Письма в ЖЭТФ, том 111, вып. 9, с. 608 – 614

О побочном квантово-классическом бинарном канале утечки информации с гауссовским шумом

С. Н. Молотков[1)]

Институт физики твердого тела РАН, 142432 Черноголовка, Россия

Академия криптографии Российской Федерации, 121552 Москва, Россия

Центр квантовых технологий, МГУ им. М. В. Ломоносова, 119899 Москва, Россия

Поступила в редакцию 4 апреля 2020 г.
После переработки 6 апреля 2020 г.
Принята к публикации 6 апреля 2020 г.

Детектирование побочного излучения передающей аппаратуры является дополнительным источником информации о передаваемых ключах. Детектирование побочного излучения в отличии от вторжения в квантовый канал связи не приводит к возмущению информационных состояний и ошибкам на приемной стороне. Оценка величины утечки информации по побочному каналу является принципиально необходимой для обеспечения криптографической стойкости систем квантовой криптографии. В работе приведен простой квантовый вывод величины утечки информации по побочному квантовому каналу с гауссовским шумом. Предложенный метод не ограничивается каналом с гауссовским шумом и применим для других типов побочных каналов утечки информации.

DOI: 10.31857/S1234567820090062

1. Введение. Побочные каналы утечки информации являются одним из эффективных способов получения информации, когда нет прямого доступа к передающей и приемной аппаратуре. Применительно к системам квантовой криптографии, кроме вторжения в квантовый канал связи, по которому передаются информационные квантовые состояния, подслушиватель может детектировать побочное электромагнитное излучение, связанное с работой передающей аппаратуры. Побочное излучение коррелировано с работой аппаратуры, точнее говоря, с приготовлением состояний, отвечающих логическому биту 0 и логичекому биту 1, что приводит к разному побочному излучению. Принципиальное отличие детектирования побочного излучения от атаки непосредственно на информационные состояния в квантовом канале связи, состоит в том, что детектирование побочного излучения позволяет получать информацию о передаваемых ключах и при этом не производить ошибок на приемной стороне.

Поскольку структура квантовых состояний, посылаемых с передающей станции в квантовый канал связи известна, то при атаке непосредственно на квантовые состояния в канале связи фундаментальные законы квантовой механики позволяют связать наблюдаемую ошибку на приемной стороне с верхней границей утечки информации к подслушивателю. Структура состояний в побочном канале из-за макроскопически большого числа степеней свободы аппаратуры, приводящей к побочному излучению, точно неизвестна, поэтому невозможно обойтись без модельных предположений о структуре состояний в побочном канале.

После того как побочное излучение покидает источник информации (например, передающую станцию) и достигает подслушивателя, к исходному побочному сигналу примешиваются внешние шумы, которые также имеют огромное число степеней свободы, и которые также точно неизвестны.

Далее, имея в виду приложение к квантовой криптографии, будем рассматривать бинарный случай, когда передающая аппаратура – источник информации приготавливает случайным образом 0 и 1. С формальной точки зрения первичный источник информации связан с подслушивателем через внешнюю среду, которая искажает первичный побочный сигнал. Такая связь в классическом случае означает, что источник информации связан с подслушивателем бинарным классическим каналом связи с искажениями. Из-за огромного числа степеней свободы внешней среды, наложение множества случайных независимых величин приводит к гауссовскому распределению суммы случайных величин. По этой причине, естественным приближением для такого кана-

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

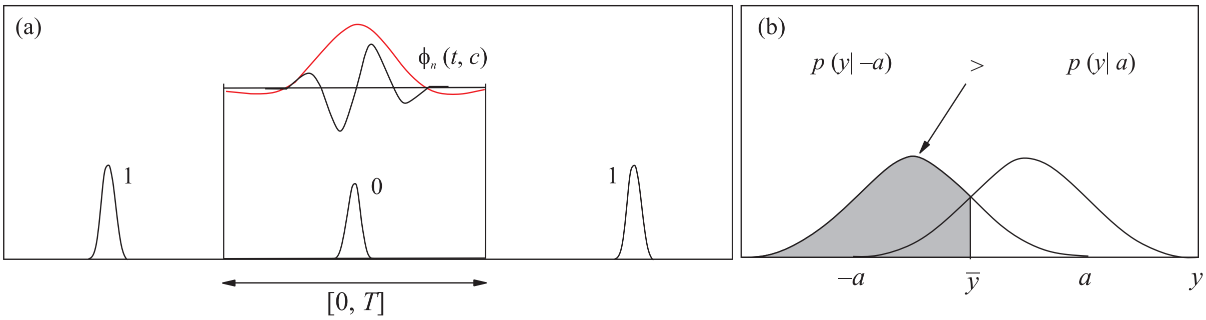

Рис. 1. (a) – Схематически показана генерация первичной информации 0 и 1. Символически показаны базичные функции вытянутого сфероида, локализованные во временном окне $[0, T]$ наблюдения подслушивателем в каждом такте сигнала в побочном канале. (b) – Условные вероятности при регистрации подслушивателем искаженных первичных сигналов, отвечающих 0 и 1. Состояния различаются по принципу максимального правдоподобия. Принимается то решение, 0 или 1, при измерении энергии сигнала, для которого вероятность при данной измеренной энергии больше. Заштрихована область энергий, при которых приинимается решение о сигнале 0

ла с искажениями является приближение бинарного аддитивного гауссовского канала с белым шумом (BAWNGC – *Binary Additive White Noise Gaussian Channel*).

Точную структуру побочного сигнала невозможно контролировать, все, что возможно контролировать, так это интенсивность сигнала в разных спектральных диапазонах. Такой контроль достигается экранированием аппаратуры. В классическом случае побочный сигнал, который достигает подслушивателя, считается классическим сигналом. Применительно к квантовой криптографии такой подход является недостаточным и неудовлетворительным, по крайней мере, двум причинам. Первая причина – искаженный сигнал при достаточном экранировании может иметь предельно низкую интенсивность, фактически является квантовым состоянием, поэтому классическое рассмотрение неприемлемо. Вторая причина – подслушиватель может проводить совместные коллективные измерения как квантового состояния в побочном канале, так и квантовых информационных состояний в квантовом канале связи. Как известно, теоретически возможный максимум информации – фундаментальная верхняя граница информации – информация Холево [1–3], которая может быть получена из ансамбля квантовых состояний, достигается на коллективных измерениях. По этим причинам требуется квантовое рассмотрение состояний в побочном канале.

Цель данной работы – дать метод описания верхней границы утечки информации по побочному каналу в зависимости от "интенсивности" состояния, более точно, среднего числа фотонов в состоянии. Рассмотрение совместной атаки на информационные квантовые состояния в квантовом канале связи и детектирование квантового побочного излучения, из-за ограниченности места будет приведено в отдельном сообщении.

Сначала кратко напомним классическую постановку задачи при детектировании побочных сигналов, а затем дадим квантовое описание, а также связь классического и квантового рассмотрения.

2. Классический случай, канал BAWGNC. Имея в виду приложение к квантовой криптографии, будем считать, что первичный источник информации – аппаратура генерирует случайным образом в каждом такте логические 0 и 1 (см. рис. 1). В реальной ситуации приготовление 0 и 1 электронной аппаратурой происходит приложением импульса напряжения разной величины на фазовый модулятор, что приводит к первичному побочному сигналу разной интенсивности. После прохождения первичного сигнала через среду спектр исходного сигнала приобретает гауссовский вид для 0 и 1 (хотя выбор гауссовского вида сигнала, как будет видно ниже, не является ограничительным, можно выбрать любой другой вид). Спектр искаженного побочного сигнала, который достигает подслушивателя, является гауссовским, центрированным в окрестности исходной энергии сигналов для 0 и 1 (см. рис. 1b). В классическом случае считается, что энергия сигнала равна квадрату амплитуды сигнала [4, 5]. Пусть амплитуда сигнала есть y, тогда наблюдаемый сигнал подслушивателем для 0 и 1 центрирован в окрестности энергий $y_0 = \sqrt{-E_s}$ и $y_1 = \sqrt{E_s}$. Начало отсчета энергии не имеет значения, важно только расстояние между энергиями сигнала для 0 и 1 (см. ниже).

Детектирование искаженного сигнала подслушивателем формализуется условными вероятностями. В результате измерений подслушиватель видит распределение энергии сигналов. Условные вероятности имеют вид

$$p(y|a) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y-a)^2}{2\sigma^2}},$$
$$p(y|-a) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y+a)^2}{2\sigma^2}}, \quad (1)$$

где для краткости введено обозначение $a = \sqrt{E_s}$, σ – дисперсии сигналов для 0 и 1 после прохождения среды, которые, для того, чтобы не загромождать выкладки, будем считать одинаковыми (обобщение на общий случай не представляет проблем). Априорные вероятности в квантовой криптографии, с которыми передающая аппаратура посылает в канал 0 и 1, считаем одинаковыми, $p(a) = p(-a) = \frac{1}{2}$.

Сигналы из-за перекрытия по спектру (см. рис. 1b) различаются подслушивателем с некоторой вероятностью ошибки. Обычно в классическом случае различение сигналов происходит по максимуму правдоподобия. При наблюдении выбирается тот сигнал, у которого вероятность больше (см. рис. 1b). Для ошибки различения получаем

$$P(\text{Err}|x=-a) = \frac{1}{\sqrt{2\pi\sigma^2}} \int\limits_{\overline{y}}^{\infty} dr e^{-\frac{(r+a)^2}{2\sigma^2}} = Q\left(\frac{\overline{y}+a}{\sigma}\right), \quad (2)$$

где $\overline{y}$ – значение, при котором условные вероятности для сигнала $y = a$ и $y = -a$ сравниваются. Аналогично для ошибки различения сигнала с $x = a$ получаем

$$P(\text{Err}|x=a) = 1 - P(\text{Err}|x=-a). \quad (3)$$

Средняя вероятность ошибки с учетом априорных вероятностей посылки сигналов, с учетом (1)–(3), равна

$$P(\text{Err}) = P(\text{Err}|x=a)p(a) + P(\text{Err}|x{=}-a)p(-a) =$$
$$= Q\left(\frac{\sqrt{E_s}}{2\sigma}\right) = Q\left(\sqrt{\frac{E_s}{N_{\text{noise}}}}\right), \quad (4)$$

где учтено, что состояния посылаются равновероятно, и в стандартных обозначениях дисперсия сигналов выражена через интенсивность шума $\sigma^2 = \frac{N_{\text{noise}}}{2}$. При стремлении $\frac{E_s}{N_{\text{noise}}} \to \infty$ – энергия исходного сигнала велика по отношению к шуму, ошибка различения состояний в побочном канале стремится к нулю – состояния различаются подслушивателем достоверно. При стремлении $\frac{E_s}{N_{\text{noise}}} \to 0$ – малая интенсивность сигнала по отношению к шуму, вероятность ошибки различения стремится к вероятности простого угадывания, в побочном канале состояния невозможно различить.

В контексте криптографии, более значимой величиной является не ошибка различения сигналов в побочном канале, а количество информации, которую подслушиватель может получить из побочного канала. Такой величиной является взаимная информация $I(X;Y)$ (см. детали в [4, 5]). Неформально взаимная информация дает информацию в битах в пересчете на каждую посылку состояний, которую может получить подслушиватель о случайной величине, принимающей значения $x = -a, a$, когда подслушиватель имеет доступ к случайной величине y с распределениями (1). С учетом (1) для взаимной информации получаем

$$I(X;Y) = \int \sum_{x=-a,a} p(x,y) \log\left(\frac{p(x,y)}{p(x)p(y)}\right) dy =$$
$$= \int \sum_{x=-a,a} p(y|x)p(x) \log\left(\frac{p(y|x)}{\sum_{x'} p(y|x')p(x')}\right) dy. \quad (5)$$

При равновероятном распределении 0 и 1 получаем

$$I(X;Y) = \frac{1}{2} \int dy \left\{ p(y|0) \log\left(\frac{2p(y|0)}{p(y|0)+p(y|1)}\right) + \right.$$
$$\left. + p(y|1) \log\left(\frac{2p(y|1)}{p(y|0)+p(y|1)}\right) \right\}. \quad (6)$$

Формулы (5), (6) дают утечку информации для классических сигналов. Состояния в побочном канале могут иметь предельно низкую интенсивность, по этой причине классическое описание становится неприемлемым. Кроме того, в контексте утечки информации в квантовой криптографии, кроме побочных каналов, имеется канал утечки при атаке на квантовые информационные состояния в квантовом канале. Для этих состояний используется квантовое описание. Поскольку подслушиватель может использовать совместную атаку на информационные состояния и состояния в побочном канале, то необходимо иметь квантовое описание утечки информации в побочном канале.

3. Постановка задачи в квантовом случае. 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. Подслушиватель измеряет состояния во временном окне в каждом такте (см. рис. 1a). Считаем, что длительность τ первичного состояния в аппаратуре в каждом такте существенно меньше длительности такта T, $\tau \ll T$. Применительно к системам квантовой криптографии, это именно так, поскольку харак-

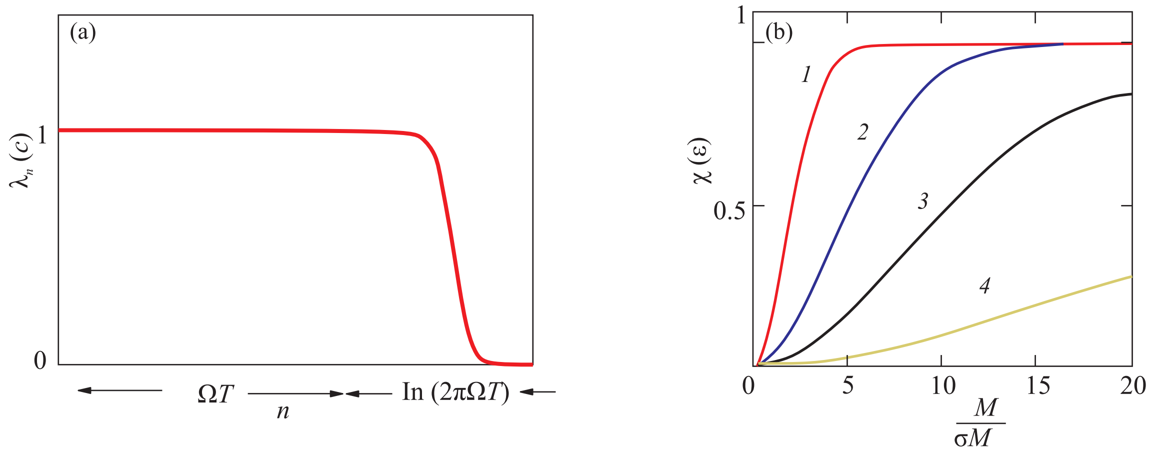

Рис. 2. (a) – Схематически показана степень локализации базисных функций вытянутого сфероида (8), (9) во временном окне наблюдения $[0, T]$ в зависимости от параметра ΩT. (b) – Величина утечки информации по побочному каналу в битах в пересчете на один такт как функция отношения $\frac{M}{\sigma_M}$ при различных отношениях "сигнал-шум" $\frac{\overline{M}}{\sigma_M}$ – среднего числа фотонов к дисперсии. Параметр $\frac{\overline{M}}{\sigma_M}$ для кривых *1–4* следующий: *1* – 0.5; *2* – 0.2; *3* – 0.1; *4* – 0.05

терные времена $\tau \approx 10^{-9}$ с, а $1/T \approx 10 \div 100$ МГц ($\tau/T \approx 10^{-1} \div 10^{-2}$). Удобно ввести характерную ширину спектра первичного состояния $\Omega = \frac{1}{\tau}$, т.е. $\Omega T \gg 1$. Удобно выбрать базисные функции максимально локализованными во временном окне $[0, T]$. Условие максимальной локализации сигнала во временном окне $[0, T]$

$$\max_{\omega\in[0,\Omega]} \int_0^T x^2(t)dt, \tag{7}$$

приводит к известному интегральному уравнению для (см. детали в [6–8])

$$\lambda_n(c)\phi_n(t,c) = \frac{1}{\pi}\int\limits_0^T \frac{\sin[\Omega(t-t')]}{t-t'}\varphi_n(t',c)dt', \;\; 2c = \Omega T. \tag{8}$$

Решением являются функции вытянутого сфероида [6–8]. При разных n и n' функции ортогональны как на конечном $[0, T]$, так и на бесконечном $(-\infty, \infty)$ интервалах,

$$\begin{gathered}\int_0^T \phi_n(t,c)\phi_{n'}(t,c)dt = \lambda_n(c)\delta_{n,n'},\\ \int_{-\infty}^{\infty} \phi_n(t,c)\phi_{n'}(t,c)dt = \delta_{n,n'}.\end{gathered} \tag{9}$$

Степень локализации во временном окне $[0, T]$ (6) собственной функции (9) с номером n уравнения (8) дается ее собственным числом

$$\int_0^T \phi_n^2(t,c)dt = \lambda_n(c). \tag{10}$$

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 субэкспоненциальной точностью [7] по параметру ΩT

$$\lambda_n(c) \sim 1 - \frac{4\sqrt{\pi}8^n c^{n+\frac{1}{2}}}{n!}e^{-c}, \quad c = \Omega \cdot T. \tag{11}$$

Имеется $N = \Omega T$ функций с вероятностью единица, локализованных в окне $[0, T]$, примерно $\log(\Omega T)$ функций в переходной области, остальные почти равны нулю в окне $[0, T]$. Принципиальным фактом при использовании в качестве базисных функций вытянутого сфероида является следующий результат [6–8]. Для любого $\varepsilon > 0$ имеет место

$$\lim_{\Omega T\to\infty} \lambda_{\Omega T(1-\varepsilon)} = 1, \quad \lim_{\Omega T\to\infty} \lambda_{\Omega T(1+\varepsilon)} = 0. \tag{12}$$

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 (см. рис. 2a).

4. Побочный бинарный квантово-классический канал с гауссовским шумом. В качестве базисных одночастичных состояний будем использовать функции (9), (10), $\varphi_n(\omega)$ фурье-образ от (9). 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 [9]

$$C^M_{N-1+M} = \frac{(N-1+M)!}{(N-1)!M!}. \tag{13}$$

Отметим, что бозе-статистика возникает в различных задачах квантовой криптографии, например, при реализации квантовых генераторах случаныйных чисел (см. подробности в [10]).

Вектор состояния, отвечающий размещению M тождественных частиц по N одночастичным состояниям – разбиению числа $n_1 + n_2 + \ldots + n_N = M$, имеет вид

$$|\Phi_{n_1,n_2,\ldots n_N}\rangle = \tag{14}$$

$$= \int_\Omega \ldots \int_\Omega d\omega_1 d\omega_2 \ldots d\omega_{n_1} \ldots d\omega_{n_1+1} d\omega_{n_1+2} \ldots d\omega_{n_2},$$
$$d\omega_{n_{N-1}+1} d\omega_{n_{N-1}+2} \ldots d\omega_{n_N}$$
$$\varphi_1(\omega_1)\varphi_1(\omega_2)\ldots\varphi_1(\omega_{n_1})\varphi_2(\omega_{n_1+1})\varphi_2(\omega_{n_1+2})\ldots$$
$$\varphi_2(\omega_{n_2})\ldots\varphi_N(\omega_{n_{N-1}+1})\varphi_N(\omega_{n_{N-1}+2})\ldots\varphi_N(\omega_{n_N})$$
$$|\omega_1, \omega_2, \ldots \omega_{n_1}, \ldots \omega_{n_1+1}, \omega_{n_1+2}, \ldots \omega_{n_2},$$
$$\omega_{n_{N-1}+1}, \omega_{n_{N-1}+2}, \ldots \omega_{n_N}\rangle.$$

После прохождения через среду – максимальная энтропия достигается в том случае, когда подслушивателю доступны все C^M_{N-1+M} ортогональных различимых состояний равновероятно – все состояния с данным числом фотонов M равновероятны – аналог белого шума.

Измерение над квантовыми состояниями, позволяющее различить все ортогональные состояния, локализованные во временном окне $[0, T]$, дается следующим разложением единицы

$$I_{N,M} = \sum_{n_1+n_2+\ldots n_N=M} \mathcal{P}_T(n_1, n_2, \ldots n_N) + I^\perp_{N,M},$$
$$I^\perp_{N,M} = \sum_{n_1+n_2+\ldots n_N=M} \mathcal{P}_\perp(n_1, n_2, \ldots n_N), \tag{15}$$

где $\mathcal{P}_T(n_1, n_2, \ldots n_N) = |\Phi_{n_1,n_2,\ldots n_N}\rangle\langle\Phi_{n_1,n_2,\ldots n_N}|$ – проектор на квантовое состояние, локализованное во временном окне $[0, T]$, и $I^\perp_{N,M}$ в (15) – дополнение до полного пространства состояний на всей временной оси, $\mathcal{P}_\perp(n_1, n_2, \ldots n_N) = |\perp_{n_1,n_2,\ldots n_N}\rangle\langle\perp_{n_1,n_2,\ldots n_N}|$ – проектор на состояния, описывающие хвосты волновых функций вытянутого сфероида вне окна $[0, T]$. Для вероятности исходов с учетом (13)–(15) получаем

$$P_T(n_1, n_2, \ldots n_N) =$$
$$= \mathrm{Tr}\{\mathcal{P}_T(n_1, n_2, \ldots n_N)\rho(N, M)\} =$$
$$= \frac{\lambda_N(n_1, n_2, \ldots n_N)}{C^M_{N-1+M}}, \tag{16}$$

поскольку $\lambda_N(n_1, n_2, \ldots n_N) = \lambda_1^{n_1}(N)\lambda_2^{n_2}(N)\ldots \ldots\lambda_N^{n_M}(N) \to 1$, то вероятность исходов вне временного окна $[0, T]$ стремится к нулю:

$$P_\perp(n_1, n_2, \ldots n_N) =$$
$$= \mathrm{Tr}\{\mathcal{P}_\perp(n_1, n_2, \ldots n_N)\rho(N, M)\} =$$
$$= \frac{1 - \lambda_N(n_1, n_2, \ldots n_N)}{C^M_{N-1+M}} \to 0. \tag{17}$$

Парциальная матрица плотности с заданным числом фотонов, с учетом (13), (14), имеет вид

$$\rho_M = \frac{1}{N_M} \sum_{M\in\{n_1,n_2,\ldots n_N\}} |\Phi_{n_1,n_2,\ldots n_N}\rangle\langle\Phi_{n_1,n_2,\ldots n_N}|. \tag{18}$$

Выше были получены матрицы плотности при фиксированном числе фотонов M. В реальной ситуации после прохождения первичного квантового состояния из аппаратуры через среду, число фотонов не задано, а задано лишь распределение по числу фотонов. Фактически, в квантовом случае вместо классических распределений (1), подслушиватель видит не чистые состояния, а матрицы плотности, отвечающие 0 и 1, – квантовый ансамбль. Получаем

$$\rho_{0,1} = \sum_{M=0}^{\infty} P_{0,1}(M)\rho_M, \tag{19}$$

где $P_0(M)$ и $P_1(M)$ – функции распределения числа фотонов в состояниях для 0 и 1 в побочном канале. Матрицы плотности являются квантовыми аналогами классических сигналов. Условие нормировки вероятностей

$$\sum_{M=0}^{\infty} P_{0,1}(M) = 1. \tag{20}$$

В итоге, подслушиватель имеет дело с квантовым ансамблем $\mathcal{E} = \{\frac{1}{2}, \rho_0; \frac{1}{2}, \rho_1\}$. Для подслушивателя возникает ситуация квантово-классического канала побочного канала с шумом. Цель подслушивателя, имея в своем распоряжении квантовые состояния в побочном канале, ассоциированные с классическими значениями бит 0 и 1, узнать, посредством измерений квантовых состояний, классические биты, т.е. получить классическую информацию из квантовых состояний. Максимум классической информации, которую можно получить из квантового ансамбля $\mathcal{E}$, дается фундаментальной величиной Холево [1–3]. Для информации Холево (см. [1–3]) получаем

$$\chi(\mathcal{E}) = H\left(\overline{\rho}\right) - \frac{1}{2}H(\rho_0) - \frac{1}{2}H(\rho_1), \tag{21}$$

где

$$\overline{\rho} = \frac{\rho_0+\rho_1}{2} = \sum_{M=0}^{\infty}\frac{P_0(M)+P_1(M)}{2N_M}\times \\ \times \sum_{M\in\{n_1,n_2,\ldots n_N\}} |\Phi_{n_1,n_2,\ldots n_N}\rangle\langle\Phi_{n_1,n_2,\ldots n_N}|, \tag{22}$$

здесь $H(\rho) = -\mathrm{Tr}\{\rho\log(\rho)\}$ – энтропия фон Неймана. Вычисление энтропий дает

$$H\left(\overline{\rho}\right) = -\sum_{M=0}^{\infty}\left(\frac{P_0(M)+P_1(M)}{2}\right)\times \\ \times\log\left(\frac{P_0(M)+P_1(M)}{2}\right) - \log\left(\frac{1}{N_M}\right). \tag{23}$$

$$H(\rho_{0,1}) = -\sum_{M=0}^{\infty}P_{0,1}(M)\log(P_{0,1}(M)) - \log\left(\frac{1}{N_M}\right). \tag{24}$$

Окончательно для величины Холево, с учетом (21)–(24), получаем

$$\chi(\mathcal{E}) = \frac{1}{2}\sum_{M=0}^{\infty}\left\{P_0(M)\log\left(\frac{2P_0(M)}{P_0(M)+P_1(M)}\right) + \right. \\ \left. + P_1(M)\log\left(\frac{2P_1(M)}{P_0(M)+P_1(M)}\right)\right\}. \tag{25}$$

Неформально фундаментальная величина Холево равна количеству информации в битах, которую подслушиватель может получить из побочного канала – квантового ансамбля в пересчете на одну посылку. Формула (25) по структуре аналогична формуле (6) для взаимной информации в классическом случае. Но в отличие от классического рассмотрения квантовый аналог (25) справедлив при любой интенсивности (числа фотонов) побочного сигнала. Кроме того, как видно по выводу (25), формула (25) не ограничена гауссовским шумом и работает при любых распределениях $P_{0,1}(M)$ числа фотонов в квантовых состояниях в побочном канале утечки информации.

Интересно сравнить (25) с классическим аналогом (6), когда число фотонов становится большим. В этом случае, считая шум в побочном канале гауссовским, как и в (6), сумму в (25) можно заменить на интеграл, $\sum_{M=0}^{\infty} \to \int_0^{\infty} dM$, а в качестве распределений взять

$$P_{0,1}(M) = \frac{1}{\sqrt{2\pi\sigma_M^2}}e^{-\frac{(M-M_{0,1})^2}{2\sigma_M^2}}, \tag{26}$$

где $M_{0,1}$ – среднее число фотонов в квантовом состоянии, отвечающем первичному сигналу 0 и 1 соответственно, σ_M – дисперсия числа фотонов в состояниях – аналог интенсивности шума в побочном канале в классическом случае.

Для иллюстрации на рис. 2b приведены зависимости информации в побочном канале при различных отношениях среднего числа фотонов в состоянии к дисперсии шума $\frac{\overline{M}}{\sigma_M}$, где $\overline{M} = \frac{M_1-M_0}{2}$. Как видно из рис. 2b, чем больше отношение $\frac{\overline{M}}{\sigma_M}$ – состояния эффективно меньше перекрываются, тем информация, получаемая из побочного канала оказывается больше.

Из-за макроскопически большого числа степеней свободы и внутренних шумов аппаратуры, состояние в побочном канале непосредственно вблизи экранированной аппаратуры будет представлять собой зашумленный сигнал, поэтому, применительно к квантовой криптографии спектральный состав и интенсивность побочного сигнала может быть измерена непосредственно вблизи экранированной аппаратуры. Консервативно в пользу подслушивателя данный сигнал может считаться сигналом, доступным для измерения подслушивателем. Таким образом может быть оценена величина утечки информации к подслушивателю. Требуемый уровень сигнала в побочном канале может регулироваться соответствующей экранировкой.

5. Заключение. Выше была получена верхняя граница утечки информации по побочному каналу, связанному с электромагнитным излучением передающей аппаратуры. Детектирование побочного излучения является информационным "бонусом" для подслушивателя, поскольку детектирование этого излучения дает дополнительную информацию о передаваемых ключах. В отличие от вторжения в квантовый канал связи детектирование в данном побочном канале не приводит к возмущению информационных состояний и ошибкам на приемной стороне.

Квантовое рассмотрение состояний в побочном канале необходимо для определения утечки информации к подслушивателю при совместном измерении информационных квантовых состояний и квантовых состояний в побочных каналах. Данный анализ требует существенно большего места, поэтому будет приведен в отдельном сообщении.

Выражаю благодарность коллегам по Академии криптографии Российской Федерации за обсуждения и поддержку. Автор благодарит также И. М. Арбекова, С. П. Кулика за интересные обсуждения и замечания.

Работа выполнена при поддержке проекта Российского научного фонда # 16-12-00015 (продолжение).

1. A. S. Holevo, Probl. Inform. Transm. **9**, 177 (1973).
2. А С. Холево, УМН **53**, 193 (1998).
3. А. С. Холево, *Квантовые системы, каналы, информация*, МЦНМО, М. (2010).
4. C. E. Shannon, Beel System Techn. J. **XXVII**, 379 (1948).
5. T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley, N.Y. (1991).
6. H. J. Landau and H. O. Pollak, Bell Syst. Techn. J. **40**, 65 (1961).
7. D. Slepian and H. O. Pollak, Bell Syst. Techn. J. **40**, 43 (1961).
8. W. H. J. Fuchs, J. Math. Anal. Appl. **9**, 317 (1964).
9. Л. Д. Ландау, Е. М. Лифшиц, *Статистическая физика*, т. V, ч. I, Наука, М. (1995).
10. С. Н. Молотков, Письма в ЖЭТФ **105**, 374 (2017).