(1^+|X=1^+), \quad (107)$$

$$Y_k^\alpha(01) = P^{(k)}_{Y|X}(0^+|X=1^+). \quad (108)$$

Полный условный темп отсчетов есть

$$P_\xi^{tot}(0^\alpha|X=0^\alpha) = e^{-2\xi}\sum_{k=0}^{\infty}\frac{(2\xi)^k}{k!}Y_k^\alpha(00), \quad (109)$$

$$P_\xi^{tot}(1^\alpha|X=0^\alpha) = e^{-2\xi}\sum_{k=0}^{\infty}\frac{(2\xi)^k}{k!}Y_k^\alpha(10), \quad (110)$$

$$P_\xi^{tot}(1^\alpha|X=1^\alpha) = e^{-2\xi}\sum_{k=0}^{\infty}\frac{(2\xi)^k}{k!}Y_k^\alpha(11), \quad (111)$$

$$P_\xi^{tot}(0^\alpha|X=1^\alpha) = e^{-2\xi}\sum_{k=0}^{\infty}\frac{(2\xi)^k}{k!}Y_k^\alpha(01), \quad (112)$$

$$P_\xi^{tot,\alpha} = P_\xi^{tot}(0^\alpha|X=0^\alpha) + P_\xi^{tot}(1^\alpha|X=0^\alpha) + \\ + P_\xi^{tot}(1^\alpha|X=1^\alpha) + P_\xi^{tot}(0^\alpha|X=^\alpha). \quad (113)$$

Дадим интерпретацию вероятностей в (105)–(113). Состояния, отвечающие 0 и 1, в каждом базисе посылаются равновероятно. Величина

$$e^{-2\xi}\frac{(2\xi)^k}{k!}$$

есть вероятность того, что в канале будет присутствовать компонента состояний с фоковским числом фотонов k при условии, что в канал было послано когерентное состояние со средним числом фотонов ξ. $Y_k^\alpha(ji)$ есть вероятность того, что Бобом будет зарегистрирован отсчет $j=0,1$ при условии, что в канал была послана компонента состояний с числом фотонов k, отвечающая логическому биту Алисы i. Данная вероятность не зависит от ξ.

Используем устоявшиеся в Decoy State-методе обозначения для данных вероятностей.

Подчеркнем, что парциальные темпы отсчетов Y_k (в англоязычной версии Yields) не зависят от среднего числа фотонов ξ в состоянии.

Определим парциальный темп ошибочных отсчетов для k-фотонной компоненты состояний, находим

$$\mathrm{Err}_k^\alpha = P^{(k)}_{Y|X}(1^\alpha|0^\alpha) + P^{(k)}_{Y|X}(0^\alpha|1^\alpha) = \\ = Y_k^\alpha(10) + Y_k^\alpha(01). \quad (114)$$

Вероятность ошибки в k-фотонной компоненте состояний

$$Q_k^\alpha = \frac{P^{(k)}_{Y|X}(1^\alpha|0^\alpha) + P^{(k)}_{Y|X}(0^\alpha|1^\alpha)}{P^{(k)}_{Y|X}(1^\alpha|0^\alpha) + P^{(k)}_{Y|X}(0^\alpha|0^\alpha) + P^{(k)}_{Y|X}(0^\alpha|1^\alpha) + P^{(k)}_{Y|X}(1^\alpha|1^\alpha)}. \quad (115)$$

Полный темп ошибочных отсчетов

$$\mathrm{Err}_\xi^\alpha = e^{-2\xi}\sum_{k=0}^{\infty}\frac{(2\xi)^k}{k!}\,\mathrm{Err}_k^\alpha, \\ Q^{tot,\alpha} = \frac{\mathrm{Err}_\xi^\alpha}{P_\xi^{tot,\alpha}}. \quad (116)$$

12.1. Оценки вероятности однофотонной компоненты состояний и ошибки по Decoy State-методу

Для дальнейшего удобно ввести обозначения (далее $\alpha = +, \times$ — индекс базиса)

$$\overline{P_\xi^{tot}(y^\alpha|X=x^\alpha)} = e^{2\xi}P_\xi^{tot}(y^\alpha|X=x^\alpha), \qquad \overline{\mathrm{Err}_\xi^\alpha} = e^{2\xi}\,\mathrm{Err}_\xi^\alpha\,. \tag{117}$$

Из (109)–(113), (117) получаем оценку вероятности вакуумной компоненты состояний на приемной стороне:

$$Y_0(y^\alpha|X=x^\alpha) \le \max\left\{\frac{2\nu_1\overline{P_{\nu_2}^{tot}(y^\alpha|X=x^\alpha)} - 2\nu_2\overline{P_{\nu_1}^{tot}(y^\alpha|X=x^\alpha)}}{2(\nu_1-\nu_2)}, 0\right\}. \tag{118}$$

Для оценки вероятности однофотонной компоненты с учетом (109)–(113), (117), (118) находим

$$\begin{aligned} Y_1(y^\alpha|X=x^\alpha) \ge \\ \ge \frac{1}{2(\nu_1-\nu_2) - \dfrac{(2\nu_1)^2-(2\nu_2)^2}{2\mu}} \times \\ \times\left\{\left[\overline{P_{\nu_1}^{tot}(y^\alpha|X=x^\alpha)} - \overline{P_{\nu_2}^{tot}(y^\alpha|X=x^\alpha)}\right] - \right. \\ - \frac{(2\nu_1)^2-(2\nu_2)^2}{(2\mu)^2}\left[\overline{P_\mu^{tot}(y^\alpha|X=x^\alpha)} - \right. \\ \left.\left. - Y_0(y^\alpha|X=x^\alpha)\right]\right\}. \end{aligned} \tag{119}$$

Полная вероятность детектирования однофотонной компоненты $Y_1(y^\alpha|X=x^\alpha)$ зависит от детектора. Удобно представить вероятности однофотонной компоненты состояний в следующем виде:

$$\begin{aligned} Y_1(0^+|X=0^+) &= \eta_0\mathcal{Y}_1(1-Q^+), \\ Y_1(1^+|X=0^+) &= \eta_1\mathcal{Y}_1Q^+, \end{aligned} \tag{120}$$

$$\begin{aligned} Y_1(1^+|X=1^+) &= \eta_1\mathcal{Y}_1(1-Q^+), \\ Y_1(0^+|X=1^+) &= \eta_0\mathcal{Y}_1Q^+. \end{aligned} \tag{121}$$

Смысл такой параметризации вероятностей следует из унитарной атаки на однофотонную компоненту состояний. Подслушиватель может блокировать часть однофотонных посылок, оставшуюся часть неблокируемых посылок, атакует унитарно. Вероятность неблокируемых посылок есть $\mathcal{Y}_1$. Если, например, в канале присутствовала однофотонная компонента состояния $|0^+\rangle$ в базисе $+$, то после унитарной атаки данное состояние превратится в искаженное состояние (42)–(45), в котором присутствуют компоненты $|0^+\rangle$ и $|1^+\rangle$ (см. формулы (42)–(45)). Компонента $|0^+\rangle$ будет давать отсчет в детекторе $D0$ с вероятностью $\eta_0(1-Q^+)$, а компонента $|1^+\rangle$ — отсчет в детекторе $D1$ с вероятностью η_1Q^+. Полное число отсчетов, правильных и ошибочных, от однофотонной компоненты состояний будет равно

$$\mathcal{Y}_1[\eta_0(1-Q^+) + \eta_1Q^+]$$

полной вероятности регистрации однофотонной компоненты (с точностью до множителя $e^{-2\xi}2\xi/1!$).

Аналогично для других компонент однофотонных состояний. Далее, принимая во внимание формулу (119) для вероятности однофотонной компоненты Y_1, находим

$$(\eta_0+\eta_1)\mathcal{Y}_1 = \sum_{i,j=0,1} Y_1(j^+|X=i^+). \tag{122}$$

В базисе $\times$ имеем

$$\begin{aligned} Y_1(0^\times|X=0^\times) &= \eta_1\mathcal{Y}_1(1-Q_1^\times), \\ Y_1(1^\times|X=0^\times) &= \eta_0\mathcal{Y}_1Q_1^+, \end{aligned} \tag{123}$$

$$\begin{aligned} Y_1(1^\times|X=1^\times) &= \eta_0\mathcal{Y}_1(1-Q_1^\times), \\ Y_1(0^\times|X=1^\times) &= \eta_1\mathcal{Y}_1Q_1^\times, \end{aligned} \tag{124}$$

$$(\eta_0+\eta_1)\mathcal{Y}_1 = \sum_{i,j=0,1} Y_1(j^\alpha|X=i^\alpha). \tag{125}$$

Представление (122)–(125) вероятности однофотонной компоненты имеет простой смысл. После обнаружения однофотонной компоненты состояний в канале (данная вероятность зависит от среднего числа фотонов в состоянии и равна $e^{-2\xi}2\xi$) подслушиватель принимает решение, с какой вероятностью блокировать данную компоненту, а с какой вероятностью доставить ее на приемную сторону после унитарной атаки. Величина Y_1 есть вероятность перепосыла искаженной однофотонной компоненты состояний, соответственно величина $\mathcal{Y}_1\eta_0$ есть полная вероятность регистрации однофотонной компоненты детектором с квантовой эффективностью η_0 с учетом правильных и неправильных отсчетов. Вероятность правильных отсчетов среди них будет $\mathcal{Y}_1\eta_0(1-Q^{+,\times})$, соответственно вероятность ошибочных отсчетов в данном детекторе есть $\mathcal{Y}_1\eta_0Q^{+,\times}$.

Для оценки вероятности ошибки в однофотонной компоненте в базисе $+$, используя (114)–(119), находим

$$\begin{aligned} (\eta_0+\eta_1)\mathcal{Y}_1Q_1^+ = Y_1^+(10) + Y_1^+(01) = \\ = \overline{\mathrm{Err}_1^+} \le \frac{\overline{\mathrm{Err}_{\nu_1}^+} - \overline{\mathrm{Err}_{\nu_2}^+}}{2(\nu_1-\nu_2)}. \end{aligned} \tag{126}$$

Аналогично для оценки вероятности ошибки в однофотонной компоненте в базисе $\times$ с учетом (114)–(119) получаем

$$(\eta_0+\eta_1)\mathcal{Y}_1 Q_1^{\times} = Y_1^{\times}(10)+Y_1^{\times}(01) = \\ = \overline{\mathrm{Err}_1^{\times}} \le \frac{\overline{\mathrm{Err}_{\nu_1}^{\times}}-\overline{\mathrm{Err}_{\nu_2}^{\times}}}{2(\nu_1-\nu_2)}. \quad (127)$$

Комбинируя (126), (127) и (119), для вероятностей $Q_1^{+,\times}$ получаем

$$Q_1^{+} \le \frac{\overline{\mathrm{Err}_1^{+}}}{(\eta_0+\eta_1)\mathcal{Y}_1}, \quad Q_1^{\times} \le \frac{\overline{\mathrm{Err}_1^{\times}}}{(\eta_0+\eta_1)\mathcal{Y}_1}, \quad (128)$$

$$Y_1^{\alpha}(00)+Y_1^{\alpha}(10)+Y_1^{\alpha}(01)+Y_1^{\alpha}(11) = \\ = (\eta_0+\eta_1)\mathcal{Y}_1 \ge \frac{1}{2(\nu_1-\nu_2)-\dfrac{(2\nu_1)^2-(2\nu_2)^2}{2\mu}} \times \\ \times \left\{ \left[\overline{P_{\nu_1}^{tot,\alpha}}-\overline{P_{\nu_2}^{tot,\alpha}}\right] - \right. \\ \left. - \frac{(2\nu_1)^2-(2\nu_2)^2}{(2\mu)^2}\left[\overline{P_{\mu}^{tot,\alpha}}-Y_0^{\alpha}\right]\right\}. \quad (129)$$

В (129) для краткости введены обозначения

$$\overline{P_{\xi}^{tot,\alpha}} = \sum_{y^\alpha}\sum_{x^\alpha}\overline{P_{\xi}^{tot}(y^\alpha|X=x^\alpha)}, \\ Y_0^{\alpha} = \sum_{y^\alpha}\sum_{x^\alpha} Y_0(y^\alpha|X=x^\alpha). \quad (130)$$

Вероятности парциальных и полных вероятностей отсчетов в разных базисах определяются из экспериментальных данных. Формулы (126)–(128) дают вероятность регистрации однофотонной компоненты и вероятность ошибки в ней.

12.2. Определение вероятностей из экспериментальных данных, концентрационные неравенства

Для определения вероятности однофотонной компоненты состояний и вероятности ошибки в ней необходимо знать вероятности отсчетов. В реальности данные вероятности неизвестны, из эксперимента определяются частоты отсчетов для соответствующих вероятностей.

Оценка условных вероятностей в (109)–(113) получается путем раскрытия части переданной последовательности состояний. Пусть Алиса посылает $N_{\xi}^{sent}(j^\alpha|X=i^\alpha)$ состояний $i=0,1$ в базисе $\alpha=+,\times$ со средним числом фотонов ξ. Боб проводит измерения в согласованном базисе и получает $N_{\xi}^{reg}(j^\alpha|X=i^\alpha)$ отсчетов для $j=0,1$. Частота отсчетов равна

$$\widetilde{P_{\xi}^{tot}}(j^\alpha|X=i^\alpha) = \frac{N_{\xi}^{reg}(j^\alpha|X=i^\alpha)}{N_{\xi}^{sent}(j^\alpha|X=i^\alpha)}. \quad (131)$$

Частота отсчетов является случайной величиной и подвержена флуктуациям.

Существует две постановки задачи.

1. Точные вероятности известны и требуется определить вероятность того, что при конечной серии испытаний произойдет число отсчетов, количество которых лежит в заданном интервале.

В такой постановке задача относится к области теории вероятностей.

2. Точные значения вероятностей неизвестны и требуется определить вероятность того, что истинная вероятность отсчетов лежит в заданном интервале значений.

Именно такая ситуация имеет место в квантовой криптографии (см. разделы выше). Такая постановка относится к области математической статистики.

Нас интересует вторая постановка задачи, а именно, вычисление вероятности $\Pr\{\Omega_1\}$ события Ω_1, что истинная вероятность лежит в заданном диапазоне значений.

Для решения задачи в такой постановке используются так называемые концентрационные неравенства. Существует обширная литература по данному вопросу и различные типы концентрационных неравенств (см., например, [18] и большое число ссылок в работе).

Удобна следующая формулировка применительно к нашему случаю: пусть ζ_i $(i=1,\ldots,n)$ — независимые случайные величины, $0 \le \zeta_i \le 1$. Пусть эмпирическое математическое ожидание

$$\overline{\zeta} = \frac{1}{n}\left(\sum_{i=1}^{n}\zeta_i\right), \quad (132)$$

тогда имеет место соотношение

$$\Pr\left(|\overline{\zeta}-\mathrm{E}(\overline{\zeta})| \le \delta\right) \ge 1-2e^{-2\delta^2 n}, \quad (133)$$

где $\mathrm{E}(\overline{\zeta})$ — математическое ожидание.

Применительно к нашей ситуации оценка вероятности выглядит следующим образом:

$$\Pr\{|\widetilde{P_{\xi}^{tot}}(j^\alpha|X=i^\alpha)-P_{\xi}^{tot}(j^\alpha|X=i^\alpha)| \le \delta(\varepsilon_1)\} \ge \\ \ge 1-2\exp\left(-2\delta^2(\varepsilon_1)N_{\xi}^{sent}(j^\alpha|X=i^\alpha)\right) = \\ = 1-\varepsilon_1. \quad (134)$$

Для получения ε-секретного ключа фиксируется значение ε_1, по этому значению определяется величина $\delta(\varepsilon_1)$ — ширина доверительного интервала, который используется при вычислении ошибки и условной сглаженной min-энтропии.

Важно отметить, что, строго говоря, оценки вероятности должны быть однородными — правые части (94), (133) не должны зависеть от самой неизвестной вероятности, которую нужно оценить.

Для того чтобы проиллюстрировать существенную разницу в оценках при первой постановке задачи (вероятности известны) и второй (вероятности неизвестны, см. выше), приведем оценку вероятности при первой постановке. Наиболее ясно это можно сделать на примере бернуллиевской схемы испытаний. Пусть случайные величины ζ_i имеют бернуллиевское распределение ($\zeta_i = *$ — есть фотоотсчет с вероятностью p, $\zeta_i = \sqcup$ — нет фотоотсчета с вероятностью $1-p$). В этом случае вероятность того, что при n испытаниях число отсчетов $\overline{p} = \tilde{n}p$ будет уклоняться от математического ожидания np не более, чем на δ, есть (см., например, [18])

$$\Pr\{|\overline{p}-p| \le \delta\} \ge 1 - 2\exp\left(-\frac{\delta^2 n}{2p(1-p)}\right). \quad (135)$$

В (135) используем стандартную оценку в правой части, существует множество вариантов с различными функциями вероятностей в правой части [18], но для наших целей достаточно такой оценки. В нашем случае оценка с известным распределением вероятностей выглядит как

$$\Pr\{|\widetilde{P_\xi^{tot}}(j^\alpha|X=i^\alpha) - P_\xi^{tot}(j^\alpha|X=i^\alpha)| \le \delta(\varepsilon_1)\} \ge$$
$$\ge 1-2\exp\left(-\frac{\delta^2(\varepsilon_1)N_\xi^{sent}(j^\alpha|X=i^\alpha)}{P_\xi^{tot}(j^\alpha|X=i^\alpha)(1-P_\xi^{tot}(j^\alpha|X=i^\alpha))}\right) = 1-\varepsilon_1. \quad (136)$$

Сравнение (134) и (136) показывает, что для того, чтобы получить оценку числа отсчетов за серию испытаний с одинаковой точностью (δ) при известной и неизвестной вероятности, длины серий испытаний должны быть существенно разными. Действительно, при неизвестной вероятности длина серии должна быть

$$N_\xi^{unknown,sent}(j^\alpha|X=i^\alpha) = N_\xi^{known,sent}(j^\alpha|X=i^\alpha) \times \frac{1}{4P_\xi^{tot}(j^\alpha|X=i^\alpha)(1-P_\xi^{tot}(j^\alpha|X=i^\alpha))}, \quad (137)$$

где

$$N_\xi^{unknown,sent}(j^\alpha|X=i^\alpha), \quad N_\xi^{known,sent}(j^\alpha|X=i^\alpha)$$

— длина серии испытаний при неизвестной и известной вероятности. Вероятность фотоотсчета $P_\xi^{tot}(j^\alpha|X=i^\alpha)$ имеет порядок $\mu\eta T(L=100\text{ км}) \approx \approx 10^{-4}$–$10^{-5}$ (при типичном среднем числе фотонов в информационном состоянии 0.1–0.5, $T(L) = 10^{-dL/10}$, $d \approx 0.2$ дБ/км, L — длина линии, $\eta \approx 0.1$ — квантовая эффективность детекторов). Сказанное означает, что длина серии, используемой для оценки параметров атаки, должна быть в 10^4–10^5 раз больше для достижения одинаковой точности δ, соответственно, параметра ε_1, определяющего секретность ключей. Как увидим ниже, поскольку требуется оценивать не единственный параметр, неточности оценок по отдельным параметрам складываются и длина требуемой серии может возрастать на 6 порядков.

Нам не известны работы, в которых бы оговаривалось данное обстоятельство. Обычно используют оценки (136) или подобные, при этом молчаливо предполагая, что вероятности известны, т. е. используют неоднородную оценку.

Однородность оценки истинной вероятности по наблюдаемой частоте означает вероятность того, что наблюдаемая частота уклоняется от истинной вероятности не более, чем на $\delta(\varepsilon_1)$, не зависит от самой истинной вероятности. Однородная оценка гарантирует, что вероятность $\Pr\{\Omega_1\}$ того, что истинные значения параметров, которые определяют секретность ключа, не выходят из заданного интервала, не менее $1-\varepsilon_1$.

12.3. Учет флуктуаций параметров

В этом разделе получим оценки вероятности однофотонной компоненты и вероятности ошибки в ней, которые затем будут использованы при оценке длины секретного ключа. Считаем, что вероятности априорно неизвестны (см. обсуждение в предыдущем разделе).

Вероятность того, что частота отсчетов $\overline{P_\xi^{tot}(y^\alpha|X=x^\alpha)}$ (умноженная на коэффициент $e^{2\xi}$) в последовательности длины N_ξ отличается от истинной вероятности $\widehat{\overline{P_\xi^{tot}(y^\alpha|X=x^\alpha)}}$ на величину не более $\overline{\delta^\alpha_{x,y,\xi}}$, оказывается не менее

$$\Pr\left\{|\overline{P_\xi^{tot}(y^\alpha|X=x^\alpha)}-\widehat{\overline{P_\xi^{tot}(y^\alpha|X=x^\alpha)}}|\le\overline{\delta^\alpha_{x,y,\xi}}\right\}\ge 1-2\exp\left\{-2(\delta^\alpha_{x,y,\xi})^2N_\xi\right\}=1-\varepsilon^\alpha_{x,y\xi}, \tag{138}$$

$$\overline{\delta^\alpha_{x,y,\xi}}=e^\xi\delta^\alpha_{x,y,\xi}.$$

Аналогично вероятность того, что частота ошибок $\overline{\mathrm{Err}^\alpha_\xi}$ в последовательности длины $N_{Err,\xi}$ отличается от истинной вероятности ошибок $\widehat{\overline{\mathrm{Err}^\alpha_\xi}}$ на величину не более $\delta^\alpha_{Err,\xi}$, не менее, чем

$$\Pr\left\{|\overline{\mathrm{Err}^\alpha_\xi}-\widehat{\overline{\mathrm{Err}^\alpha_\xi}}|\le\overline{\delta^\alpha_{Err,\xi}}\right\}\ge$$
$$\ge 1-2\exp\left\{-2(\delta^\alpha_{Err,\xi})^2N_{Err,\xi}\right\}=1-\varepsilon^\alpha_{Err,\xi}, \tag{139}$$

$$\overline{\delta^\alpha_{Err,\xi}}=e^\xi\delta^\alpha_{Err,\xi}.$$

Для дальнейшего нам понадобятся значения параметров на левой и правой границах доверительного интервала. Значения на границах доверительного интервала обозначим как

$$\overline{P_\xi^{tot}(y^\alpha|X=x^\alpha)}^\pm=\overline{P_\xi^{tot}(y^\alpha|X=x^\alpha)}\pm\overline{\delta^\alpha_{x,y,\xi}}, \tag{140}$$

$$\overline{\mathrm{Err}^\alpha_\xi}^\pm=\overline{\mathrm{Err}^\alpha_\xi}\pm\overline{\delta^\alpha_{Err,\xi}}. \tag{141}$$

Для вероятности ошибки нужна консервативная оценка в пользу подслушивателя, т. е. необходимо выбирать значение на правой границе, для $(Q_1^{+,\times})^+$ получаем

$$(Q_1^+)^+\le\frac{\overline{\mathrm{Err}_1^+}^+}{(\eta_0+\eta_1)\mathcal{Y}_1^-},$$
$$(Q_1^\times)^+\le\frac{\overline{\mathrm{Err}_1^\times}^+}{(\eta_0+\eta_1)\mathcal{Y}_1^-}. \tag{142}$$

Индекс «+» в (140)–(142) отвечает значениям на правой границе доверительного интервала, а индекс «−» — на левой.

При вычислении $\overline{\mathrm{Err}_1^+}^+$ и $\overline{\mathrm{Err}_1^\times}^+$ в (142) используются формулы (128), в которых оценки вероятностей, входящие со знаком «+», берутся на правой границе доверительного интервала, а входящие со знаком «−» берутся на левой границе доверительного интервала.

Аналогично при вычислении оценки вероятности однофотонной компоненты нужно брать ее значение на левой границе доверительного интервала, с учетом (129) находим

$$(\eta_0+\eta_1)\mathcal{Y}_1^-\ge$$
$$\ge\frac{1}{2(\nu_1-\nu_2)-\dfrac{(2\nu_1)^2-(2\nu_2)^2}{2\mu}}\times$$
$$\times\left\{\left[\overline{P_{\nu_1}^{tot,\alpha}}^--\overline{P_{\nu_2}^{tot,\alpha}}^+\right]-\frac{(2\nu_1)^2-(2\nu_2)^2}{(2\mu)^2}\times\right.$$
$$\left.\times\left[\overline{P_\mu^{tot,\alpha}}^+-(Y_0^\alpha)^-\right]\right\}. \tag{143}$$

12.4. Матрицы плотности и оценка длины секретного ключа с учетом флуктуаций параметров

Набором наблюдаемых флуктуирующих параметров являются

$$\mathcal{Q}=\left\{\overline{P_\xi^{tot}(y^\alpha|X=x^\alpha)},\overline{\mathrm{Err}^\alpha_\xi}\right\},$$
$$\alpha=+,\times,\quad x,y=0,1. \tag{144}$$

Вероятность события Ω_1 — все параметры лежат в доверительном интервале — есть

$$\Pr\{\Omega_1\}\ge 1-\sum_{\alpha=+,\times}\varepsilon^\alpha_{Err,\xi}-$$
$$-\sum_{\alpha=+,\times}\sum_{x,y=0,1}\varepsilon^\alpha_{x,y\xi}=1-\varepsilon_{\Omega_1}. \tag{145}$$

Однофотонная компонента частичной матрицы плотности Алиса–Ева, из которой формируется секретный ключ, после первого усечения, с использованием оценок параметров (138)–(143), имеет вид

$$\rho^\alpha_{XE}=|0^\alpha\rangle_{XX}\langle 0^\alpha|\otimes[\xi^\alpha_0(1-(Q^\alpha)^+)|\Phi_{0^\alpha}\rangle_Q\times$$
$$\times{}_Q\langle\Phi_{0^\alpha}|+\xi^\alpha_1(Q^\alpha)^+|\Theta_{0^\alpha}\rangle_{QQ}\langle\Theta_{0^\alpha}|]+$$
$$+|1^\alpha\rangle_{XX}\langle 1^\alpha|\otimes[\xi^\alpha_1(1-(Q^\alpha)^+)|\Phi_{1^\alpha}\rangle_{QQ}\langle\Phi_{1^\alpha}|+$$
$$+\xi^\alpha_0(Q^\alpha)^+|\Theta_{1^\alpha}\rangle_{QQ}\langle\Theta_{1^\alpha}|]. \tag{146}$$

Частичная матрица плотности Евы после первого усечения

$$\rho_E^\alpha = \big\{(1-(Q_1^\alpha)^+)[\xi_0^\alpha|\Phi_{0^\alpha}\rangle_{EE}\langle\Phi_{0^\alpha}| + \\ + \xi_1^\alpha|\Phi_{1^\alpha}\rangle_{EE}\langle\Phi_{1^\alpha}|] + (Q_1^\alpha)^+[\xi_1^\alpha|\Theta_{0^\alpha}\rangle_E \times \\ \times\ {}_E\langle\Theta_{0^\alpha}| + \xi_1^\alpha|\Theta_{1^\alpha}\rangle_{EE}\langle\Theta_{1^\alpha}|]\big\}. \quad (147)$$

Оценка числа информационных однофотонных посылок n_μ^α с учетом (138)–(143) дает

$$n_\mu^\alpha = e^{-2\mu}(2\mu)(\eta_0+\eta_1)\mathcal{Y}_1^- N_\mu^\alpha, \quad (148)$$

где N_μ^α — полное число зарегистрированных информационных посылок в базисе $\alpha = +, \times$.

Условная сглаженная энтропия вычисляется на матрице плотности для однофотонных посылок. В (148) n_μ^α — число однофотонных посылок. Второе усечение матрицы плотности возникает при вычислении условной сглаженной min-энтропии от тензорного произведения матриц плотности, с учетом (146), (147) получаем

$$H_{min}^{\varepsilon_{\Omega_1}+\varepsilon_{\Omega_2}}\left((\rho_{XE}^\alpha)^{\otimes n_\mu^\alpha}\,|\,(\rho_E^\alpha)^{\otimes n_\mu^\alpha}\right) \geq \\ \geq n_\mu^\alpha H\left(\rho_{XE}^\alpha|\rho_E^\alpha\right) - \mathrm{const}\sqrt{n_\mu^\alpha \log\left(\frac{1}{\varepsilon_{\Omega_2}}\right)}, \quad (149)$$

где

$$\varepsilon_\Omega = \varepsilon_{\Omega_1\cap\Omega_2} = \varepsilon_{\Omega_1} + \varepsilon_{\Omega_2}. \quad (150)$$

Для утечки информации при коррекции ошибок получаем

$$\mathrm{leak}^\alpha \leq N_\mu^\alpha h((Q_\mu^{tot,\alpha})^+) + \\ + \mathrm{const}\sqrt{N_\mu^\alpha \log\left(\frac{1}{\varepsilon_{\Omega_2}}\right)}. \quad (151)$$

Считаем для экономии обозначений, что длина серии для оценки различных параметров одинакова и равна N_μ. Правая граница доверительного интервала — величина $(Q_\mu^{tot,\alpha})^+$ в (151) вычисляется с использованием $\delta(N_\mu, \varepsilon_2)$, а оценки величин в (149) вычисляются с использованием $\delta(n_\mu, \varepsilon_2)$ (см. формулы (138), (139)).

Наконец, для длины ε_Ω-секретного ключа в базисе α получаем

$$\ell_{\varepsilon_\Omega}^\alpha \geq \\ \geq H_{min}^{\varepsilon_{\Omega_1}+\varepsilon_{\Omega_2}}\left((\rho_{XE}^\alpha)^{\otimes n_\mu^\alpha}\,|\,(\rho_E^\alpha)^{\otimes n_\mu^\alpha}\right) - \mathrm{leak}^\alpha \geq \\ \geq n_\mu^\alpha\left\{h(\xi_0) - \left[(1-(Q_1^\alpha)^+)h(\Phi^\alpha) + (Q_1^+)^+ h(\Theta^\alpha)\right]\right\} - \\ - N_\mu^\alpha h(Q_\mu^{tot,\alpha,+}) - \mathrm{const}\sqrt{n_\mu^\alpha \log\left(\frac{1}{\varepsilon_{\Omega_2}}\right)} - \\ - \mathrm{const}\sqrt{N_\mu^\alpha \log\left(\frac{1}{\varepsilon_{\Omega_2}}\right)}, \quad (152)$$

где

$$h(\xi_0) = -\xi_0\log(\xi_0) - \xi_1\log(\xi_1), \quad \xi_1 = 1-\xi_0, \quad (153)$$

$$h(\Theta^\alpha) = -\lambda_+(\Theta^\alpha)\log(\lambda_+(\Theta^\alpha)) + \\ + \lambda_-(\Theta^\alpha)\log(\lambda_-(\Theta^\alpha)), \quad (154)$$

$$h(\Phi^\alpha) = -\lambda_+(\Phi^\alpha)\log(\lambda_+(\Phi^\alpha)) + \\ + \lambda_-(\Phi^\alpha)\log(\lambda_-(\Phi^\alpha)). \quad (155)$$

Собственные числа вычисляются по формулам (81)–(90), где в качестве вероятностей ошибок Q^α в базисе α используются их оценки из (138)–(143) $(Q^\alpha)^+$.

Финальная длина секретного ключа по двум базисам определяется минимизацией по ненаблюдаемых скрытым параметрам, получаем

$$\ell_{\varepsilon_\Omega}^\Sigma = \min_{x\in[0,1]}\left\{\ell_{\varepsilon_\Omega}^+ + \ell_{\varepsilon_\Omega}^\times\right\}. \quad (156)$$

13. КВАНТОВЫЕ ПОБОЧНЫЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

Системы квантовой криптографии являются открытыми системами. Кроме вторжения в квантовый канал связи при передаче информационных состояний подслушиватель может детектировать побочное излучение передающей и приемной аппаратуры, а также активно зондировать состояние элементов аппаратуры через волоконную линию связи. В данном направлении имеются только отдельные разрозненные результаты [23–25], которые не учитывают все критические факторы, в том числе различную квантовую эффективность.

Критическими побочными каналами утечки информации являются следующие: электромагнитное излучение приемной и передающей аппаратуры, активное зондирование фазового модулятора и модулятора интенсивности, обратное переизлучение лавинных детекторов (back-flash radiadion) при регистрации информационных состояний. Состояния во всех перечисленных побочных каналах несут информацию о передаваемом ключе. Генерация случайных чисел, наложение импульсов напряжения на фазовый модулятор, приложение стробирующих импульсов на лавинные детекторы приводит к излучению, состояния излучения различаются при генерации 0 и 1. Поэтому регистрация состояний в побочных каналах дает дополнительную информацию о битах

передаваемого ключа. Аналогично активное зондирование фазового модулятора с последующим измерением отраженного зондирующего излучения также дает информацию о состоянии фазового модулятора, а значит, о битах ключа. При регистрации информационных состояний на приемной стороне происходит образование лавины носителей, которая при рекомбинации приводит к обратному переизлучению в линию связи. Обычно в системах квантовой криптографии используется пара лавинных детекторов, отсчет в одном детекторе интерпретируется как логический 0, во втором — как логическая 1. Поскольку характеристики детекторов всегда несколько различаются, обратное переизлучение также различается при регистрации детектором 0 и 1. Регистрация back-flash-излучения также дает дополнительную информацию о битах ключа.

Важно отметить, что в отличие от вторжения в квантовый канал связи, которое приводит к возмущению информационных состояний и ошибкам на приемной стороне, детектирование (пассивное или активное) в побочных каналах не приводит к возмущению информационных состояний и, соответственно, к ошибкам на приемной стороне. Побочные каналы утечки информации являются дополнительным информационным «бонусом» для подслушивателя. При наличии побочных каналов утечки информации фундаментальная связь между возмущением состояний и извлечением информации из них разрывается. По этой причине фундаментальные энтропийные соотношения неопределенностей [5], которые связывают возмущение состояний с утечкой информации к подслушивателю, оказываются неприменимыми.

Имеется принципиальное отличие состояний в побочных каналах от информационных состояний в квантовом канале. Перед посылкой информационных квантовых состояний, последние контролируемым образом приготавливаются на передающей станции. Иначе говоря, известно, какие состояния посылаются в канал связи, которые будут атаковаться подслушивателем. Поскольку состояния известны, это позволяет связать возмущение исходно известных состояний с утечкой информации из них. Состояния в побочных каналах, вообще говоря, неизвестны. Действительно, побочное излучение передающей и приемной аппаратуры представляет собой источник с макроскопически большим числом степеней свободы, состояния которых точно неизвестно. Все, что можно контролировать, так это интенсивность побочного излучения в разных спектральных диапазонах. Это достигается аккуратным экранированием аппаратуры. По этой причине можно считать, что спектральная функция распределения числа излученных фотонов известна.

Ситуация с состояниями в побочных каналах при активном зондировании более деликатная. Состояния при активном зондировании элементов системы полностью определяются подслушивателем, поэтому напрямую никак не контролируются легитимными пользователями.

Возникает вопрос: как учитывать побочные каналы утечки информации?

Для каналов с активным зондированием возможно только контролировать верхнюю границу интенсивности отраженных зондирующих состояний, в идеале в разных спектральных диапазонах. Уточним, что имеется в виду. Для волоконных систем квантовой криптографии существует верхняя граница интенсивности (или мощности) излучения, при которой волокно еще не начинает плавиться. Поэтому верхнюю границу по интенсивности входного зондирующего излучения можно считать известной для конкретного типа волокна (см., например, [26]). Зная максимальную интенсивность входного излучения, используя асимметричные оптические изоляторы, можно указать верхнюю границу по интенсивности (числу фотонов) выходного зондирующего излучения, которое будет доступно подслушитателю для детектирования. По этой причине далее будем считать эту границу заданной.

Таким образом, кроме информационных состояний подслушиватель имеет в своем распоряжении квантовые состояния в побочных каналах, которые могут совместно измеряться с информационными состояниями. Максимально допустимая информация, которую может получить подслушиватель, достигается на совместных коллективных измерениях информационных состояний и состояний в побочных каналах.

Перейдем к детальному описанию состояний в побочных каналах.

13.1. Побочный канал — зондирование фазового модулятора

При активном зондировании фазового модулятора подслушиватель будет иметь в своем распоряжении кроме информационных состояний еще и отраженные зондирующие состояния, которые зависят от того, в каком состоянии находится фазовый модулятор — какой логический бит кодируется, 0 или 1. В пользу подслушивателя можно считать отраженные состояния чистыми, поскольку чистые со-

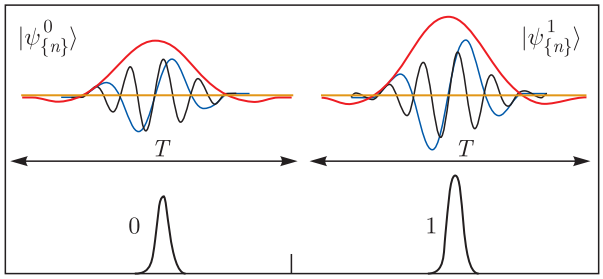

Рис. 5. Схематичное представление состояний в побочном канале, связанном с излучением аппаратуры, в каждом такте передачи квантовых состояний. $|\psi^{0,1}_{\{n\}}\rangle$ — квантовые состояния, возникающие в побочном канале при передаче 0 и 1

стояния более различимы, чем смешанные состояния. В дальнейшем будет видно, что непосредственная структура отраженных от фазового модулятора состояний непринципиальна. В формулу для длины секретного ключа будет входит лишь скалярное произведение (перекрытие) отраженных зондирующих квантовых состояний, отвечающих 0 и 1. Запишем отраженные зондирующие состояния в виде

$$\rho^{0^\alpha,1^\alpha}_{PM} = |\psi_{0^\alpha,1^\alpha}\rangle_{PM\,PM}\langle\psi_{0^\alpha,1^\alpha}|, \qquad (157)$$

здесь $|\psi_{0^\alpha,1^\alpha}\rangle_{PM}$ — отраженные зондирующие состояния для 0 и 1 в разных базисах $\alpha = +, \times$. Индекс «PM» символизирует зондирование фазового модулятора (Phase Modulator).

В окончательный ответ для длины секретного ключа будет входить лишь модуль перекрытия состояний $|_{PM}\langle\psi_{0^\alpha,1^\alpha}|\psi_{0^\alpha,1^\alpha}\rangle_{PM}|$.

13.2. Побочный канал — излучение аппаратуры

Излучение аппаратуры приводит к излучению в некотором частотном диапазоне Ω. Ширина спектра излучения Ω определяется наименьшей длительностью импульсов τ при работе управляющей электроники. Подслушиватель для различения состояний излучения в побочном канале проводит измерения в каждом такте длительностью T посылки информационных состояний (см. рис. 5). Максимальная различимость состояний возникает, если состояния в побочном канале в разных тактах не перекрываются между собой.

Для описания квантовых состояний в побочном канале необходимо выбрать набор базисных функций, по которым будет раскладываться квантовое состояние. Таким естественным набором базисных функций являются функции вытянутого сфероида. Удобно выбрать базисные функции максимально локализованными во временном окне $[0, T]$. Условие максимальной локализации состояний во временном окне $[0, T]$, фактически базисных функций $\phi_n(t, c)$, имеющих ширину спектра Ω,

$$\max_{\omega\in[0,\Omega]} \int_0^T |\phi_n(t,c)|^2(t)\,dt, \qquad (158)$$

приводит к известному интегральному уравнению [27–29]

$$\lambda_n(c)\phi_n(t,c) = \frac{1}{\pi}\int_0^T \frac{\sin[\Omega(t-t')]}{t-t'} \times \\ \times\, \phi_n(t',c)\,dt', \quad c = \Omega T. \qquad (159)$$

Решением являются функции вытянутого сфероида [27–29]. При разных n и n' функции ортогональны как на конечном $[0, T]$, так и на бесконечном $(-\infty, \infty)$ интервалах,

$$\int_0^T \phi_n(t,c)\phi_{n'}(t,c)\,dt = \lambda_n(c)\delta_{n,n'}, \\ \int_{-\infty}^{\infty} \phi_n(t,c)\phi_{n'}(t,c)\,dt = \delta_{n,n'}. \qquad (160)$$

Степень локализации во временном окне $[0, T]$ собственной функции с номером n, являющейся решением уравнения (159), дается ее собственным числом:

$$\int_0^T \phi_n^2(t,c)\,dt = \lambda_n(c). \qquad (161)$$

Для дальнейшего удобно перейти к нормированным на отрезке функциям

$$\sqrt{\lambda_n(c)}\,\varphi_n(t) = \phi_n(t,c),$$

параметр c фиксирован. Уникальным свойством волновых функций вытянутого сфероида является их поведение в зависимости от величины параметра ΩT. При значении параметра $\Omega T \gg 1$ имеется $N = \Omega T$ функций, которые локализованы во временном окне с экспоненциальной точностью [29] по параметру ΩT:

$$\lambda_n(c) \sim 1 - \frac{4\sqrt{\pi}8^n c^{n+1/2}}{n!}\,e^{-c}, \quad c = \Omega T. \qquad (162)$$

Имеются также примерно $\log(\Omega T)$ функций в переходной области номеров собственных чисел, которые стремятся к нулю. Для остальных номеров

собственные числа почти равны нулю в окне $[0,T]$. Принципиальным фактом при использовании в качестве базисных функций вытянутого сфероида является следующий результат [27]. Для любого $\varepsilon>0$ имеет место

$$\lim_{\Omega T\to\infty}\lambda_{\Omega T(1-\varepsilon)}=1,\quad \lim_{\Omega T\to\infty}\lambda_{\Omega T(1+\varepsilon)}=0. \qquad (163)$$

Неформально это означает, что имеется ΩT номеров функций, которые почти целиком локализованы во временном окне T. Для остальных номеров функции равны нулю (при этом они остаются нормированными, нормировка набирается на всем бесконечном интервале). Переходная область по номерам имеет масштаб $\sim\ln(2\pi\Omega T)$, т. е. является крайне узкой — логарифмически узкой по сравнению с ΩT.

Перейдем к построению квантового состояния.

Логика построения квантового состояния с носителем в частотной полосе Ω будет сводиться к следующему. В пользу подслушивателя будем строить состояние так, чтобы из него можно было извлечь максимум информации. Пусть полное число фотонов в состоянии равно M. Данное полное число фотонов нужно таким образом распределить по $N=\Omega T$ одночастичным состояниям, чтобы из него можно было получить максимум информации. Максимум извлекаемой информации достигается на состоянии, в котором различные ортогональные (достоверно различимые) компоненты присутствуют с равной вероятностью. Энтропия такого состояния будет максимальной, соответственно, максимальной будет информация.

В качестве базисных одночастичных состояний будем использовать функции (158) $\phi_n(\omega)$ — фурье-образ от функций в (158). Рассмотрим квантовое состояние поля, которое содержит M фотонов. Число многочастичных ортогональных векторов состояний с M фотонами, локализованных во временном окне T (таких функций $N=\Omega T$), равно числу способов размещения M фотонов по N одночастичным состояниям. Число размещений бозе-частиц по N состояниям равно [30]

$$C^M_{N-1+M}=\frac{(N-1+M)!}{(N-1)!M!}. \qquad (164)$$

Вектор состояния, отвечающий размещению M тождественных частиц по N одночастичным состояниям, имеет вид (ниже введено символическое обозначение $\{n\}$ для разбиения числа фотонов $M=n_1+n_2+\ldots+n_N$)

$$\begin{aligned}|\psi_{\{n\}}\rangle=\int\limits_{\Omega}\ldots\times\\ \times\int\limits_{\Omega}d\omega_1 d\omega_2\ldots d\omega_{n_1}d\omega_{n_1+1}d\omega_{n_1+2}\ldots d\omega_{n_2}\ldots\times\\ \times d\omega_{n_{N-1}+1}d\omega_{n_{N-1}+2}\ldots d\omega_{n_N}\times\\ \times\varphi_1(\omega_1)\varphi_1(\omega_2)\ldots\varphi_1(\omega_{n_1})\varphi_2(\omega_{n_1+1})\times\\ \times\varphi_2(\omega_{n_1+2})\ldots\varphi_2(\omega_{n_2})\ldots\varphi_N(\omega_{n_{N-1}+1})\times\\ \times\varphi_N(\omega_{n_{N-1}+2})\ldots\varphi_N(\omega_{n_N})\times\\ \times|\omega_1,\omega_2,\ldots\omega_{n_1},\omega_{n_1+1},\omega_{n_1+2},\ldots\omega_{n_2},\ldots\omega_{n_{N-1}+1},\\ \omega_{n_{N-1}+2},\ldots\omega_{n_N}\rangle. \qquad (165)\end{aligned}$$

Максимальное количество информации, которое можно извлечь при измерениях квантового состояния, достигается, если ортогональные компоненты состояний с разными разбиениями числа фотонов M присутствуют с одинаковой вероятностью. С учетом сказанного в пользу подслушивателя считаем, что состояние в побочном канале, связанном с излучением аппаратуры, имеет вид

$$\begin{aligned}\rho^{0^\alpha,1^\alpha}_{G\dot{X},GY}=\sum_{M=0}^{\infty}P^{0^\alpha,1^\alpha}_{G\dot{X},GY}\frac{1}{N}\times\\ \times\sum_{\{n\}=n_1+n_2+\ldots=M}|\psi_{\{n\}}\rangle\langle\psi_{\{n\}}|, \qquad (166)\end{aligned}$$

здесь $P^{0^\alpha,1^\alpha}_{GX,GY}$ — функция распределения по числу фотонов в побочном канале при генерации аппаратурой 0^α или 1^α в базисе α. Данные функции распределения, по сути, описывают распределение фотонов по спектру. Индексы «GX» и «GY» относятся к передающей и приемной аппаратуре соответственно.

Как будет видно ниже, полное число одночастичных ортогональных состояний N, имеющих спектр в частотной полосе Ω и максимально локализованных во временном окне T, в окончательный ответ для длины секретного ключа не входит. Длина ключа зависит лишь от функции распределения по числу фотонов $P^{0^\alpha,1^\alpha}_{GX,GY}$, последняя должна определяться экспериментально для каждой конкретной технической реализации системы.

13.3. Побочный канал — back flash однофотонных детекторов

При построении состояний в побочном канале, связанном с обратным переизлучением детекторов,

применима та же логика, что и в предыдущем разделе. Излучение детектируется подслушивателем в каждом временном такте посылки/регистрации состояний. Аналогично рассуждениям в предыдущем разделе, для квантовых состояний в этом побочном канале утечки информации получаем

$$\rho_D^{0^\alpha,1^\alpha} = \sum_{M=0}^{\infty} P_D^{0^\alpha,1^\alpha} \frac{1}{N} \times$$
$$\times \sum_{\{n\}=n_1+n_2+\ldots=M} |\psi_{\{n\}}\rangle\langle\psi_{\{n\}}|, \qquad (167)$$
$$N = \frac{(N+M-1)!}{(N-1)!M!}.$$

Индекс «D» обозначает побочный канал переизлучения детекторов. Здесь $P_D^{0^\alpha,1^\alpha}$ — функции распределения числа фотонов при переизлучении детекторов при регистрации 0^α и 1^α в базисах $\alpha = +, \times$. Вид функций распределения по числу фотонов должен определяться экспериментально для данного типа детекторов и конкретной реализации системы.

13.4. Матрицы плотности с учетом побочных каналов

При реализации Decoy State-метода используется модуляция интенсивности состояний при помощи модулятора интенсивности. Существуют реализации систем квантовой криптографии, в которых модуляция интенсивности проводится фазовым модулятором. Далее будем иметь в виду такую реализацию системы. Если модуляция интенсивности информационных состояний проводится модулятором интенсивности, то нужно добавить побочный канал утечки, связанный с модулятором интенсивности, что можно сделать методом, приведенным в работе [7].

Как отмечалось выше, секретный ключ формируется только из однофотонной компоненты состояний, достигающей приемной стороны. Информация, заключенная в многофотонных компонентах информационных состояний, в пользу подслушивателя считается ему известной.

Разумеется, что побочное излучение аппаратуры, зондирование фазового модулятора, измерение обратного переизлучения детекторов имеют место независимо от того, какая компонента информационных состояний приготавливается или регистрируется. Но поскольку информация многофотонных компонент и так считается известной подслушивателю, достаточно «подцепить» состояния в побочных каналах только к однофотонной компоненте информационных состояний.

Матрица плотности с учетом побочных каналов может быть записана в виде

$$\rho^\alpha_{XEG_XG_YPMD} = \Big\{ |0^\alpha\rangle_{XX}\langle 0^\alpha| \otimes \rho^{0^\alpha}_{G_X} \otimes \rho^{0^\alpha}_{PM} \otimes$$
$$\otimes \Big[\xi_{0^\alpha}(1-Q^\alpha)\rho^{0^\alpha}_{G_Y} \otimes \rho^{0^\alpha}_D \otimes |\Phi_0\rangle_{EE}\langle\Phi_{0^\alpha}| +$$
$$+ \xi_{1^\alpha} Q^\alpha \rho^{1^\alpha}_{G_Y} \otimes \rho^{1^\alpha}_D \otimes |\Theta_{0^\alpha}\rangle_{EE}\langle\Theta_{0^\alpha}| \Big] +$$
$$+ |1\rangle_{XX}\langle 1| \otimes \rho^{1^\alpha}_{G_X} \otimes \rho^{1^\alpha}_{PM} \otimes$$
$$\otimes \Big[\xi_{1^\alpha}(1-Q^\alpha)\rho^{1^\alpha}_{G_Y} \otimes \rho^{1^\alpha}_D \otimes |\Phi_{1^\alpha}\rangle_{EE}\langle\Phi_{1^\alpha}| +$$
$$+ \xi_{0^\alpha} Q^\alpha \rho^{0^\alpha}_{G_Y} \otimes \rho^{0^\alpha}_D \otimes |\Theta_{1^\alpha}\rangle_{EE}\langle\Theta_{1^\alpha}| \Big] \Big\}. \qquad (168)$$

Интерпретация (168) имеет простой смысл. Пусть аппаратура Алисы приготавливает состояние 0^α, это приводит к появлению квантового состояния $\rho^{0^\alpha}_{G_X}$ в побочном канале излучения аппаратуры Алисы. Кроме того, подслушиватель может активно зондировать состояние фазового модулятора, и это приводит к тому, что подслушиватель дополнительно имеет в своем распоряжении состояние $\rho^{0^\alpha}_{PM}$.

Далее, если на приемной стороне станции происходит стробирование детектора, например, 0 в базисе α, то это приводит к излучению аппаратуры, что описывается состоянием в побочном канале $\rho^{0^\alpha}_{G_Y}$. Правильное детектирование информационного состояния с вероятностью $(1-Q^\alpha)$ приводит к обратному переизлучению данного детектора в линию связи, которое дается состоянием $\rho^{0^\alpha}_D$.

Частичный след (168) по состояниям Алисы дает матрицу плотности Евы с учетом всех каналов утечки информации, находим

$$\rho^\alpha_{EG_XG_YPMD} = \Big\{ (1-Q^\alpha) \Big[\xi_{0^\alpha} \rho^{0^\alpha}_{G_X} \otimes \rho^{0^\alpha}_{PM} \otimes$$
$$\otimes \rho^{0^\alpha}_{G_Y} \otimes \rho^{0^\alpha}_D \otimes |\Phi_{0^\alpha}\rangle_{EE}\langle\Phi_{0^\alpha}| +$$
$$+ \xi_{1^\alpha} \rho^{1^\alpha}_{G_X} \otimes \rho^{1^\alpha}_{PM} \otimes \rho^{1^\alpha}_{G_Y} \otimes \rho^{1^\alpha}_D \otimes |\Phi_{1^\alpha}\rangle_{EE}\langle\Phi_{1^\alpha}| \Big] +$$
$$+ Q^\alpha \Big[\xi_{1^\alpha} \rho^{0^\alpha}_{G_X} \otimes \rho^{0^\alpha}_{PM} \otimes \rho^{1^\alpha}_{G_Y} \otimes \rho^{1^\alpha}_D \otimes |\Theta_{0^\alpha}\rangle_{EE}\langle\Theta_{0^\alpha}| +$$
$$+ \xi_{0^\alpha} \rho^{1^\alpha}_{G_X} \otimes \rho^{1^\alpha}_{PM} \otimes \rho^{0^\alpha}_{G_Y} \otimes \rho^{0^\alpha}_D \otimes$$
$$\otimes |\Theta_{1^\alpha}\rangle_{EE}\langle\Theta_{1^\alpha}| \Big] \Big\}. \qquad (169)$$

13.5. Собственные числа матриц плотности

Для вычисления сглаженной условной энтропии, фигурирующей в оценке для длины ключа, потре-

буются собственные числа матриц плотности Алисы–Евы и Евы (168), (169), находим две группы собственных чисел матрицы плотности $\rho^{\alpha}_{XEG_XG_YPMD}$:

$$\begin{gathered}[(1-Q^{\alpha})\xi_{0^{\alpha}}]\cdot\left[\frac{P^{0^{\alpha}}_{GX}}{N}\right]\cdot\left[\frac{P^{0^{\alpha}}_{GY}}{N}\right]\cdot\left[\frac{P^{0^{\alpha}}_{D}}{N}\right],\\ [(1-Q^{\alpha})\xi_{1^{\alpha}}]\cdot\left[\frac{P^{1^{\alpha}}_{GX}}{N}\right]\cdot\left[\frac{P^{1^{\alpha}}_{GY}}{N}\right]\cdot\left[\frac{P^{1^{\alpha}}_{D}}{N}\right],\end{gathered}\tag{170}$$

$$\begin{gathered}[Q^{\alpha}\xi_{1^{\alpha}}]\cdot\left[\frac{P^{0^{\alpha}}_{GX}}{N}\right]\cdot\left[\frac{P^{1^{\alpha}}_{GY}}{N}\right]\cdot\left[\frac{P^{1^{\alpha}}_{D}}{N}\right],\\ [Q^{\alpha}\xi_{0^{\alpha}}]\cdot\left[\frac{P^{1^{\alpha}}_{GX}}{N}\right]\cdot\left[\frac{P^{0^{\alpha}}_{GY}}{N}\right]\cdot\left[\frac{P^{0^{\alpha}}_{D}}{N}\right].\end{gathered}\tag{171}$$

Собственные числа матрицы плотности $\rho^{\alpha}_{EG_XG_YPMD}$ имеют вид

$$(1-Q^{\alpha})\frac{1}{N}\frac{1}{N}\frac{1}{N}\Lambda^{\pm}_{\Phi^{\alpha}},\quad Q^{\alpha}\frac{1}{N}\frac{1}{N}\frac{1}{N}\Lambda^{\pm}_{\Theta^{\alpha}},\tag{172}$$

где

$$\begin{aligned}\Lambda^{\pm}_{\Phi^{\alpha}}&=\frac{1}{2}\left\{1\pm\sqrt{1-\frac{4(\mathcal{A}_{\Phi^{\alpha}}\mathcal{B}_{\Phi^{\alpha}}-\mathcal{E}^2_{\Phi^{\alpha}})}{1-\mathcal{E}^2_{\Phi^{\alpha}}}}\right\},\\ \Lambda^{\pm}_{\Theta^{\alpha}}&=\frac{1}{2}\left\{1\pm\sqrt{1-\frac{4(\mathcal{A}_{\Theta^{\alpha}}\mathcal{B}_{\Theta^{\alpha}}-\mathcal{E}^2_{\Theta^{\alpha}})}{1-\mathcal{E}^2_{\Theta^{\alpha}}}}\right\}.\end{aligned}\tag{173}$$

Как видно из (170)–(172), собственные числа являются N^3-кратно вырожденными. Далее,

$$\begin{aligned}\mathcal{A}_{\Phi^{\alpha}}&=\xi_{0^{\alpha}}P^{0^{\alpha}}_{GX}(M_{GX})P^{0^{\alpha}}_{GY}(M_{GY})P^{0^{\alpha}}_{D}(M_D)+\\&+\xi_{1^{\alpha}}P^{1^{\alpha}}_{GX}(M_{GX})P^{1^{\alpha}}_{GY}(M_{GY})P^{1^{\alpha}}_{D}(M_D)\mathcal{E}^2_{\Phi^{\alpha}},\end{aligned}\tag{174}$$

$$\begin{aligned}\mathcal{B}_{\Phi^{\alpha}}&=\xi_{0^{\alpha}}P^{0^{\alpha}}_{GX}(M_{GX})P^{0^{\alpha}}_{GY}(M_{GY})P^{0^{\alpha}}_{D}(M_D)\mathcal{E}^2_{\Phi^{\alpha}}+\\&+\xi_{1^{\alpha}}P^{1^{\alpha}}_{GX}(M_{GX})P^{1^{\alpha}}_{GY}(M_{GY})P^{1^{\alpha}}_{D}(M_D),\end{aligned}\tag{175}$$

$$\begin{aligned}\mathcal{A}_{\Theta^{\alpha}}&=\xi_{1^{\alpha}}P^{0^{\alpha}}_{GX}(M_{GX})P^{1^{\alpha}}_{GY}(M_{GY})P^{1^{\alpha}}_{D}(M_D)+\\&+\xi_{0^{\alpha}}P^{1^{\alpha}}_{GX}(M_{GX})P^{0^{\alpha}}_{GY}(M_{GY})P^{0^{\alpha}}_{D}(M_D)\mathcal{E}^2_{\Theta^{\alpha}},\end{aligned}\tag{176}$$

$$\begin{aligned}\mathcal{B}_{\Theta^{\alpha}}&=\xi_{1^{\alpha}}P^{0^{\alpha}}_{GX}(M_{GX})P^{1^{\alpha}}_{GY}(M_{GY})P^{1^{\alpha}}_{D}(M_D)\mathcal{E}^2_{\Theta^{\alpha}}+\\&+\xi_{0^{\alpha}}P^{1^{\alpha}}_{GX}(M_{GX})P^{0^{\alpha}}_{GY}(M_{GY})P^{0^{\alpha}}_{D}(M_D),\end{aligned}\tag{177}$$

переменные M_{GX}, M_{GY}, M_D отвечают за число фотонов в функциях распределения вероятностей в побочных каналах. Также введены обозначения

$$\mathcal{E}_{\Phi^{\alpha}}=|_{PM}\langle\psi_{0^{\alpha}}|\psi_{1^{\alpha}}\rangle_{PM}|\cdot|_{E}\langle\Phi_{0^{\alpha}}|\Phi_{1^{\alpha}}\rangle_{E}|,\tag{178}$$

$$\mathcal{E}_{\Theta^{\alpha}}=|_{PM}\langle\psi_{0^{\alpha}}|\psi_{1^{\alpha}}\rangle_{PM}|\cdot|_{E}\langle\Theta_{0^{\alpha}}|\Theta_{1^{\alpha}}\rangle_{E}|.\tag{179}$$

Величины в правой части (170)–(177) зависят от наблюдаемых параметров Q^{α} и скрытых для легитимных пользователей параметров — скалярных произведений (65)–(68) векторов состояний подслушивателя. Учет конечной длины передаваемых последовательностей сводится к тому, что в формулах (168), (169) вместо значений Q^{α} и при вычислении скалярных произведений в (65)–(68) нужно использовать оценки вероятности ошибок. Фактически нужно заменить Q^{α} на $(Q^{\alpha})^{+}$.

После подстановки соответствующих значений параметров, при вычислении длины секретного ключа необходимо сделать поиск минимума по одной переменной $x\in[0,1]$ (см. формулу (78)).

14. УСЛОВНАЯ СГЛАЖЕННАЯ ЭНТРОПИЯ ОДНОФОТОННОЙ КОМПОНЕНТЫ СОСТОЯНИЙ, ОЦЕНКА ДЛИНЫ СЕКРЕТНОГО КЛЮЧА

При вычислении условной энтропии с учетом побочных каналов утечки информации будем считать, что параметры, описывающие состояния в побочных каналах, известны подслушивателю точно. Консервативно в пользу подслушивателя можно считать, что подслушиватель может иметь точную копию аппаратуры, используемой Алисой и Бобом. Имея точную копию аппаратуры, подслушиватель не ограничен во времени, чтобы, проводя длительные измерения, точно определить параметры состояний в побочных каналах. Разумеется, в реальной ситуации у подслушивателя такой возможности нет, и параметры состояний в побочных каналах также подвержены флуктуациям за счет конечной длины последовательностей. Такие флуктуации также могут быть учтены способом, который использовался для оценки параметров выше. Для того чтобы не загромождать изложение излишними выкладками, будем считать, что параметры состояний в побочных каналах известны точно.

Вычисление условной сглаженной min-энтропии для однофотонной компоненты состояний после первого и второго усечений дает

$$H_{min}^{\varepsilon_{\Omega_1}+\varepsilon_{\Omega_2}}\left((\rho_{XE})^{\otimes n_\mu^\alpha}\,|\,(\rho_E)^{\otimes n_\mu^\alpha}\right)\geq$$
$$\geq n_\mu^\alpha\left\{h(\xi_0)+[H(P_{GX}^\alpha)+H(P_{GY}^\alpha)+H(P_D^\alpha)]-\right.$$
$$\left.-\left[(1-(Q_1^\alpha)^+)h(\Phi^\alpha)+(Q_1^\alpha)^+h(\Theta^\alpha)\right]\right\}-$$
$$-\operatorname{const}\sqrt{n_\mu^\alpha\log\left(\frac{1}{\varepsilon_{\Omega_2}}\right)},\quad(180)$$

где

$$H(P_{GX}^\alpha)=-\sum_M\Big[[\xi_0^\alpha(1-Q^\alpha)+\xi_1^\alpha Q^\alpha]P_{GX}^{0^\alpha}(M)\times$$
$$\times\log\left(P_{GX}^{0^\alpha}(M)\right)+[\xi_1^\alpha(1-Q^\alpha)+\xi_0^\alpha Q^\alpha]P_{GX}^{1^\alpha}(M)\times$$
$$\times\log\left(P_{GX}^{1^\alpha}(M)\right)\Big],\quad(181)$$

$$H(P_{GY,D}^\alpha)=$$
$$=-\sum_M\Big[\xi_0^\alpha P_{GY,D}^{0^\alpha}(M)\log\left(P_{GY,D}^{0^\alpha}(M)\right)+$$
$$+\xi_1^\alpha P_{GY,D}^{1^\alpha}(M)\log\left(P_{GY,D}^{1^\alpha}(M)\right)\Big].\quad(182)$$

Далее,

$$h(\Phi^\alpha)=-\sum_{M_{GX}}\sum_{M_{GY}}\sum_{M_D}\left[\Lambda_{\Phi^\alpha}^+\log\left(\Lambda_{\Phi^\alpha}^+\right)+\right.$$
$$\left.+\,\Lambda_{\Phi^\alpha}^-\log\left(\Lambda_{\Phi^\alpha}^-\right)\right],\quad(183)$$

$$h(\Theta^\alpha)=-\sum_{M_{GX}}\sum_{M_{GY}}\sum_{M_D}\left[\Lambda_{\Theta^\alpha}^+\log\left(\Lambda_{\Theta^\alpha}^+\right)+\right.$$
$$\left.+\,\Lambda_{\Theta^\alpha}^-\log\left(\Lambda_{\Theta^\alpha}^-\right)\right]\quad(184)$$

и в (180)–(184) используются оценки параметров из (140)–(143).

Для утечки информации при коррекции ошибок в шенноновском пределе получаем

$$\operatorname{leak}^\alpha\leq N_\mu^\alpha h((Q_\mu^{tot,\alpha})^+)+$$
$$+\operatorname{const}\sqrt{N_\mu^\alpha\log\left(\frac{1}{\varepsilon_{\Omega_2}}\right)}.\quad(185)$$

Наконец, для оценки длины ε_Ω-секретного ключа в двух базисах получаем

$$\ell_\Sigma^{\varepsilon_\Omega}\geq\min_{x\in[0,1]}\left\{\sum_{\alpha=+,\times}H_{min}^{\varepsilon_{\Omega_1}+\varepsilon_{\Omega_2}}\left((\rho_{XE})^{\otimes n_\mu^\alpha}\,|\,(\rho_E)^{\otimes n_\mu^\alpha}\right)\right\}-\sum_{\alpha=+,\times}\left\{N_\mu^\alpha h((Q_\mu^{tot,\alpha})^+)-\operatorname{const}\sqrt{N_\mu^\alpha\log\left(\frac{1}{\varepsilon_{\Omega_2}}\right)}\right\}-$$
$$-\log\left(\frac{1}{\varepsilon_{corr}}\right)=n_\mu^\alpha\min_{x\in[0,1]}\left\{\sum_{\alpha=+,\times}\left\{h(\xi_0)+[H(P_{GX}^\alpha)+H(P_{GY}^\alpha)\;+\right.\right.$$
$$\left.\left.+\;H(P_D^\alpha)]-\left[(1-(Q_1^\alpha)^+)h(\Phi^\alpha)+(Q_1^\alpha)^+h(\Theta^\alpha)\right]\right\}\right\}-\sum_{\alpha=+,\times}\left\{N_\mu^\alpha h((Q_\mu^{tot,\alpha})^+)-\operatorname{const}\sqrt{N_\mu^\alpha\log\left(\frac{1}{\varepsilon_{\Omega_2}}\right)}\right\}-$$
$$-\log\left(\frac{1}{\varepsilon_{corr}}\right),\quad(186)$$

где N_μ^α — общее число зарегистрированных посылок в базисе α, n_μ^α — число однофотонных посылок в базисе α, $\varepsilon_{corr}=1/2^M$ — параметр корректности при исправлении ошибок, M — число раундов проверки по идентичности очищенных ключей. В формуле (186) считается, что проверка корректности ключей — равенства очищенных ключей Алисы и Боба после исправления ошибок проводится совместно в двух базисах.

Для иллюстрации разработанного метода приведем зависимости длины секретного ключа от длины линии связи с учетом всех факторов: неоднофотонности информационных состояний, различных квантовых эффективностей детекторов, побочных каналов утечки и конечной длины последовательности. Для того чтобы не загромождать изложение, примем в расчет только утечку информации при детектировании излучения передающей аппаратуры Алисы. Для примера будем считать, что побочное излучение подчиняется пуассоновской статистике по числу фотонов k, т. е. функция распределения при приготовлении 0 и 1 на передающей стороне имеет вид

$$P_{GX}^0(k)=e^{-M_0}\frac{M_0^k}{k!},\quad P_{GX}^1(k)=e^{-M_1}\frac{M_1^k}{k!}.\quad(187)$$

Для простоты считаем, что функции распределения в (187) не зависят от базиса.

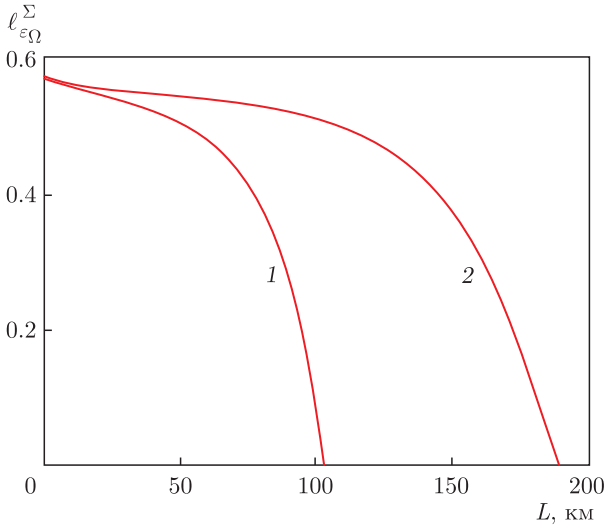

Рис. 6. Зависимости длины секретного ключа от длины линии связи. Параметры для кривых (общие): квантовые эффективности детекторов $\xi_0 = \xi_1$ ($\eta_0 = \eta_1 = 0.15$), среднее число в информационных состояниях $\mu = 0.5$, в состояниях ловушках $\nu_1 = 0.32$, $\nu_2 = 0$, вероятность темновых шумов для обоих детекторов $p_d = 10^{-6}$ отсч./строб. Для кривой *1* оценка параметров по наблюдаемым проводилась с помощью однородной оценки (134), для кривой *2* — с помощью неоднородной оценки (136). Длина последовательности n, используемой для оценок параметров, $n = 10^{10}$ (*1*), 10^6 (*2*), параметры секретности $\varepsilon_1 = \varepsilon_2 = 10^{-9}$ общие для обеих кривых. Среднее число фотонов в состояниях (см. формулу (187)) в побочном канале выбрано равным $M_0 = M_1 = 0.2$

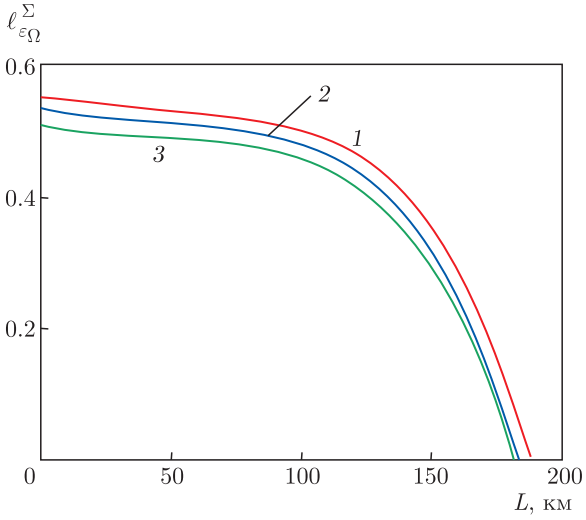

Рис. 7. Зависимости длины секретного ключа от длины линии связи. Параметры для кривых: кривая *1* — квантовые эффективности детекторов $\eta_0 = \eta_1 = 0.15$, $M_0 = 0.2$, $M_1 = 0.4$; кривая *2* — $\eta_0 = 0.1$, $\eta_1 = 0.15$, $M_0 = 0.2$, $M_1 = 0.4$; кривая *3* — $\eta_0 = \eta_1 = 0.15$, $M_0 = 0.2$, $M_1 = 0.6$. Вероятность темновых шумов одинакова для двух детекторов $p_d = 10^{-6}$, $\mu = 0.5$, $\nu_1 = 0.32$, $\nu_2 = 0$. Удельные потери в волоконной линии 0.2 дБ/км. Длина последовательности при оценке вероятностей $n = 10^6$ для всех кривых, использовалась неоднородная оценка вероятностей (136). При вычислениях использовалась минимизация длины секретного ключа с учетом конечных последовательностей и побочных каналов утечки информации

Как видно из сравнения кривых *1* и *2* на рис. 6, дальность секретного распределения ключей существенно зависит от точности оценки истинных вероятностей. При однородной оценке вероятностей длина последовательности n, по которой проводится оценка, на несколько порядков превосходит длину последовательности при неоднородной оценке.

Строго говоря, при оценке вероятностей по наблюдаемым частотам отсчетов требуется однородная оценка, однако на практике почти все системы используют нестрогую неоднородную оценку вероятностей.

На рис. 7 приведены зависимости длины секретного ключа от длины линии связи. Минимизация длины секретного ключа проводилась с использованием неоднородной оценки вероятностей по наблюдаемым частотам. При среднем числе фотонов в побочном канале, связанным с излучением передающей аппаратуры, не превышающем нескольких десятых, влияние утечки по данному каналу на длину секретного ключа является несущественным. Исходя из этого, можно получить степень экранирования аппаратуры, при которой гарантируется такой уровень интенсивности побочного излучения. Кроме того, при длинах последовательностей $n \approx 10^6$, используемых для оценки вероятностей, длина секретного ключа практически выходит на асимптотическую зависимость ($n \to \infty$). Различие квантовых эффективностей детекторов на 10–15 % также не является критичным для длины секретного ключа.

15. ПРЕДЕЛЬНЫЕ СЛУЧАИ

Интересно рассмотреть некоторые предельные случаи, которые позволят оценить характерные величины параметров состояний в побочных каналах, при которых еще возможно секретное распределение ключей. Такие оценки необходимы при экспериментальной реализации систем, например, они позволяют оценить требуемые потери в оптических изоляторах, ограничивающих мощность выходного зондирующего излучения.

15.1. Зондирование фазового модулятора Алисы

Первый пример — активное зондирование фазового модулятора. Пусть выходное зондирующее излучение представляет собой когерентное состояние. Кодирование битов ключа происходит приложением импульсов напряжения на фазовый модулятор. При приложении напряжения на фазовый модулятор происходит изменение фазы отраженного зондирующего состояния. В пользу подслушивателя будем считать, что фаза зондирующего когерентного состояния при двух состояниях фазового модулятора, отвечающих кодированию 0 и 1, изменяется на максимально возможную величину π, что соответствует максимальной различимости отраженных состояний.

В целях иллюстрации считаем, что отраженные состояния, отвечающие 0 и 1, одинаковы в разных базисах. В этом случае подслушиватель будет иметь в своем распоряжении одно из двух состояний (индекс базиса опускаем):

$$|\psi_0\rangle_{PM} = |\alpha_S\rangle_{PM}, \quad |\psi_1\rangle_{PM} = |-\alpha_S\rangle_{PM}, \quad \mu_S = |\alpha_S|^2, \tag{188}$$

где μ_S — среднее число фотонов в отраженном зондирующем когерентном состоянии, индекс «S» отвечает за побочный канал утечки информации (Side Channel).

Матрица плотности с учетом зондирования только фазового модулятора Алисы имеет вид

$$\rho_{XPM} = \frac{1}{2}\left\{|0\rangle_{X\,X}\langle 0| \otimes |\psi_0\rangle_{PM\,PM}\langle\psi_0| + |1\rangle_{X\,X}\langle 1| \otimes |\psi_1\rangle_{PM\,PM}\langle\psi_1|\right\}, \tag{189}$$

соответственно, матрица плотности Евы имеет вид

$$\rho_{PM} = \frac{1}{2}\left\{|\psi_0\rangle_{PM\,PM}\langle\psi_0| + |\psi_1\rangle_{PM\,PM}\langle\psi_1|\right\}. \tag{190}$$

Условная энтропия, отнесенная к одной посылке, принимает вид

$$H(\rho_{XPM}|\rho_{PM}) = 1 - \chi(\mathcal{E}_{PM}), \tag{191}$$

где

$$\chi(\mathcal{E}_{PM}) = -\frac{1-\epsilon}{2}\log\left(\frac{1-\epsilon}{2}\right) - \frac{1+\epsilon}{2}\log\left(\frac{1+\epsilon}{2}\right) \tag{192}$$

— величина Холево для квантового ансамбля

$$\mathcal{E}_{PM} = \left\{\frac{1}{2}|\psi_0\rangle_{PM}, \frac{1}{2}|\psi_1\rangle_{PM}\right\}. \tag{193}$$

Максимально достижимая классическая информация (192) совпадает с пропускной способностью идеального классически-квантового канала связи с входными состояниями (193) и достигается на коллективных измерениях [31].

В (192) введено обозначение для перекрытия отраженных состояний:

$$\varepsilon = |{}_{PM}\langle\psi_0|\psi_1\rangle_{PM}| = |\langle\alpha_S| - \alpha_S\rangle| = e^{-2\mu_S}.$$

Оценка длины секретного ключа в пересчете на одну зарегистрированную посылку дает

$$\ell_{PM} = 1 - \chi(\mathcal{E}_{PM}). \tag{194}$$

Для выяснения критической мощности отраженного зондирующего состояниями от фазового модулятора приведем зависимости длины секретного ключа от среднего числа фотонов в отраженном когерентном состоянии (рис. 8*a*). Как следует из рис. 8*a*, при среднем числе фотонов $\mu_S \approx 1$ секретное распределение ключей оказывается уже невозможным, длина секретного ключа $\ell_{PM} \to 0$ без вторжений в квантовый канал связи. Таким образом, для обеспечения секретности ключа требуется уровень отраженного зондирующего излучения $\mu_S \ll 0.1$ фотона. Это достигается асимметричными оптическими изоляторами.

15.2. Регистрация back-flash-излучения детекторов

Рассмотрим предельный случай, когда подслушиватель измеряет только побочное back-flash-излучение лавинных детекторов. Для простоты будем считать, что обратное переизлучение не зависит от базиса.

Матрица плотности Алиса–Ева с учетом только переизлучения детекторов на приемной станции имеет вид

$$\rho_{XED} = \frac{1}{2}\left\{|0\rangle_{X\,X}\langle 0| \otimes \rho_D^0 + |1\rangle_{X\,X}\langle 1| \otimes \rho_D^1\right\}. \tag{195}$$

Частичная матрица плотности

$$\rho_{ED} = \frac{1}{2}\left\{\rho_D^0 + \rho_D^1\right\}. \tag{196}$$

Подслушиватель имеет дело с квантовым ансамблем

$$\mathcal{E}_D = \left\{\frac{1}{2}, \rho_D^0; \frac{1}{2}, \rho_D^1\right\}.$$

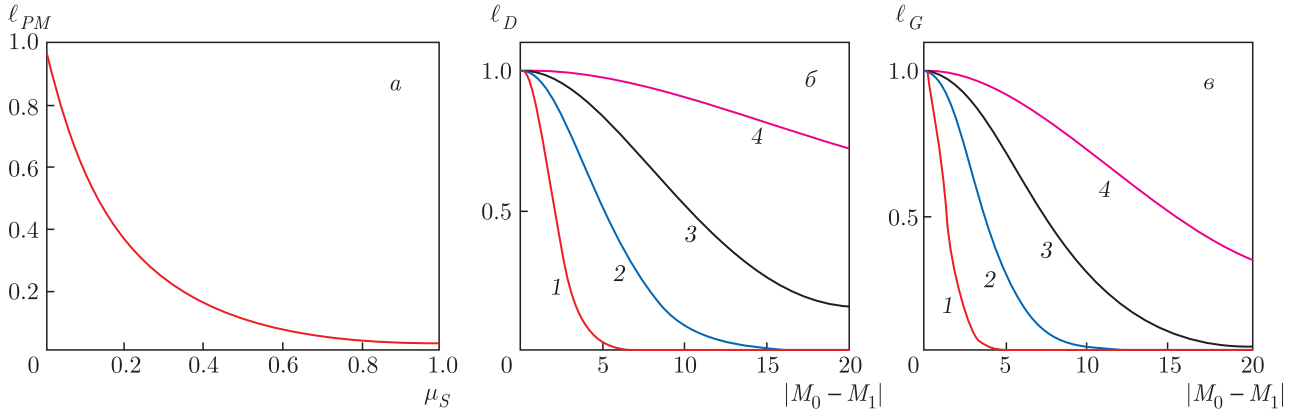

Рис. 8. Зависимости длины секретного ключа: *а*) от среднего числа фотонов μ_S в отраженном от фазового модулятора зондирующем излучении; *б*) от среднего числа фотонов при детектировании переизлучения детекторов на приемной стороне; *в*) от среднего числа фотонов при детектировании излучения передающей и приемной аппаратуры. Параметр $\sigma = 2$ (*1*), 5 (*2*), 10 (*3*), 20 (*4*). Дисперсии состояний в (204) для всех кривых рис. *б,в* выбраны одинаковыми при регистрации 0 и 1

Для подслушивателя возникает ситуация идеального квантово-классического канала побочного канала. Цель подслушивателя, имея в своем распоряжении квантовые состояния в побочном канале, ассоциированные с классическими значениями битов 0 и 1, узнать классические биты посредством измерений квантовых состояний, т. е. получить классическую информацию из квантовых состояний. Максимум классической информации, которую можно получить из квантового ансамбля $\mathcal{E}_D$, дается фундаментальной величиной Холево [31–33]. Для информации Холево (см. [33]) получаем

$$\chi(\mathcal{E}_D) = H\left(\overline{\rho_D}\right) - \frac{1}{2}H(\rho_D^0) - \frac{1}{2}H(\rho_D^1), \qquad (197)$$

где матрицы плотности берутся из (195), (196),

$$\overline{\rho_D} = \frac{\rho_D^0 + \rho_D^1}{2}. \qquad (198)$$

Вычисляя энтропии в (197), получаем

$$H\left(\overline{\rho_D}\right) = -\sum_{M=0}^{\infty} \frac{P_D^0(M) + P_D^1(M)}{2} \times$$

$$\times \log\left(\frac{P_D^0(M) + P_D^1(M)}{2}\right) - \log\left(\frac{1}{N}\right), \qquad (199)$$

$$H(\rho_D^{0,1}) = -\sum_{M=0}^{\infty} P_D^{0,1}(M) \log(P_D^{0,1}(M)) -$$

$$- \log\left(\frac{1}{N}\right). \qquad (200)$$

Учитывая, что

$$H(\rho_{XED}|\rho_{ED}) = 1 - \chi(\mathcal{E}_D), \qquad (201)$$

окончательно для величины Холево получаем

$$\chi(\mathcal{E}_D) = \frac{1}{2}\sum_{M=0}^{\infty}\left\{P_D^0(M)\log\left(\frac{2P_D^0(M)}{P_D^0(M)+P_D^1(M)}\right) + \right.$$

$$\left. + P_D^1(M)\log\left(\frac{2P_D^1(M)}{P_D^0(M)+P_D^1(M)}\right)\right\}, \qquad (202)$$

здесь $P_D^0(M)$, $P_D^1(M)$ — функции распределения числа фотонов обратного переизлучения лавинных детекторов при регистрации соответственно 0 и 1.

Напомним, что подслушиватель при детектировании обратного побочного переизлучения детекторов в линию связи не производит ошибок на приемной стороне, leak = 0.

Для оценки длины секретного ключа находим

$$\ell_D = 1 - \chi(\mathcal{E}_D). \qquad (203)$$

Отметим, что число состояний, локализованных во временном окне T каждого такта посылки информационных состояний N (слагаемое $\log(1/N)$ в (199), (200)), при вычислении условной энтропии сокращается. На рис. 8*б* представлены зависимости длины секретного ключа, если подслушиватель измеряет переизлучение лавинных детекторов. Для иллюстрации считаем, что распределение по числу фотонов при регистрации детектором 0 и 1 имеет гауссовский вид:

$$P_D^0(M) = \frac{1}{\sqrt{2\pi}\sigma_0}\exp\left(-\frac{(M-M_0)^2}{2\sigma_0^2}\right),$$
$$P_D^1(M) = \frac{1}{\sqrt{2\pi}\sigma_1}\exp\left(-\frac{(M-M_1)^2}{2\sigma_1^2}\right). \quad (204)$$

Различимость состояний ρ_D^0 и ρ_D^1 в побочном канале зависит от среднего числа фотонов $M_{0,1}$ и дисперсий $\sigma_{0,1}$, определяющих перекрытие состояний. На рис. 8*б* приведены зависимости длины секретного ключа при различных средних числах фотонов и перекрытиях состояний.

Как следует из рис. 8*б*, даже при достаточно большом среднем числе фотонов в переизлученном состоянии при перекрытии (дисперсии) состояний, различимость состояний оказывается малой. Как показывает опыт, если характеристики спектра переизлучения лавинных детекторов из одной серии мало отличаются друг от друга, то данный побочный канал не является столь критичным.

15.3. Детектирование побочного излучения от передающей и приемной аппаратуры

Рассмотрим последний частный пример, когда подслушиватель может одновременно детектировать побочное излучение аппаратуры Алисы и Боба.

Матрица плотности только с учетом побочного излучения от аппаратуры Алисы и Боба имеет вид (считаем для простоты, что излучение не зависит от базиса, поэтому индекс базиса опускаем)

$$\rho_{XEG_XG_Y} = \frac{1}{2}\left\{|0\rangle_{XX}\langle 0|\otimes\rho_{G_X}^0\otimes\rho_{G_Y}^0 + |1\rangle_{XX}\langle 1|\otimes\rho_{G_X}^1\otimes\rho_{G_Y}^1\right\}. \quad (205)$$

Частичная матрица плотности Евы

$$\rho_{EG_XG_Y} = \frac{1}{2}\left\{\rho_{G_X}^0\otimes\rho_{G_Y}^0 + \rho_{G_X}^1\otimes\rho_{G_Y}^1\right\}. \quad (206)$$

Для оценки длины секретного ключа получаем

$$\ell_G = H(\rho_{XG_XG_Y}) - H(\rho_{G_XG_Y}) = 1-\chi(\mathcal{E}_G), \quad (207)$$

$$\chi(\mathcal{E}_G) = H(\overline{\rho}_{XG_XG_Y}) - \frac{1}{2}\left[H(\rho_{G_X}^0\otimes\rho_{G_Y}^0) + H(\rho_{G_X}^1\otimes\rho_{G_Y}^1)\right], \quad (208)$$

где величина Холево для ансамбля $\mathcal{E}_G$

$$\overline{\rho}_{G_XG_Y} = \frac{1}{2}\left\{\rho_{G_X}^0\otimes\rho_{G_Y}^0 + \rho_{G_X}^1\otimes\rho_{G_Y}^1\right\}. \quad (209)$$

Вычисление энтропий дает

$$\chi(\mathcal{E}_G) = -\sum_{M_x=0}^{\infty}\sum_{M_y=0}^{\infty}\frac{P_{G_X}^0(M_x)P_{G_Y}^0(M_y)+P_{G_X}^1(M_x)P_{G_Y}^1(M_y)}{2}\times \log\left(\frac{P_{G_X}^0(M_x)P_{G_Y}^0(M_y)+P_{G_X}^1(M_x)P_{G_Y}^1(M_y)}{2}\right) + \frac{1}{2}\sum_{M=0}^{N}\left[\left(P_{G_X}^0(M)\log(P_{G_X}^0(M)) + P_{G_X}^1(M)\log(P_{G_X}^1(M))\right) + \left(P_{G_Y}^0(M)\log(P_{G_Y}^0(M)) + P_{G_Y}^1(M)\log(P_{G_Y}^1(M))\right)\right]. \quad (210)$$

Для длины ключа получаем (напомним, что подслушиватель в этом случае не производит ошибок, leak = 0)

$$\ell_G = 1-\chi(\mathcal{E}_G). \quad (211)$$

Максимум величины (210) достигается на совместных коллективных измерениях побочного излучения передающей и приемной аппаратуры, что находится за пределами современных технологий. Однако знание данной границы является принципиально важным для понимания, поскольку данная граница является фундаментальной верхней границей информации, которую позволяет получить Природа при измерении квантовых состояний в побочном канале утечки информации.

На рис. 8*в* для иллюстрации приведены результаты расчетов длины секретного ключа (211) при совместных коллективных измерениях побочного излучения передающей и приемной аппаратуры. Функции распределения по числу фотонов (210) выбраны гауссовскими, аналогично (204). Как видно из сравнения рис. 8*б* и 8*в*, появление еще одного побочного канала уменьшает длину секретного ключа. Длина ключа зависит от среднего числа фотонов в состояниях, отвечающих приготовлению и регистрации 0 и 1, и дисперсии состояний. Длина ключа обращается в нуль, когда среднее число фотонов и дисперсия оказываются одного порядка величины. В отсутствие других каналов утечки данный факт интуитивно понятен. Однако в общем случае, когда имеется несколько побочных каналов утечки, а так-

же вторжение в квантовый канал, и подслушиватель использует совместные коллективные измерения во всех каналах, ситуация не столь очевидна.

16. ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Резюмируем полученные результаты. Разработан метод, который позволяет учесть конструктивным образом все неидеальности реальных систем квантовой криптографии: нестрогую однофотонность информационных состояний, неидеальную и разную квантовую эффективность детекторов, различные побочные каналы утечки информации и конечные передаваемые последовательности.

Результат, который получен в работе, в отличие от многочисленных работ, где рассматривались отдельные разрозненные каналы утечки информации, состоит в том, что с использованием предложенного метода дано доказательство секретности ключей, которое позволяет определить максимально возможную длину секретного ключа при заданных экспериментально наблюдаемых на приемной стороне величинах, а также состояниях в побочных каналах утечки информации. Определение максимально возможной длины секретного ключа проводится минимизацией всего лишь по одному параметру, при этом совместно учитываются все каналы утечки информации.

В заключение во избежание недоразумений отметим следующее. Не нужно думать, что учет побочных каналов утечки информации переводит системы квантовой криптографии из разряда криптографических систем, где секретность ключей гарантируется фундаментальными законами квантовой механики, в разряд систем, где секретность гарантируется техническими ограничениями. Даже при наличии побочных каналов утечки информации секретность ключей по-прежнему гарантируется фундаментальными ограничениями квантовой механики на различимость состояний.

Среднее число фотонов в информационных квазиоднофотонных состояниях, выходящих из передающей станции, также достигается техническими средствами — ослаблением до нужного уровня исходного сигнала. При заданном уровне сигналов их максимально допустимая различимость диктуется квантовой механикой. Точно так же и для состояний в побочных каналах. Верхняя граница интенсивности состояний в побочных каналах достигается техническими средствами при реализации системы — экранированием аппаратуры, использованием асимметричных оптических изоляторов и т. д. При известной верхней границе интенсивности состояний существует фундаментальная верхняя граница информации, которая может быть получена при самых общих измерениях над квантовым ансамблем состояний в побочных каналах. Как было видно из рассмотрения предельных случаев детектирования только побочного излучения, данная фундаментальная граница является границей Холево [31–33].

Благодарности. Выражаем благодарность коллегам по Академии криптографии Российской Федерации за обсуждения и поддержку, а также И. М. Арбекову и С. П. Кулику за многочисленные интересные обсуждения и замечания, позволившие улучшить изложение.

ЛИТЕРАТУРА

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

2. P. Smulders, Computers & Security **9**, 53 (1990).

3. M. G. Kuhn, Technical Report, Cambridge Univ., UCAM-CL-TR-577, ISSN 1476-2986, Number 577 (2003).

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

5. M. Tomamichel, Ch. Ci Wen Lim, N. Gisin, and R. Renner, arXiv:1103.4130 v2; Nature Commun. **3**, 1 (2012).

6. C.-H. F. Fung, K. Tamaki, B. Qi, H.-K.Lo, and X. Ma, Quant. Inf. Comput. **9**, 131 (2009).

7. С. Н. Молотков, ЖЭТФ **157**, 963 (2020).

8. С. Н. Молотков, ЖЭТФ **158**, 1011 (2020).

9. H. P. Yuen, Phys. Rev. A **82**, 062304 (2010); H. P. Yuen, arXiv:1109.1051 [quant-ph]; H. P. Yuen, arXiv:1109.2675 [quant-ph]; H. P. Yuen, arXiv:1109.1066 [quant-ph].

10. R. Renner, arXiv:1209.2423 [quant-ph].

11. И. М. Арбеков, С. Н. Молотков, ЖЭТФ **152**, 62 (2017).

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

13. K. Kraus, *States, Effects and Operations*: *Fundamental Notions of Quantum Theory*, Springer Verlag (1983).

14. W. F. Stinespring, *Proc. Amer. Math. Soc.* (1955), pp. 211–216.

15. С. Н. Молотков, ЖЭТФ **153**, 895 (2018).

16. S. N. Molotkov, Laser Phys. Lett. **18**, 045202 (2021).

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

18. S. Bouceron, G. Lugosi, and P. Massart, *Concentration Inequalities. A Nonasymptotic Theory of Independence*, Clarendon Press, Oxford (2012).

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

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

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

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

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

24. M. Pereira, M. Curty, and K. Tamaki, Nature Parther Journals, Quant. Inf. **62**, 1 (2019).

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

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

27. H. J. Landau and H. O. Pollak, Bell Syst. Techn. J. **40**, 65 (1961).

28. D. Slepian and H. O. Pollak, Bell Syst. Techn. J. **40**, 43 (1961).

29. W. H. J. Fuchs, J. Math. Anal. Appl. **9**, 317 (1964).

30. Л. Д. Ландау, Е. М. Лифшиц, *Статистическая физика*, т. V, ч. I, Наука, Москва (1995).

31. A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973).

32. А. С. Холево, УМН **53**, 193 (1998).

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