Письма в ЖЭТФ, том 119, вып. 5, с. 390 – 401

О стойкости систем квантового распределения ключей типа RFI (Reference Frame Independent) к атакам активного зондирования

С. Н. Молотков[+*1)], *А. А. Щербаченко*[×°]

[+]*Академия криптографии Российской Федерации, 119331 Москва, Россия*

[*]*Институт физики твердого тела имени Ю. А. Осипьяна РАН, 142432 Черноголовка, Россия*

[×]*ООО "СФБ Лаб", 127273 Москва, Россия*

[°]*Национальный исследовательский университет "Высшая школа экономики", 101000 Москва, Россия*

Поступила в редакцию 30 ноября 2023 г.
После переработки 12 января 2024 г.
Принята к публикации 24 января 2024 г.

Приведен протокол квантового распределения ключей для волоконных систем, который не требует подстройки оптической части системы на приемной стороне, что существенно упрощает экспериментальную реализацию системы и обеспечивает устойчивую работу даже при разбалансировке оптической части системы на приемной стороне. Получено явное доказательство стойкости протокола с учетом побочных каналов утечки информации.

DOI: 10.31857/S1234567824050112, EDN: IJWXBJ

1. Введение. Системы квантовой криптографии используются для распределения ключей через волоконные линии связи и через открытое пространство. Стандартное одномодовое волокно, которое используется в волоконных линиях связи, не сохраняет состояние поляризации, поэтому обычно используется не поляризационное, а фазовое кодирование. Для открытого пространства удобнее использовать поляризационное кодирование, поскольку в открытом пространстве поляризация сохраняется.

Фундаментальные законы квантовой механики позволяют связать вероятность ошибки на приемной стороне с верхней границей утечки информации к нарушителю при его атаках на передаваемые квантовые состояния. Системы квантового распределения ключей гарантируют секретность ключей при условии, что вероятность ошибок на приемной стороне не превышают некоторой критической величины. Поскольку принципиально невозможно отличить ошибки на приемной стороне, которые возникают от неидеальностей аппаратуры, от ошибок, вызванных действиями подслушивателя, то все ошибки приходится списывать на действия нарушителя. Для устойчивой работы систем квантовой криптографии важно обеспечить устойчивую работу аппаратуры, т.е. уменьшить вероятность собственных ошибок на приемной стороне из-за неидеальностей аппаратуры.

Одним из источников ошибок при поляризационном кодировании при распределении ключей между стационарными и подвижными (между подвижными) объектами является не строго согласованная ориентация системы координат передающей и приемной станций, что приводит к рассогласованию осей поляризации и появлению ошибок на приемной стороне даже в отсутствии вторжения в канал связи. Согласование координатных осей требует постоянной подстройки взаимной ориентации передающей и приемной станций. При фазовом кодировании на передающей и приемной станциях используются интерферометры, которые должны быть одинаковыми для достижения идеальной безошибочной интерференции на приемной стороне. Для этого также требуется постоянная подстройка интерферометра на приемной стороне, что снижает скорость распределения ключей и усложняет систему.

Одной из задач теории является разработка протоколов квантового распределения ключей, которые не требуют согласования координатных осей в случае поляризационного кодирования и балансировки интерферометра в случае фазового кодирования. Один из таких протоколов был предложен в работе [1]. В [1] был также приведен набросок доказательства стойкости протокола.

Возможны различные атаки на передаваемые состояния. Индивидуальная атака – Ева атакует каждую посылку отдельно, а затем отдельно измеряет

[1)]e-mail: sergei.molotkov@gmail.com

свое квантовое состояния. Более эффективная коллективная атака – Ева атакует каждую посылку отдельно, но сохраняет свою квантовую подсистему в каждой посылке в квантовой памяти, а затем производит коллективные измерения над всей последовательностью своих состояний. На первый взгляд, еще более эффективная когерентная атака – Ева атакует сразу всю передаваемую последовательность, используя свое вспомогательное квантовое состояние большой размерности, а затем производя измерение свое квантовой системы. На сегодняшний день установлено (см., например, детали в [2–8]), что когерентная атака не является более эффективной, чем коллективная атака, они эквивалентны. Формальное доказательство основано на квантовом варианте теоремы де Финетти [8]. Неформальная причина состоит в том, что индивидуальные измерения на приемной стороне разрушают сцепленность (запутанность) состояния Евы со всеми передаваемыми состояниями Алисы, что приводит к эффективному "расцеплению" состояния на состояние в отдельных посылках. Поэтому ниже рассматривается коллективная атака Евы.

Системы квантовой криптографии являются открытыми системами, т.е. кроме атак на состояния в квантовом канале связи возможны атаки на передающую и приемную аппаратуру [2]. Часто такие атаки являются более критическими, чем атаки на состояния в канале связи, по этой причине невозможно говорить о стойкости таких систем без учета утечки информации через побочные каналы.

Целью работы является доказательство стойкости RFI протокола с фазовым кодированием с учетом побочных каналов утечки информации.

2. Описание протокола. Общая идея протокола состоит в использовании дополнительного базиса. Напомним, что в стандартном протоколе BB84 используется два базиса. Один из базисов является информационным, два других контрольными.

Состояния в информационном базисе устроены таким образом, что разбалансированность интерферометра на приемной стороне не приводит к ошибкам. Состояния в двух контрольных базисах устроены таким образом, что существует определенный инвариант, который формируется из результатов измерений при рассогласованных осях ориентации или несбалансированном интерферометре и не зависит от рассогласования осей или несбалансированности интерферометра.

В качестве базисных информационных состояний выбираются состояния $|0_Z\rangle$ и $|1_Z\rangle$, локализованные во временных окнах 1 и 2 (рис. 1). *Безошибочность*

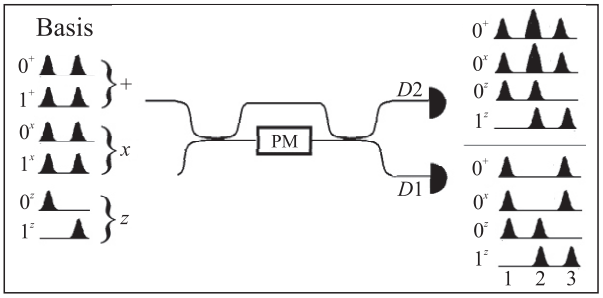

Рис. 1. Состояния, прибывающие на приемную сторону в базисах Z, $+$ и $\times$. Состояния в контрольных базисах $+$ и $\times$ детектируются во временном окне 2. В зависимости от входного состояния деструктивная интерференция для состояния $|0_+\rangle$ имеет место на детекторе $D1$, и конструктивная на детекторе $D2$. Аналогично для состояния $|0_\times\rangle$ в базисе $\times$. Выбор базиса осуществляется выбором фазы на фазовом модуляторе PM. Показана только интерференция для состояний 0 в базисах $+$ и $\times$. *Точность интерференции состояний в базисах $+$ и $\times$ зависит от балансировки интерферометра, которая определяет вероятность ошибки.* Состояния в информационном базисе Z детектируются во временных окнах 1 или 3 в детекторах $D1$ и $D2$. *Безошибочность детектирования состояний в базисе Z не зависит от точности балансировки интерферометра*

детектирования состояний в базисе Z не зависит от точности балансировки интерферометра. Данные состояния являются собственными векторами оператора σ_Z, который в базисе собственных векторов имеет вид

$$\sigma_Z = |0_Z\rangle\langle 0_Z| - |1_Z\rangle\langle 1_Z|, \tag{1}$$

с собственными числами 1 и -1.

Состояния 0 и 1 Алисы и Боба в базисах $+$ и $\times$ будем обозначать соответственно как $|\pm\rangle_{A,B}$ и $|\widetilde{\pm}\rangle_{A,B}$, которые выражаются через состояния $|0_Z\rangle$ и $|1_Z\rangle$ в базисе Z как (см. рис. 1):

$$|\pm\rangle_{A,B} = \frac{1}{\sqrt{2}}\left(|0_Z\rangle_{A,B} \pm |1_Z\rangle_{A,B}\right), \tag{2}$$

$$|\widetilde{\pm}\rangle_{A,B} = \frac{1}{\sqrt{2}}\left(|0_Z\rangle_{A,B} \pm i|1_Z\rangle_{A,B}\right). \tag{3}$$

Данные состояния являются собственными состояниями следующих операторов, которые в базисе собственных векторов имеют вид:

$$\sigma_X^{A,B} = |+\rangle_{A,B\,A,B}\langle +| - |-\rangle_{A,B\,A,B}\langle -|, \tag{4}$$

$$\sigma_Y^{A,B} = |\widetilde{+}\rangle_{A,B\,A,B}\langle \widetilde{+}| - |\widetilde{-}\rangle_{A,B\,A,B}\langle \widetilde{-}|, \tag{5}$$

с собственными значениями ± 1.

Имеется формальное соответствие между базисными состояниями $|+\rangle$ и $|-\rangle$ и базисными состояниями системы координат x и y. Неточность согласования координатных осей Алисы и Боба дается преобразованием координат

$$x' = c_{\beta/2}x + s_{\beta/2}y, \quad y' = -s_{\beta/2}x + c_{\beta/2}y, \\ c_{\beta/2} = \cos(\beta/2), \quad s_{\beta/2} = \sin(\beta/2), \tag{6}$$

где $\beta = \beta_A - \beta_B$ есть неточность установки фазы на стороне Боба (β_B) по отношению к фазе на стороне Алисы (β_A).[2)] При неточной балансировке интерферометра Боба аналогичным преобразованиям подвергаются состояния $|\pm\rangle_{A,B}$ и $|\widetilde{\pm}\rangle_{A,B}$. Соответствующие преобразования операторов $\sigma^B_{X_\beta}$ и $\sigma^B_{Y_\beta}$ имеют вид

$$\sigma^B_{X_\beta} = c_\beta\sigma^B_X + s_\beta\sigma^B_Y, \quad \sigma^B_{Y_\beta} = -s_\beta\sigma^B_X + c_\beta\sigma^B_Y. \tag{7}$$

Отметим, что в преобразование состояний (2, (3) при несогласованности интерферометров Алисы и Боба входит угол $\beta/2$, а в преобразование операторов входит угол β [3]. Для дальнейшего потребуются средние значения от произведения операторов Алисы и Боба – коррелятор $\sigma^A_{X,Y}\sigma^B_{X_\beta,Y_\beta}$ (о физической интерпретации средних значений см. ниже).

Далее считаем, что Алиса оставляет копию посланного к Бобу квантового состояния у себя как эталонную копию. Данное состояние никому, кроме Алисы, недоступно, состояние, посланное к Бобу, подвергается атаке Евы. В результате имеется совместная матрица плотности Алиса–Боб ρ_{AB}. Определим коррелятор как

$$\overline{\sigma^A_R\sigma^B_{F_\beta}} = \mathrm{Tr}_{AB}\{\rho_{AB}\sigma^A_R\sigma^B_{F_\beta}\}, \quad R,F = X,Y, \tag{8}$$

тогда, с учетом (2)–(8), прямыми вычислениями находим

$$\left(\overline{\sigma^A_X\sigma^B_{X_\beta}}\right)^2 + \left(\overline{\sigma^A_X\sigma^B_{Y_\beta}}\right)^2 + \left(\overline{\sigma^A_Y\sigma^B_{X_\beta}}\right)^2 + \left(\overline{\sigma^A_Y\sigma^B_{Y_\beta}}\right)^2 = \tag{9}$$

$$= \left(\overline{\sigma^A_X\sigma^B_X}\right)^2 + \left(\overline{\sigma^A_X\sigma^B_Y}\right)^2 + \left(\overline{\sigma^A_Y\sigma^B_X}\right)^2 + \left(\overline{\sigma^A_Y\sigma^B_Y}\right)^2.$$

Таким образом, сумма квадратов корреляторов в контрольных базисах $+$ и $\times$ не зависит от угла β рассогласования интерферометров Алисы и Боба – является инвариантом. Данный факт будет использован при анализе стойкости протокола.

3. Унитарное представление супероператора. Для учета утечки информации через побочные каналы требуется явное знание состояний подслушивателя. В [1] был приведен набросок доказательства стойкости протокола и была получена формула для длины секретного ключа, однако непрямое доказательство стойкости – без явного получения состояний нарушителя – не позволяет учесть побочные каналы утечки информации (см., например, [2]).

Действия нарушителя сводятся к действию супероператора [4], который переводит исходные квантовые состояния в выходные квантовые состояния – в общем виде в матрицы плотности. Любой супероператор унитарно представим [5] – задается действием унитарного оператора U_{BE} на исходные квантовые состояния и вспомогательное квантовое состояние нарушителя $|E\rangle$. Унитарное представление атаки позволяет получить в явном виде состояния подслушивателя. Рассмотрим унитарную атаку на информационные состояния. Действие унитарного оператора на состояния в базисе Z имеет вид

$$|\Psi(0)\rangle_{ABE} = (U_{BE}\otimes I_A)|0_Z\rangle_A\otimes|0_Z\rangle_B\otimes|E\rangle = \tag{10}$$

$$= |0_Z\rangle_A\otimes[\sqrt{1-Q}|0_Z\rangle_B\otimes|\Phi_0\rangle + \sqrt{Q}|1_Z\rangle_B\otimes|\Theta_0\rangle],$$

$$|\Psi(1)\rangle_{ABE} = (U_{BE}\otimes I_A)|1_Z\rangle_A\otimes|1_Z\rangle_B\otimes|E\rangle = \tag{11}$$

$$= |1_Z\rangle_A\otimes[\sqrt{1-Q}|1_Z\rangle_B\otimes|\Phi_1\rangle + \sqrt{Q}|0_Z\rangle_B\otimes|\Theta_1\rangle].$$

Формулы (10), (11) представляют собой разложение по базисным векторам в тензорном произведении пространств состояний Алиса–Боб–Ева. В качестве базисных векторов в пространстве Боба размерностью $\dim\mathcal{H}_B = 2$ выбрана пара ортогональных состояний $|0_Z, 1_Z\rangle_B$. Базисными состояниями в пространстве Евы выбраны состояния $|\Phi_{0,1}\rangle$, $|\Theta_{0,1}\rangle$. Размерность пространства Евы $\dim\mathcal{H}_E = 4$ (см. детали в [6, 7]), унитарность U_{BE} диктует следующие условия на скалярные произведения [6, 7],

$$\langle\Phi_0|\Phi_1\rangle = u, \quad \langle\Theta_0|\Theta_1\rangle = v, \quad \langle\Phi_{0,1}|\Theta_{0,1}\rangle = 0, \tag{12}$$

где параметры u, v – скалярные произведения остаются пока свободными.

Сделаем комментарий по выбору параметра Q.

В квантовой криптографии всегда считается, что нарушитель знает параметры системы, в том числе и квантовые эффективности детекторов. Данные знания Ева может использовать при построении своей атаки на состояния – при построении унитарного оператора.

Если квантовые эффективности детекторов одинаковы, то естественно, по соображениям симметрии использовать симметричную атаку по 0 и 1, поэтому параметр Q в (10) и (11) выбран одинаковым.

[2)] Расчет оптического тракта системы представляет стандартную задачу волоконной оптики, см., например, [3].

Если квантовые эффективности разные, то оптимальная (оптимальная в смысле, максимум утечки информации к Еве при заданных наблюдаемых ошибках в канале регистрации 0 и 1) атака, очевидно, не будет симметричной. Даже при одинаковых эффективностях, можно изначально заложить в атаку разные параметры ошибок в каналах 0 и 1, Q_0 и Q_1, а затем найти максимум утечки по Q_0 и Q_1. Такую процедуру можно проделать, например, методом работы [7], и использованием неравенства Йенсена и убедиться в оптимальности симметричной атаки. По этой причине, чтобы не усложнять выкладки техническими деталями, рассматриваем симметричную атаку.

Есть еще одно соображение в пользу симметричной атаки при равных эффективностях детекторов. Напомним, что для протокола BB84, именно, на симметричной атаке достигается нижняя граница фундаментальных энтропийных соотношений неопределенностей.

Матрица плотности для информационных посылок в базисе Z имеет вид (чтобы не загромождать выкладки, считаем, что состояния 0 и 1 посылаются равновероятно)

$$\rho_{\inf}(X) = \tfrac{1}{2}\Big(|\Psi(0)\rangle_{ABEABE}\langle\Psi(0)| + |\Psi(1)\rangle_{ABEABE}\langle\Psi(1)|\Big). \tag{13}$$

Атака на состояния в других базисах получается из (10), (11) унитарным преобразованием (2), (3) состояний. В базисе + собственных векторов оператора σ_X получаем

$$|\Psi(+)\rangle_{ABE} = (U_{BE}\otimes I_A)|+\rangle_A\otimes|+\rangle_B\otimes|E\rangle = \tag{14}$$
$$= \frac{1}{2}|+\rangle_A\otimes\Big\{|+\rangle_B\otimes\Big[\sqrt{1-Q}|\Phi_+\rangle + \sqrt{Q}|\Theta_+\rangle\Big] + |-\rangle_B\otimes\Big[\sqrt{1-Q}|\Phi_-\rangle + \sqrt{Q}|\Theta_-\rangle\Big]\Big\},$$
$$|\Psi(-)\rangle_{ABE} = (U_{BE}\otimes I_A)|-\rangle_A\otimes|-\rangle_B\otimes|E\rangle = \tag{15}$$
$$= \frac{1}{2}|-\rangle_A\otimes\Big\{|-\rangle_B\otimes\Big[\sqrt{1-Q}|\Phi_-\rangle + \sqrt{Q}|\Theta_-\rangle\Big] + |-\rangle_B\otimes\Big[\sqrt{1-Q}|\Phi_+\rangle - \sqrt{Q}|\Theta_+\rangle\Big]\Big\},$$

где

$$|\Phi_\pm\rangle = |\Phi_0\rangle \pm |\Phi_1\rangle, \quad |\Theta_\pm\rangle = |\Theta_0\rangle \pm |\Theta_1\rangle, \tag{16}$$

В базисе × собственных векторов оператора σ_Y имеем

$$|\Psi(\widetilde{+})\rangle_{ABE} = (U_{BE}\otimes I_A)|\widetilde{+}\rangle_A\otimes|\widetilde{+}\rangle_B\otimes|E\rangle = \tag{17}$$
$$= \frac{1}{2}|\widetilde{+}\rangle_A\otimes\Big\{|\widetilde{+}\rangle_B\otimes\Big[\sqrt{1-Q}|\Phi_+\rangle + i\sqrt{Q}|\Theta_-\rangle\Big] + |-\rangle_B\otimes\Big[\sqrt{1-Q}|\Phi_-\rangle + i\sqrt{Q}|\Theta_+\rangle\Big]\Big\},$$
$$|\Psi(\widetilde{-})\rangle_{ABE} = (U_{BE}\otimes I_A)|\widetilde{-}\rangle_A\otimes|\widetilde{-}\rangle_B\otimes|E\rangle = \tag{18}$$
$$= \frac{1}{2}|\widetilde{-}\rangle_A\otimes\Big\{|\widetilde{+}\rangle_B\otimes\Big[\sqrt{1-Q}|\Phi_-\rangle - i\sqrt{Q}|\Theta_+\rangle\Big] + |\widetilde{-}\rangle_B\otimes\Big[\sqrt{1-Q}|\Phi_+\rangle + i\sqrt{Q}|\Theta_-\rangle\Big]\Big\}.$$

Матрица плотности для посылок в контрольных базисах + и × имеет вид

$$\rho_{\text{contr}} = \frac{1}{2}\left(\rho_{\text{contr}}(X) + \rho_{\text{contr}}(Y)\right) = \tag{19}$$
$$= \frac{1}{2}\Big\{\frac{1}{2}\Big(|\Psi(+)\rangle_{ABEABE}\langle\Psi(+)| + |\Psi(-)\rangle_{ABEABE}\langle\Psi(-)|\Big) + \frac{1}{2}\left(|\Psi(\widetilde{+})\rangle_{ABEABE}\langle\Psi(\widetilde{+})| + |\Psi(\widetilde{-})\rangle_{ABEABE}\langle\Psi(\widetilde{-})|\right)\Big\}.$$

4. Вычисление корреляторов. В этом разделе, используя результаты предыдущих разделов, будет приведено вычисление инварианта (9).

Важно отметить, что при подсчете инварианта корреляторы вычисляются на операторах, отвечающих идеальной согласованной балансировке интерферометров Алисы и Боба ($\beta = 0$, см. формулы (9), (10)). Для корреляторов, с учетом (14)–(19), получаем

$$\overline{\sigma_X^A\sigma_X^B} = \mathrm{Tr}_{ABE}\left\{\frac{1}{2}\left(\rho_{\text{contr}}(+) + \rho_{\text{contr}}(-)\right)\sigma_X^A\sigma_X^B\right\} = (1-Q)u + Qv. \tag{20}$$

$$\overline{\sigma_Y^A\sigma_Y^B} = \mathrm{Tr}_{ABE}\left\{\frac{1}{2}\left(\rho_{\text{contr}}(\widetilde{+}) + \rho_{\text{contr}}(\widetilde{-})\right)\sigma_X^A\sigma_X^B\right\} = (1-Q)u - Qv. \tag{21}$$

Аналогично для остальных средних. Окончательно для инварианта находим

$$C(Q,u,v) = \left(\overline{\sigma_X^A\sigma_X^B}\right)^2 + \left(\overline{\sigma_Y^A\sigma_Y^B}\right)^2 = 2[(1-Q)^2u^2 + Q^2v^2]. \tag{22}$$

Данный коррелятор является инвариантом, т.е. не зависит от угла β рассогласования интерферометров. Параметры u, v пока остаются свободными, в дальнейшем будут определяться из условия максимизации утечки информации к подслушивателю (см. ниже).

5. Частичные матрицы плотности. Алиса и Боб оставляют только те посылки, в которых базисы измерений совпадали. После измерений Алисы и Боба в информационном базисе Z матрица плотности принимает вид

$$\rho_{X_A X_B E}(Z) = \tag{23}$$
$$= \frac{1}{2}|0\rangle_{X_A X_A}\langle 0| \otimes \Big\{(1-Q)|0\rangle_{X_B X_B}\langle 0| \otimes |\Phi_0\rangle\langle\Phi_0| + Q|1\rangle_{X_B X_B}\langle 1| \otimes |\Theta_0\rangle\langle\Theta_0|\Big\} +$$
$$+\frac{1}{2}|1\rangle_{X_A X_A}\langle 1| \otimes \Big\{(1-Q)|1\rangle_{X_B X_B}\langle 1| \otimes |\Phi_1\rangle\langle\Phi_1| + Q|0\rangle_{X_B X_B}\langle 0| \otimes |\Theta_1\rangle\langle\Theta_1|\Big\}.$$

Частичные матрицы плотности

$$\rho_{X_A E}(Z) = \tag{24}$$
$$= \frac{1}{2}|0\rangle_{X_A X_A}\langle 0| \otimes \{(1-Q)|\Phi_0\rangle\langle\Phi_0| + Q|\Theta_0\rangle\langle\Theta_0|\} +$$
$$+\frac{1}{2}|1\rangle_{X_A X_A}\langle 1| \otimes \{(1-Q)|\Phi_1\rangle\langle\Phi_1| + Q|\Theta_1\rangle\langle\Theta_1|\}.$$

$$\rho_E(Z) = \tag{25}$$
$$= \frac{1}{2}\Big\{(1-Q)\left[|\Phi_0\rangle\langle\Phi_0| + |\Phi_1\rangle\langle\Phi_1|\right] + Q\left[|\Theta_0\rangle\langle\Theta_0| + |\Theta_1\rangle\langle\Theta_1|\right]\Big\}.$$

$$\rho_{X_A X_B}(Z) = \tag{26}$$
$$= \frac{1}{2}(1-Q)\Big\{|0\rangle_{X_A X_A}\langle 0| \otimes |0\rangle_{X_B X_B}\langle 0| + |1\rangle_{X_A X_A}\langle 1| \otimes |1\rangle_{X_B X_B}\langle 1|\Big\} +$$
$$+\frac{1}{2}Q\Big\{|0\rangle_{X_A X_A}\langle 0| \otimes |1\rangle_{X_B X_B}\langle 1| + |1\rangle_{X_A X_A}\langle 1| \otimes |0\rangle_{X_B X_B}\langle 0|\Big\}.$$

Матрица плотности Боба

$$\rho_{X_B}(Z) = \frac{1}{2}\left\{|0\rangle_{X_B X_B}\langle 0| + |0\rangle_{X_B X_B}\langle 0|\right\}. \tag{27}$$

6. Вычисление условных энтропий. Длина секретного ключа в асимптотическом пределе длинных последовательностей определяется через условные энтропии фон Неймана. Для условной энтропии Алиса–Ева в информационном базисе Z с учетом (23)–(27) находим

$$H(X_A^Z E|E) = H(\rho_{X_A E}(Z)|\rho_E(Z)) = \tag{28}$$
$$= H(\rho_{X_A E}(Z)) - H(\rho_E(Z)) =$$
$$= 1 - \left((1-Q)h\left(\frac{1+u}{2}\right) + Qh\left(\frac{1+v}{2}\right)\right).$$

Далее, для условной энтропии Алиса–Боб в базисе Z получаем

$$H(X_A^Z X_B^Z|X_B^Z) = H(\rho_{X_A X_B}(Z)|\rho_{X_B}(Z)) = H(\rho_{X_A X_B}(Z)) - H(\rho_{X_B}(Z)) = h(Q), \tag{29}$$

где бинарная энтропийная функция Шеннона $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

7. Длина ключа. Длина секретного ключа есть разность дефицита информации Евы о битовой строке Алисы, при условии, что Ева имеет в своем распоряжении квантовую систему $(\rho(Z)_E)$, коррелированную со строкой Алисы и дефицита информации Боба о битовой строке Алисы, при условии, что Боб имеет битовую строку (X_B), коррелированную с битовой строкой Алисы (X_A) (см., детали в [8]).

$$\ell_Z = H(X_A^Z E|E) - H(X_A^Z X_B^Z|X_B^Z) = \tag{30}$$
$$= 1 - \max_{u,v,C(Q,u,v)}\left((1-Q)h\left(\frac{1+u}{2}\right) + Qh\left(\frac{1+v}{2}\right)\right) - h(Q).$$

Отметим, что в наброске доказательства [1] без детального вывода формула (30) для длины ключа была получена исходя совсем из других рассуждений. Кроме того в [1], полные зависимости длины секретного ключа, а также критическая ошибка протокола, до которой гарантируется секретное распределение ключей, не была приведена.

8. Результаты численных расчетов. Вычисление зависимости длины секретного ключа ℓ_Z требует максимизации утечки информации к подслушивателю по свободным параметрам u, v при условии, что вероятность ошибки в информационном базисе есть Q, и значение инварианта в контрольных базисах есть $C(Q,u,v)$. Инвариант как функция (u,v) представляет собой уравнение эллипса $C^*(Q,u,v) = \frac{C(Q,u,v)}{2} = (1-Q)^2u^2 + Q^2v^2$ $(0 \le C^*(Q,u,v) \le 1)$, и главными осями $(\frac{\sqrt{C^*}}{1-Q}, \frac{\sqrt{C^*}}{Q})$. Параметры u, v меняются в пределах $(0 \le |u| \le 1,\ 0 \le |v| \le 1)$.

Заметим, что при любом фиксированном значении вероятности ошибки $Q \in (0,1)$ функция $\ell_Z^Q(u,v) = 1 - \left((1-Q)h\left(\frac{1+u}{2}\right) + Qh\left(\frac{1+v}{2}\right)\right) - h(Q)$ в указанной области является выпуклой вверх, что следует из положительной определенности ее гессиана

$$\nabla^2 \ell_Z^Q = \frac{1}{\ln 2}\begin{bmatrix} \frac{1-Q}{1-u^2} & 0 \\ 0 & \frac{Q}{1-v^2} \end{bmatrix}$$

при всех возможных значениях u, v внутри единичного квадрата. Минимум функции ℓ_Z^Q ищется вдоль

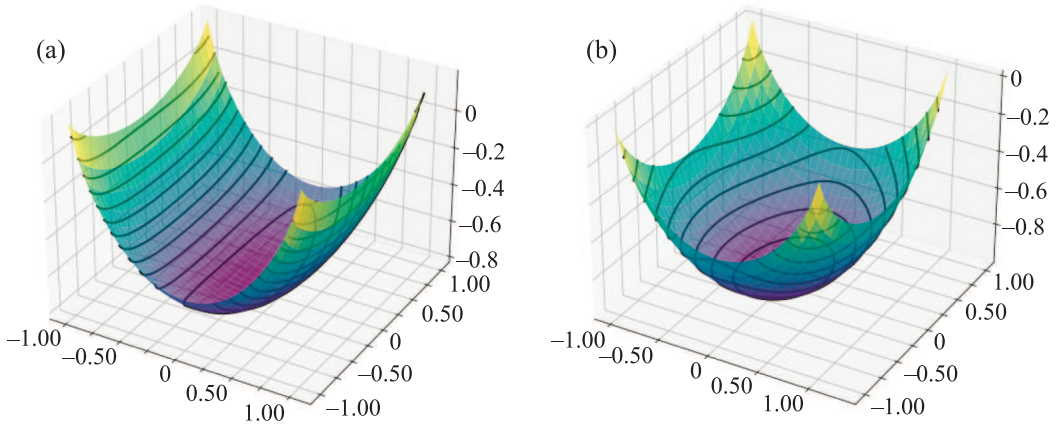

Рис. 2. (Цветной онлайн) Графики поверхности $\ell_Z^Q(u,v)$ при $Q=0.25$ (a) и $Q=0.45$ (b). Геодезические линии отвечают кривым на поверхности $C^*(Q,u,v)=C^*$, где C^* принимает значения от 0 с шагом 0.05 и не более $(1-Q)^2+Q^2$

геодезической линии $(1-Q)^2u^2+Q^2v^2=C^*$. Таким образом, в каждой точке Q решается задача выпуклой оптимизации (с нелинейным ограничением). Применим метод множителей Лагранжа, для этого рассмотрим целевую функцию вида $F_Q(u,v,\lambda)=\ell_Z^Q(u,v)-\lambda\left((1-Q)^2u^2+Q^2v^2-C^*\right)$. Найдем стационарные точки:

$$\begin{cases} \frac{\partial F_Q}{\partial u}=\frac{1-Q}{2}\log_2\left(\frac{1+u}{1-u}\right)-2\lambda(1-Q)^2u=0 \\ \frac{\partial F_Q}{\partial v}=\frac{Q}{2}\log_2\left(\frac{1+v}{1-v}\right)-2\lambda Q^2v=0 \\ \frac{\partial F_Q}{\partial\lambda}=-(1-Q)^2u^2-Q^2v^2+C^*=0 \end{cases} \Longrightarrow$$

$$\Longrightarrow \begin{cases} \log_2\left(\frac{1+u}{1-u}\right)=4\lambda(1-Q)u \\ \log_2\left(\frac{1+v}{1-v}\right)=4\lambda Qv \\ \lambda=\pm\frac{1}{4}\sqrt{\frac{\log_2\left(\frac{1+u}{1-u}\right)^2+\log_2\left(\frac{1+v}{1-v}\right)^2}{C^*}} \end{cases}.$$

Система имеет решение в точках $(u=\pm\frac{\sqrt{C^*}}{1-Q},v=0)$ и $(u=0,v=\pm\frac{\sqrt{C^*}}{Q})$. При $Q<1/2$ минимум, соответственно, будет достигаться в точке $(u=\pm\frac{\sqrt{C^*}}{1-Q},v=0)$. При подстановке получаем следующий вид функции $\ell_Z(Q)=1-(1-Q)h\left(\frac{1-Q+\sqrt{C^*}}{2(1-Q)}\right)-Q-h(Q)$.

В зависимости от значения инварианта C^*, критическая величина ошибки Q_0 достигается при различных условиях. Точный минимум кривой достигается в точке $Q_0=\frac{1-C^*}{2}$ ($Q_0=\frac{1+C^*}{2}$ соответственно при $Q>1/2$), при этом в случае $C^*\geq C_0^*$, где $C_0^*=0,608313066\ldots$ ($Q_0=0,195843467\ldots$) является решением трансцедентного уравнения $\frac{1+C_0^*}{2}-h\left(\frac{1-C_0^*}{2}\right)-h\left(\frac{(1+\sqrt{C_0^*})^2}{2(1+C_0^*)}\right)=0$ (точка, в которой функция касается оси абсцисс), данный минимум неотрицателен. При $C^*<C_0^*$ критическая величина ошибки Q_0 находится из уравнения $1-(1-Q_0)h\left(\frac{1-Q_0+\sqrt{C^*}}{2(1-Q_0)}\right)-Q_0-h(Q_0)=0$. Таким образом, имеем (при $Q<1/2$):

$$Q_0=\begin{cases} \frac{1-C^*}{2},\ C^*\geq C_0^* \\ Q_0:\ell_Z(Q_0)=0,\ C^*<C_0^* \end{cases};$$

$$\ell_Z(Q_0)=\begin{cases} \frac{1+C^*}{2}-h\left(\frac{1-C^*}{2}\right)-h\left(\frac{(1+\sqrt{C^*})^2}{2(1+C^*)}\right),\ C^*\geq C_0^* \\ 0,\ C^*<C_0^* \end{cases}$$

Отметим, что минимум функции ℓ_Z^Q существует в том числе при достижении границы единичного квадрата при $|u|=1$ (достигается при $Q\geq 1-\sqrt{C^*}$), $v=\pm\sqrt{\frac{C^*-(1-Q)^2}{Q^2}}$. Размерность пространства Евы в таком случае понижается на 1 ($\dim\mathcal{H}_E=3$) в силу того, что состояния Φ_0, Φ_1 становятся неразличимыми. При увеличении v утечка убывает вплоть до достижения вершины квадрата $|v|=1$ ($Q=\frac{1-\sqrt{2C^*-1}}{2}$). Графики поверхности $\ell_Z^Q(u,v)$ приведены на рис. 2, соответственно, зависимости длины секретного ключа как функции вероятности ошибки на приемной стороне при разных значениях инварианта $C^*(Q,u,v)$ показаны на рис. 3.

Из наблюдений за положением максимума утечки (минимума длины ключа) при различных значениях C^*, u, v можно сделать выводы об оптимальной стратегии Евы, позволяющие добиться максимальной утечки бит ключа в условиях рассогласования осей. При фиксированном значении инварианта C^* наибольшую информацию Ева получает, когда состояния $|\Theta_0\rangle$, $|\Theta_1\rangle$ являются ортогональными, что соответствует значению $v=\langle\Theta_0|\Theta_1\rangle=0$, при этом положение состояний $|\Phi_0\rangle$, $|\Phi_1\rangle$ таково, что $u=\langle\Phi_0|\Phi_1\rangle=$

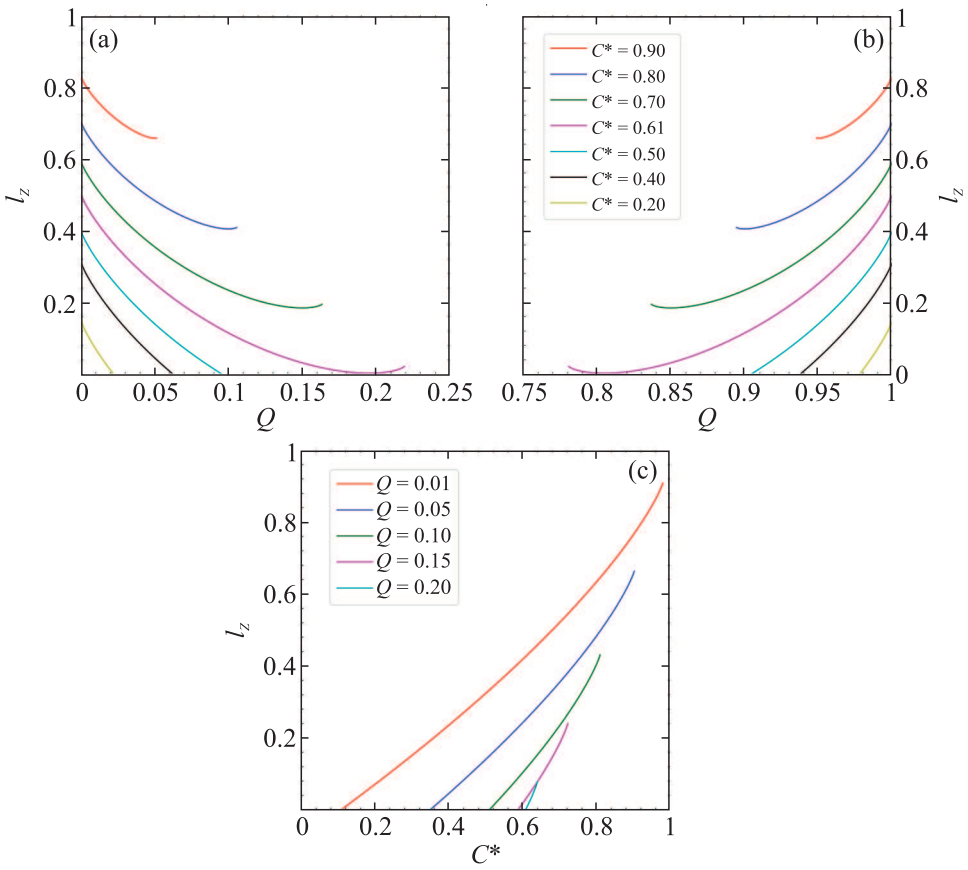

Рис. 3. (Цветной онлайн) (a), (b) – Зависимости длины секретного ключа как функции вероятности ошибки на приемной стороне при разных значениях инварианта $C^*(Q,u,v)$ (значения для кривых следующие: $C^* = 0.9$; 0.8; 0.7; $C_0^* \approx 0.61$; 0.5; 0.4; 0.2). (c) – Зависимости длины секретного ключа как функции инварианта C^* при различных значениях ошибки Q (значения вероятности ошибки Q для кривых следующие: $Q = 0.01$; 0.05; 0.1; 0.15; 0.2). Точки окончания кривых соответствуют положению на границе единичного квадрата и отвечают значениям $u^2 = 1$, $C^* = (1 - Q^2)$

$= \frac{\sqrt{C^*}}{1-Q}$. Отметим, что из результатов анализа следует, что существует такое положение осей, что при вероятности ошибки $Q = \frac{1-C^*}{2}$ Ева не может получить больше информации, варьируя значение u.

9. Связь RFI протокола со стандартным протоколом BB84 и физическая интерпретация измерений корреляторов. Протокол RFI является в определенном смысле расширением классического стандартного протокола квантового распределения ключей BB84, поэтому интересно установить связь стойкости RFI протокола со стойкостью BB84.

Как следует из (14)–(18), условная вероятность того, что послано состояние $|+\rangle_A$ и Боб зарегистрировал $|+\rangle_B$ есть

$$\Pr(+|+) = \frac{1}{4}\left|\left[\sqrt{1-Q}|\Phi_+\rangle + \sqrt{Q}|\Theta_+\rangle\right]\right|^2 = \\ = \frac{1}{2}\left(1 + (1-Q)u + Qv\right) = 1 - Q^+, \qquad (31)$$

аналогично послано состояние $|+\rangle_A$ и Боб зарегистрировал $|-\rangle_B$ есть

$$\Pr(+|-) = \frac{1}{4}\left|\left[\sqrt{1-Q}|\Phi_-\rangle + \sqrt{Q}|\Theta_-\rangle\right]\right|^2 = \\ = \frac{1}{2}\left(1 - (1-Q)u - Qv\right) = Q^+, \qquad (32)$$

где Q^+ – вероятность ошибки в базисе $+$. Далее послано состояние $|-\rangle_A$ и Боб зарегистрировал $|-\rangle_B$ есть

$$\Pr(-|-) = \frac{1}{4}\left|\left[\sqrt{1-Q}|\Phi_+\rangle - \sqrt{Q}|\Theta_+\rangle\right]\right|^2 = \\ = \frac{1}{2}\left(1 + (1-Q)u + Qv\right) = 1 - Q^+, \qquad (33)$$

аналогично послано состояние $|-\rangle_A$ и Боб зарегистрировал $|+\rangle_B$ есть

$$\Pr(-|+) = \frac{1}{4}\left|\left[\sqrt{1-Q}|\Phi_-\rangle + \sqrt{Q}|\Theta_-\rangle\right]\right|^2 = \\ = \frac{1}{2}\left(1-(1-Q)u - Qv\right) = Q^+. \qquad (34)$$

Из энтропийных соотношений неопределенностей [9–13] получаем

$$H(X_A^Z E|E) + H(X_A^+ X_B^+|X_B^+) \geq 1, \qquad (35)$$

соответственно для длины ключа для протокола BB84, с учетом (28) и (35) находим

$$\ell_Z \geq H(X_A^Z E|E) - H(X_A^Z X_B^Z|X_B^Z) \geq \qquad (36)$$
$$\geq 1 - H(X_A^+ X_B^+|X_B^+) - H(X_A^Z X_B^Z|X_B^Z) \geq$$
$$\geq 1 - h\left((1-Q)\frac{1+u}{2} + Q\frac{1+v}{2}\right) - h(Q) =$$
$$= 1 - h(Q^+) - h(Q),$$

где $Q^+ = (1-Q)\frac{1+u}{2} + Q\frac{1+v}{2}$ – ошибка в сопряженном базисе, и при переходе к последнему неравенству было использовано неравенство Йенсена для энтропии. Приведенные выкладки выше являются прямой демонстрацией известного факта для протокола BB84, который был впервые установлен в работе [14] с использованием квантовых кодов – утечка информации к Еве в прямом базисе выражается через ошибку в сопряженном базисе, или, иначе говоря, фазовая и битовые ошибки совместно определяют длину ключа.

Сравнивая выражения для длины секретного ключа для протокола RFI (30) и протокола BB84 (36), можно установить следующее.

В стандартном протоколе BB84 используется два экспериментальных параметра (точнее оценка параметров) – вероятности ошибок в классическом канале Алиса–Боб в базисе Z и в базисе $+$.

Длину секретного ключа в протоколе BB84 можно получить и через оптимизацию по этим параметрам, но с другими ограничениями. В протоколе BB84 в качестве ограничений используются наблюдаемые величины Q и Q^*, а в протоколе RFI величины Q и C.

В протоколе RFI экспериментальными параметрами являются ошибка в информационном базисе Q (точнее оценка вероятности ошибки) и оценка значения корреляторов $C(Q,u,v)$, которая зависит от вероятности ошибки в информационном базисе и двух свободных параметров u,v, по которым проводится максимизация условной энтропии.

Обсудим интерпретацию измерений корреляторов. Фактически величина коррелятора $C(Q,u,v)$ производится следующими измерениями. Пусть измерения проводятся в базисе $+$. Пусть Алиса посылает состояния 0 в базисе $+$, Боб подсчитывает число отсчетов в канале измерений $+$ (см. формулы (14)–(18)), отвечающих регистрации 0 в этом базисе. Далее подсчитывается число отсчетов в канале $-$, отвечающих регистрации 1 в этом базисе. Разность числа отсчетов в каналах 0 и 1 у Боба есть оценка среднего значения коррелятора $C(+) = \overline{|+\rangle_{AA}\langle+|(|+\rangle_{BB}\langle+| - |-\rangle_{BB}\langle-|)}$. Аналогично подсчет происходит, когда Алиса посылала 1 в базисе $+$, в этом случае определяется $C(-) = \overline{|-\rangle_{AA}\langle-|(|+\rangle_{BB}\langle+| - |-\rangle_{BB}\langle-|)}$. Разность значений $C(+) - C(-)$ дает коррелятор $C(+) - C(-) = \overline{\sigma_A^X \sigma_B^X}$. Аналогичным образом определяются остальные корреляторы.

10. Учет побочных каналов утечки информации. Квантовая криптография гарантирует безусловную секретность ключей, если учитывать только атаки на передаваемые квантовые состояния, когда подслушиватель не имеет ни прямого, ни косвенного доступа к передающей и приемной станциям. Системы квантовой криптографии являются открытыми системами, в том смысле, что подслушиватель может иметь косвенный доступ к приемо- передающей аппаратуре, используя зондирующее излучение. Обычно такие атаки называются атаками на техническую реализацию или Trojan-horse attacks [2]. Без устойчивости системы к таким атакам невозможно всерьез говорить о секретности распределяемых ключей. Все атаки на системы квантовой криптографии условно можно разделить на следующие классы:

1. Атаки непосредственно на информационные квантовые состояния в канале связи.

2. Пассивные атаки, использующие детектирование побочного электромагнитного излучения от аппаратуры приемной и передающей станций.

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

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

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

Второй класс атак связан с пассивным детектированием слабых (фактически квантовых) побочных сигналов от работы элементов приемной и передающей аппаратуры – излучения от фазовых модуляторов, модуляторов интенсивности, генераторов случайных чисел, от схемы стробирования лавинных детекторов, обратного переизлучения лавинных детекторов при их срабатывании и др.

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

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

Излучение передающей аппаратуры Алисы и активное зондирование фазового модулятора сводится к введению дополнительного квантового состояния $\rho_A^S(0)$ или $\rho_A^S(1)$, доступного Еве, которое "привязано" к квантовым состояниям Алисы $|0\rangle_{X_A}$ или $|1\rangle_{X_A}$, которые она посылает в канал связи и которое зависит от посылаемого состояния Алисы.

Состояния в побочных каналах от приемной станции зависит от того, какое состояние зарегистрировано Бобом. Если Боб зарегистрировал состояние $|0\rangle_{X_B}$, то Ева в качестве информационного бонуса будет иметь в своем распоряжении состояние $\rho_B^S(0)$, аналогично, если Боб зарегистрировал состояние $|1\rangle_{X_B}$, то Ева дополнительно получает состояние в побочном канале $\rho_B^S(1)$.

Ниже, чтобы проиллюстрировать общий подход учета побочных каналов, мы не разделяем отдельные побочные каналы, а объединяем их в общие матрицы плотности $\rho_A^S(i)$ и $\rho_B^S(i)$ $(i = 0, 1)$, которые включают как излучение аппаратуры, зондирование фазового модулятора, обратное излучение (back flash) лавинных детекторов на стороне Боба. Это не уменьшает общности рассмотрения, поскольку каждый побочный канал задается своей матрицей плотности, "суммарный" побочный канал в этом случае также задается суммарной матрицей плотности $\rho_A^S(i)$ и $\rho_B^S(i)$.

Важно отметить некоторые особенности учета побочных каналов. Побочные каналы утечки информации являются дополнительным информационным "бонусом" для Евы. Например, Ева может производить измерение только квантовых состояний в побочных каналах без вторжения в квантовый канал связи, при этом Ева не будет приводить ошибок на приемной стороне, поскольку информационные состояния (а именно, только их "видит" Боб на приемной стороне) остаются невозмущенными.

Энтропийные соотношения неопределенностей связывают ошибки на приемной стороне с утечкой информации к подслушивателю. Из-за того, что измерение состояний в побочных каналах не приводит к ошибкам, то учет побочных каналов находится за пределами энтропийных соотношений неопределенностей, и требуется прямой учет дополнительных каналов, что требует в свою очередь явного вида квантовых состояний.

В общем случае нарушитель имеет доступ к квантовому каналу связи и состояниям в побочных каналах, поэтому в более общей атаке Ева может атаковать как информационные квантовые состояния, и извлекать информацию посредством коллективных измерений сразу над состояниями во всех каналах, что будет приводить, в общем случае, к ошибкам на приемной стороне. По этой причине требуется совместный учет утечек информации по всем каналам, именно, такая ситуация рассмотрена ниже.

Поскольку задача стойкости систем квантовой криптографии с учетом побочных каналов является достаточно сложной, и, на наш взгляд, в полном объеме универсальные подходы к ее решению еще до конца не "выкристаллизовались", то существуют и опробуются различные подходы к учету утечек информации с учетом побочных каналов. Один из таких подходов развивается в работе [15] (и ссылки в ней), который основан, фактически, на очищении ЭПР пары (аналогично тому как это делалось в первой работе по RFI системам [1]) вместе состояния в побочных каналах.

В реальной практике состояния в каждом побочном канале "восстанавливаются" при "калибровке" системы. Например, исследуется отражение от фазового модулятора зондирующих состояний разной интенсивности и спектрального состава. Опре-

деляет верхняя граница интенсивности входных (и соответственно верхняя граница интенсивности отраженных состояний, которые могут быть доступны Еве), при которой еще не происходит "разрушение" системы – плавление волокна. Аналогично для других каналов. В результате такой "томографии" восстанавливается матрица плотности в каждом канале. Это входные данные для анализа стойкости. По этой причине, требуются методы, которые позволяют, явно включать в анализ матрицы плотности в побочных каналах.

Учитывая сказанное и (23)–(26), для матриц плотности для состояний в побочных каналах, получаем (считаем, что вид матриц плотности в побочных каналах установлен "калибровкой" системы, как было отмечено выше)

$$\rho_{X_A X_B ES}(Z) = \tag{37}$$

$$= \frac{1}{2}|0\rangle_{X_A X_A}\langle 0| \otimes \rho_A^S(0) \otimes \Big\{(1-Q)|0\rangle_{X_B X_B}\langle 0| \otimes \rho_B^S(0) \otimes$$

$$\otimes |\Phi_0\rangle\langle\Phi_0| + Q|1\rangle_{X_B X_B}\langle 1| \otimes \rho_B^S(1) \otimes |\Theta_0\rangle\langle\Theta_0|\Big\} +$$

$$+\frac{1}{2}|1\rangle_{X_A X_A}\langle 1| \otimes \rho_A^S(1) \otimes \Big\{(1-Q)|1\rangle_{X_B X_B}\langle 1| \otimes \rho_B^S(1) \otimes$$

$$\otimes |\Phi_1\rangle\langle\Phi_1| + Q|0\rangle_{X_B X_B}\langle 0| \otimes \rho_B^S(0) \otimes |\Theta_1\rangle\langle\Theta_1|\Big\}.$$

Далее

$$\rho_{X_A ES}(Z) = \tag{38}$$

$$= \frac{1}{2}|0\rangle_{X_A X_A}\langle 0| \otimes \rho_A^S(0) \otimes \Big\{(1-Q)\rho_B^S(0) \otimes$$

$$\otimes |\Phi_0\rangle\langle\Phi_0| + Q\rho_B^S(1) \otimes |\Theta_0\rangle\langle\Theta_0|\Big\} +$$

$$+ \frac{1}{2}|1\rangle_{X_A X_A}\langle 1| \otimes \rho_A^S(1) \otimes \Big\{(1-Q)\rho_B^S(1) \otimes$$

$$\otimes |\Phi_1\rangle\langle\Phi_1| + Q\rho_B^S(0) \otimes |\Theta_1\rangle\langle\Theta_1|\Big\}.$$

$$\rho_{ES}(Z) = \tag{39}$$

$$= \frac{1}{2}\rho_A^S(0) \otimes \Big\{(1-Q)\rho_B^S(0) \otimes |\Phi_0\rangle\langle\Phi_0| +$$

$$+ Q\rho_B^S(1) \otimes |\Theta_0\rangle\langle\Theta_0|\Big\} +$$

$$+\frac{1}{2}\rho_A^S(1) \otimes \Big\{(1-Q)\rho_B^S(1) \otimes |\Phi_1\rangle\langle\Phi_1| +$$

$$+ Q\rho_B^S(0) \otimes |\Theta_1\rangle\langle\Theta_1|\Big\}.$$

Здесь мы не конкретизируем явный вид матриц плотности, а используем общие выражения. *Явный вид матриц плотности в каждом побочном канале получается в результате специальных исследований побочных каналов для каждой конкретной реализации системы. Имеем*

$$\rho_A^S(j) = \sum_i \lambda_{Ai}(j)|\lambda_{Ai}(j)\rangle\langle\lambda_{Ai}(j)|,$$

$$\rho_B^S(j) = \sum_i \lambda_{Bi}(j)|\lambda_{Bi}(j)\rangle\langle\lambda_{Bi}(j)|, \tag{40}$$

значенние бита $j = 0, 1$.

Собственные числа матрицы плотности $\rho_{X_A ES}(Z)$

$$\frac{1}{2}(1-Q)\lambda_{Ai}(0)\lambda_{Bj}(0), \quad \frac{1}{2}(1-Q)\lambda_{Ai}(1)\lambda_{Bj}(1), \tag{41}$$

$$\frac{1}{2}Q\lambda_{Ai}(0)\lambda_{Bj}(1), \quad \frac{1}{2}Q\lambda_{Ai}(1)\lambda_{Bj}(0). \tag{42}$$

Собственные числа матрицы плотности $\rho_{ES}(Z)$

$$\Lambda^{\pm}_{ij,1-Q} = (1-Q) \times \tag{43}$$

$$\times \left(\frac{\lambda_{ij}^{00} + \lambda_{i,j}^{11} \pm \sqrt{(\lambda_{ij}^{00} + \lambda_{i,j}^{11})^2 - 4\lambda_{ij}^{00}\lambda_{i,j}^{11}(1-u^2\eta_{ij,u}^2)}}{2}\right),$$

$$\Lambda^{\pm}_{ij,Q} = Q \times \tag{44}$$

$$\times \left(\frac{\lambda_{ij}^{01} + \lambda_{i,j}^{10} \pm \sqrt{(\lambda_{ij}^{01} + \lambda_{i,j}^{10})^2 - 4\lambda_{ij}^{01}\lambda_{i,j}^{10}(1-v^2\eta_{ij,v}^2)}}{2}\right).$$

$$\lambda_{ij}^{lm} = \lambda_{Ai}(l)\lambda_{Bj}(m), \quad l, m = 0, 1. \tag{45}$$

$$\eta_{ij,u} = \langle\lambda_{Ai}(0)|\lambda_{Ai}(0)\rangle\langle\lambda_{Bi}(1)|\lambda_{Bi}(1)\rangle,$$

$$\eta_{ij,v} = |\langle\lambda_{Ai}(0)|\lambda_{Ai}(1)\rangle\langle\lambda_{Bi}(1)|\lambda_{Bi}(0)\rangle|. \tag{46}$$

11. Длина ключа с учетом побочных каналов. Длина секретного ключа с учетом побочных каналов получается аналогично разделу 7 выше, как разность условных энтропий фон Неймана, которые вычисляются на матрицах плотности (37)–(39). Используя (40)–(46), приведем выражение для длины ключа ℓ_Z^{side} в информационном базисе Z, находим

$$\ell_Z^{\text{side}} = 1 + \sum_{k=0,1}\big(\chi(\rho_A^S(k)) + \chi(\rho_B^S(k))\big) - \tag{47}$$

$$- \max_{u,v,C(Q,u,v)}\Big\{(1-Q)\sum_{i,j}\Big(\chi(\Lambda^+_{ij,1-Q}) + \chi(\Lambda^-_{ij,1-Q})\Big) +$$

$$+ Q\sum_{i,j}\Big(\chi(\Lambda^+_{ij,Q}) + \chi(\Lambda^-_{ij,Q})\Big)\Big\},$$

$$\chi(\rho_A^S(k)) = -\sum_i \lambda_{Ai}(k)\log_2(\lambda_{Ai}(k)), \tag{48}$$

$$\chi(\rho_B^S(k)) = -\sum_j \lambda_{Bj}(k)\log_2(\lambda_{Bj}(k)), \quad k=0,1,$$

$$\chi(\Lambda^{\pm}_{ij,1-Q}) = -\Lambda^{\pm}_{ij,1-Q}\log_2(\Lambda^{\pm}_{ij,1-Q}), \qquad (49)$$

$$\chi(\Lambda^{\pm}_{ij,Q}) = -\Lambda^{\pm}_{ij,Q}\log_2(\Lambda^{\pm}_{ij,Q}).$$

Отметим, что инвариант $C(Q,u,v)$ не зависит от состояний в побочных каналах.

12. Иллюстративный пример. Общие выражения (47)–(49) для длины ключа зависят от структуры состояний в побочных каналах. Интуитивно понятно, что дополнительная информация, полученная Евой из побочных каналов, должна приводить к уменьшению длины секретного ключа. Удобно привести пример, иллюстрирующий данный факт. Пусть зондирующие состояния являются чистыми

$$\rho_A^S(i) = |\mu_i\rangle_{AA}\langle\mu_i|, \quad \rho_B^S(i) = |\mu_i\rangle_{BB}\langle\mu_i|, \quad i=0,1, \qquad (50)$$

$$|\mu_{ij}\rangle = |\mu_i\rangle_A \otimes |\mu_j\rangle_B, \quad i,j=0,1,$$

$$\eta_{lm}^{ij} = {}_{AB}\langle\mu_{ij}|\mu_{lm}\rangle_{AB}, \quad l,m=0,1, \qquad (51)$$

и пусть скалярные произведения, отвечающие зондирующим состояниям для 0 и 1, одинаковы $\eta = \eta_{lm}^{ij}$. Собственные числа ρ_{X_AES} матриц плотности (37)–(39) двукратно вырождены и равны

$$\frac{1}{2}(1-Q)\left(\frac{1\pm u\eta}{2}\right), \quad \frac{1}{2}Q\left(\frac{1\pm v\eta}{2}\right). \qquad (52)$$

Для условных энтропий (28), (29), получаем

$$H(X_A^Z ES|ES) = \\ = 1 - \left((1-Q)h\left(\frac{1+u\eta}{2}\right) + Qh\left(\frac{1+v\eta}{2}\right)\right). \qquad (53)$$

Длина секретного ключа (54) становится равной

$$\ell_Z^{\text{side}} = H(X_A^Z ES|ES) - H(X_A^Z X_B^Z|X_B^Z) = \qquad (54)$$
$$= 1 - \max_{u,v,C(Q,u,v)}\left((1-Q)h\left(\frac{1+u\eta}{2}\right) + Qh\left(\frac{1+v\eta}{2}\right)\right) - h(Q).$$

Как следует из формул (30) и (54), длина ключа при утечке информации по побочным каналам в данном иллюстративном примере масштабируется – получается из (30) заменой $u\to u\eta$, $v\to v\eta$, что приводит к масштабированию кривых рис. 2. Различимость состояний в побочных каналах определяется скалярным произведением η между состояниями в побочных каналах, отвечающих 0 и 1. При $\eta=1$ состояния в побочных каналах полностью неразличимы – состояния для 0 и 1 "слипаются", поэтому не дают дополнительной информации о ключе по отношению к информации, полученной при атаке только на передаваемые состояния в квантовом канале связи. При $\eta=0$ состояния в побочных каналах, отвечающих 0 и 1, ортогональны, поэтому с достоверностью различимы. При этом Ева знает передаваемые состояния из измерений состояний в побочном канале без вторжения в квантовый канал связи, и не производя ошибок на приемной стороне. В этом случае $h\left(\frac{1+u\eta}{2}\right) = h\left(\frac{1}{2}\right) = 1$, $h\left(\frac{1+v\eta}{2}\right) = h\left(\frac{1}{2}\right) = 1$, длина секретного ключа (54) обращается в нуль $\ell_Z^{side} = 0$ даже при нулевой вероятности ошибки $Q=0$ на приемной стороне.

Действуя аналогичным образом как в разделе 8, получаем, что при $\eta \geq 1$ ($Q<1/2$) минимум достигается в точке $u = \pm\frac{\sqrt{C^*}}{\eta(1-Q)}$, $v=0$, неотрицательный минимум длины ключа при этом достигается в точке $Q_0 = \frac{1-C^*/\eta^2}{2}$ при $C^* \geq C_0^*\eta^2$.

Выражаем благодарность И. М. Арбекову, К. А. Балыгину, С. П. Кулику, А. В. Уривскому, за обсуждения и замечания, а также коллегам по Академии криптографии Российской Федерации, ИнфоТекс и СФБ Лаборатории за обсуждения и постоянную поддержку. Отдельная благодарность А. Н. Климову, который фактически инициировал данное исследование для поддержки экспериментальных работ.

Финансирование работы. Данная работа финансировалась за счет средств бюджета организаций (СНМ – ИФТТ РАН в рамках Госзадания, ААЩ – ООО "СФБ Лаб"). Никаких дополнительных грантов на проведение или руководство данным конкретным исследованием получено не было.

Конфликт интересов. Авторы не имеют конфликта интересов.

1. A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, Phys. Rev. A **82**, 012304 (2010); arXiv/quant-ph:1003.1050.
2. С. Н. Молотков, ЖЭТФ **160**, 327 (2021).
3. openedu.ru/course/kvant-cryptography.
4. K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory*, Springer Verlag, Berlin (1983).
5. W. F. Stinespring, Proc. Am. Math. Soc. **6**, 211 (1955).
6. С. Н. Молотков, А. В. Тимофеев, Письма в ЖЭТФ **85**, 632 (2007).
7. S. N. Molotkov, Laser Phys. Lett. **18**, 045202 (2021).
8. R. Renner, *Security of Quantum Key Distribution*, PhD thesis, ETH Zürich (2005); arXiv/quant-ph:0512258.
9. D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).
10. H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).

11. M. Tomamichel and R.Renner, Phys. Rev. Lett. **106**, 110506 (2011).
12. M. Tomamichel, *A Framework for Non-Asymptotic Quantum Information Theory*, PhD thesis, ETH Zürich (2012); arXiv/quant-ph:1203.2142.
13. M. Tomamichel, Ch. Ci Wen Lim, N. Gisin, and R. Renner, *Tight finite-key analysis for quantum cryptography*, Nat. Commun. **3**, 1 (2012).
14. P.Shor and J.Preskill, Phys. Rev. Lett. **85**, 441 (2000).
15. Sh. Sun, Phys. Rev. **104**, 022423 (2021).