Письма в ЖЭТФ, том 111, вып. 11, с. 778 – 786 © 2020 г. 10 июня

О подслушивании в квантовой криптографии через побочные каналы утечки информации

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 16 апреля 2020 г.
После переработки 18 апреля 2020 г.
Принята к публикации 18 апреля 2020 г.

В квантовой криптографии, кроме атак на передаваемые квантовые состояния, возможно детектирование состояний в побочных каналах утечки информации. Без учета утечки информации по побочным каналам невозможно всерьез говорить о секретности ключей в реальных системах квантовой криптографии. В работе предложен квантово-механический метод учета утечки ключевой информаци через побочные каналы – детектирование электромагнитного побочного излучения, активное зондирование фазового модулятора на передающей станции и переизлучения лавинных детекторов на приемной стороне. Метод учитывает совместные коллективные измерения квантовых состояний во всех каналах утечки информации и работает при любой интенсивности и структуре состояний в побочных каналах. Выбор специальных базисных функций вытянутого сфероида позволяет "сшить" квантовое и классическое описание сигналов в побочных каналах. Установлена связь между утечкой информации и фундаментальной величиной Холево, также дана прозрачная и интуитивно ясная на физическом уровне интерпретация результатов.

DOI: 10.31857/S1234567820110105

Введение. Методы несакционированного съема информации развиваются по мере развития способов передачи и защиты информации. В классической области носителями информации являются электромагнитные сигналы, которые передаются либо через открытое пространство, по кабельным или волоконным линиям связи. Несакционированный съем информации для классических сигналов возможен как с кабельных линий связи, так и с волоконно-оптических линий. Например, подслушивание с телефонных линий связи в полевых условиях использовалось еще в период Первой мировой войны (см., например, [1]). Для получения информации не обязательно иметь непосредственный доступ к самой линии связи [2], поскольку работа передающей и приемной аппаратуры приводит к побочному электромагнитному излучению, которое может детектироваться. В качестве примера, в [3] было продемонстрировано, что контент и изображение видео дисплея могут быть воспроизведены дистанционно относительно недорогими техническими средствами. Детектирование побочного электромагнитного излучения может приводит к компроментации работы электронного криптографического оборудования [4] (некоторые исторические примеры см., например, в [5]). Различные типы интерфейсов между отдельными модулями аппаратуры также приводят к компроментирующему побочному излучению (например, [6], где был продемонстрирован несанкционированный съем информации при излучении кабеля интерфейса RS-232 без прямого доступа). Отдельные технические детали измерения побочного излучения можно найти в [7]. Существуют и другие побочные каналы утечки информации: электромагнитное излучение, оптическое излучение (электромагнитное в оптическом диапазоне), акустические каналы, ультразвуковые, механические и пр., которые могут приводить к утечке информации без непосредственного доступа к источнику информации. Большой набор методов и экспериментальных устройств, существующих в данной области, обычно широко не освещается.

Понижение уровня оптического сигнала до однофотонного уровня приводит к тому, что сигнал становится квантовым, и это приводит к принципиально качественно новой ситуации. В отличии от интенсивного классического оптического сигнала, передаваемого по волоконной линии связи, попытки под-

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

слушать – измерить неизвестное состояние в линии связи, приводят к возмущению квантового состояния и ошибкам на приемной стороне [8]. По этой причине любое вторжение в квантовый канал связи детектируется, что гарантируется фундаментальными законами квантового мира. Более того, фундаментальные ограничения квантовой механики позволяют связать наблюдаемый уровень возмущения квантовых состояний (уровень ошибок) на приемной стороне с верхней границей утечки информации [9, 10]. Собственно, на этом и строится квантовая криптография – квантовое распределение секретных ключей [8]. В этом смысле, системы квантовой криптографии защищены от атак непосредственно на линию связи. Более того, считается, что линия связи непосредственно доступна для активного прослушивания – вторжения.

На сегодняшний день касательно атак на квантовые состояния в квантовой линии связи – попыток съема передаваемой ключевой информации, достигнуто достаточно глубокое понимание. Существуют методы учета не строгой однофотонности источника квантовых состояний, потерь в линии связи, не единичной квантовой эффективности однофотонных детекторов и пр. Относительно атак на квантовый канал связи можно говорить, что квантовая криптография обеспечивает безусловную секретность ключей, которая базируется только на фундаментальных законах квантовой механики.

Системы квантовой криптографии представляют собой достаточно сложные и насыщенные активными волоконными компонентами устройства – фазовыми модуляторами, модуляторами интенсивности, контроллерами поляризации, управляющей электроникой с различными внешними и внутренними интерфейсами. Работа электроники и электронно-управляемых активных волоконных элементов приводит к побочному излучению, которое несет на себе информацию о передаваемых ключах.

В квантовой криптографии ситуация еще более деликатная, чем в классических криптографических системах. Системы квантовой криптографии являются открытыми системами, в том смысле, что кроме детектирования побочного излучения, подслушиватель может активно зондировать через волоконную линию связи состояние волоконных элементов (фазовых модуляторов, модуляторов интенсивности, контроллеров поляризации и пр.), которые дают информацию о передаваемых ключах. *Без понимания и учета утечки информации по побочным каналам невозможно всерьез говорить о секретности ключей в реальных системах квантовой криптографии.* Еще одно принципиальное отличие побочных каналов в квантовой криптографии от побочных каналов в классических системах состоит в том, что невозможно рассматривать состояния в побочных каналах классическим образом. Подслушиватель может совместно измерять информационные квантовые состояния и состояния в побочных каналах, что требует полного квантового рассмотрения.

На сегодняшний день полный набор методов учета атак на аппаратуру и учет побочных каналов утечки находится в стадии активного исследования. В отличие от классических криптографических систем исследование утечки информации по побочным каналам началось совсем недавно. Напомним, что по времени понимание и развитие доказательств секретности ключей даже для строго однофотонного источника и без побочных каналов утечки заняло около 10 лет. Опробываются различные подходы. В работе [11] был поставлен вопрос об учете побочных каналов. Дальнейшее развитие этого подхода было дано в [12, 13]. Однако метод учета неоднофотонности источника при наличии побочных каналов в [11] приводит к задаче оптимизации, которую приходится решать интенсивными численными методами, используемых в задачах оптимизации линейного программирования (см., например, Appendix C в [11]). В работах [14–17] был разработан метод, который позволяет решить задачу аналитически до конца. Поскольку при введении побочных каналов нельзя обойтись без модельных предположений, то в [11, 12, 14, 16, 17] использовались простейшие дискретные побочные каналы, которые не содержат явно временных и частотных характеристик каналов. Модельные параметры таких каналов часто невозможно “привязать” к реально измеряемым характеристикам – спектральным и временным характеристикам. В реальной ситуации при детектировании побочного излучения всегда используются в том или ином виде спектральные приборы. Детектирование происходит в отдельные временные такты. По этой причине требуются гораздо более реалистичные модели побочных каналов, такие как распределение числа фотонов в спектральных и временных окнах.

В данной работе развивается подход, который позволяет ответить на поставленные вопросы. Будут получены формулы для длины секретного ключа, в которые входят явно спектральные характеристики состояний в побочных каналах утечки информации. Метод достаточно прост и универсален, в том смысле, что работает при любом спектре побочных состояний, а также имеет простую и интуитивно понятную на физическом уровне интерпретацию. Поскольку в системах квантовой криптографии используются различные протоколы распределения ключей, то для каждого протокола приходится строить методы учета утечки индивидуально (см., например, [11–17]). Предлагаемый аналитический метод достаточно универсален и может быть использован для других протоколов. Выбор специальных базисных функций для состояний позволяет естественным образом "сшить" – единообразно рассматривать утечки по побочным каналам в квантовой и классической области, а также рассматривать комбинированные. Возможны также активные атаки, которые изменяют работу отдельных элементов системы, например, лавинных детекторов – атака с ослеплением детекторов (Blinding Attack) и атака, основанная на разных временных характеристиках детекторов – Detector Mismatch (см. ссылки в [18]). Отдельные методы защиты от таких атак обсуждались в [19, 20].

Длина секретного ключа при утечке информации по побочным каналам. Нашей целью будет вычисление длины секретного ключа. Для сокращения выкладок ограничимся пределом асимптотически длинных последовательностей. Учет конечной длины передаваемых последовательностей приводит к флуктуациям параметров, что учитывается стандартными методами классической теории вероятностей.

В реальных системах источник информационных состояний представляет собой ослабленные когерентные состояния с пуассоновской статистикой по числу фотонов, и не является строго однофотонным. Секретный ключ набирается только из однофотонной компоненты когерентных состояний. Информация, заключенная в многофотонных компонентах состояний с числом фотонов $k > 1$, консервативно в пользу Евы, считается ей известной. Доля однофотонной компоненты на приемной стороне оценивается модифицированным Decoy State методом (см. детали в [11]). Без побочных каналов утечки информации самой общей атакой на однофотонную компоненту состояний является унитарная атака. Для протокола BB84 такую оптимальную атаку можно построить явно [11].

Поскольку многофотонные компоненты состояний "отдаются" (считаются известными) подслушивателю, то дальнейшая задача сводится к построению атаки на однофотонную компоненту с учетом побочных каналов утечки. Вся информация об атаках Евы заключена в условной энтропии фон Неймана. Длина секретного ключа ℓ_n дается общей формулой [9]

$$\ell = \frac{\ell_n}{n} = H_{\min}^{\varepsilon}(X|E) - \mathrm{leak}, \qquad (1)$$

где n – число зарегистрированных посылок в базисе, leak – информация в битах в пересчете на одну посылку, фактически израсходованная на коррекцию ошибок Алисой и Бобом, $H_{\min}^{\varepsilon}(X|E)$ – условная сглаженная min энтропия, $X \in \mathcal{X} = \{0,1\}^n$ – битовая строка Алисы, E – квантовая система Евы, коррелированная с битовой строкой. Неформально, $H_{\min}^{\varepsilon}(X|E)$ есть дефицит информации подслушивателя о битовой строке Алисы. Данная величина включает в себя всевозможные атаки Евы. В асимптотическом пределе $n \to \infty$ сглаженная min энтропия в (1) переходит в условную энтропию фон Неймана [9, 10]

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

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

Далее будем рассматривать протокол BB84, поскольку он является базовым. Предлагаемый метод переносится и на другие протоколы. Без побочных каналов утечки информации длина секретного ключа в однофотонном случае имеет вид

$$\ell = (1 - h(Q)) - h(Q), \qquad (3)$$

где первое слагаемое есть нехватка информации Евы при наблюдаемой вероятности ошибки на приемной стороне Q, второе – утечка информации при коррекции ошибок Алисой и Бобом. Первое слагаемое – убывающая функция Q. Неформально, чем сильнее возмущение состояний Евой (больше ошибка на приемной стороне), тем меньше нехватка информации Евы о передаваемом бите ключа. Второе слагаемое – растущая функция, чем больше ошибка, тем больше бит информации требуется раскрыть Алисе для Боба (соответственно и Евы) для исправления ошибок. Если возмущение состояний (ошибка) достигает критической величины $(1 - h(Q_c) = h(Q_c)$, $Q_c \approx 11\,\%)$, то длина ключа – число секретных бит стремится к нулю, секретный ключ получить нельзя.

Побочные каналы утечки информации. Структура информационных состояний, направляемых в канал связи Алисой, известна. При рассмотрении побочных каналов утечки информации невозможно обойтись без модельных предположений о структуре побочных каналов. Существует несколько существенных побочных каналов – пассивные каналы утечки, связанные с побочным электромагнитным излучением аппаратуры передающей и приемной станций, пассивный канал утечки связанный с переизлучением лавинных детекторов/детектора на приемной станции при регистрации информационных состояний, каналы, связанные с активным зондированием через линию связи фазовых модуляторов на обеих станциях. Данные каналы утечки информации являются дополнительным информационным "бонусом" для подслушивателя и не приводят к ошибкам на приемной стороне, поскольку не возмущают передаваемых информационных состояний.

Состояния в канале утечки, связанным с излучение электроники передающей станции, из-за огромного числа степеней свободы электронной аппаратуры, точно неизвестны. Максимум на что можно рассчитывать, это знание интенсивности побочного сигнала в разных частях спектра, что достигается измерениями для каждой конкретной реализации системы. По этой причине состояние в этом канале должно описываться матрицей плотности (см. ниже).

При активном зондировании состояния фазового модулятора на передающей станции, консервативно в пользу подслушивателя можно считать, что отраженные состояния являются чистыми. Интенсивность входных зондирующих состояний задается подслушивателем. Чем больше интенсивность входных состояний, тем больше интенсивность отраженных состояний, тем они более различимы. Однако входная мощность зондирующего состояния ограничена некоторой критической величиной, определяемой плавлением волокна (см., например, [21]), поэтому использование оптических изоляторов с нужным обратным коэффициентом пропускания позволяет оценить верхнюю границу интенсивности выходных зондирующих состояний.

Каналы утечки информации приемной станции следующие. Имеются реализации, которые не используют фазового модулятора на приемной стороне [22], поэтому канал утечки, связанный с зондированием фазового модулятора на приемной стороне, отсутствует.

Работа электроники включает стробирование лавинных детекторов при регистрации состояний. При регистрации в лавинных детекторах возникает лавина неравновесных носителей, рекомбинация которых приводит в переизлучению в линию связи. Данный канал нужно принять во внимание. Состояние переизлучения из-за большого числа неконтролируемых степеней свободы должно описываться матрицей плотности. В принципе, интенсивность переизлученных состояний в разных частях спектра может быть измерена, и определяется конкретной реализацией системы.

Квантовые состояния в побочных каналах. Перейдем к построению квантовых состояний в упомянутых побочных каналах. Рассмотрим побочный канал, связанный с излучением передающей аппаратуры. Необходимо выбрать набор базисных функций, по которым будет раскладываться квантовое состояние. Таким естественным набором базисных функций являются функции вытянутого сфероида [23–25]. Подслушиватель измеряет состояния во временном окне в каждом такте (см. детали и рис. 1 в [26]). 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 характерные 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. $\Omega T \gg 1$. Базисными функциями максимально локализованными во временном окне $[0,T]$ являются функции вытянутого сфероида (Prolate Spheroidal Functions), которые удовлетворяют интегральному уравнению (см. детали в [23–25])

$$\lambda_n(c)\phi_n(t,c) = \frac{1}{\pi}\int_0^T \frac{\sin[\Omega(t-t')]}{t-t'}\phi_n(t',c)dt', \quad 2c = \Omega T. \tag{4}$$

При разных n и n' функции ортогональны как на конечном $[0,T]$, так и на бесконечном $(-\infty,\infty)$ интервалах,

$$\begin{gathered}\int_0^T \phi_n(t,c)\phi_{n'}(t,c)dt = \lambda_n(c)\delta_{n,n'},\\ \int_{-\infty}^{\infty} \phi_n(t,c)\phi_{n'}(t,c)dt = \delta_{n,n'}.\end{gathered} \tag{5}$$

Степень локализации во временном окне $[0,T]$ собственной функции (5) с номером n уравнения (4) дается ее собственным числом $\lambda_n(c)$. 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 [25] по параметру ΩT, $\lambda_n(c) \approx 1 - e^{-c}$ для $n = 1, 2, ..., N$.

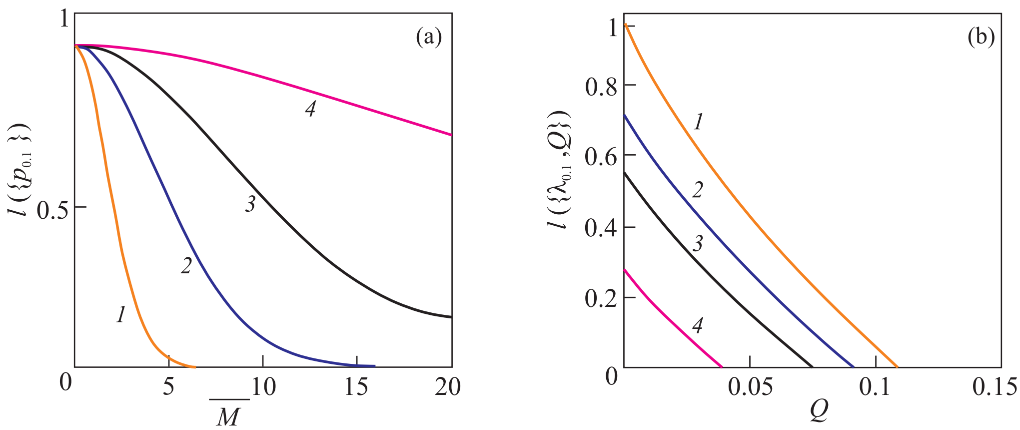

Рис. 1. (Цветной онлайн) (a) – Длина секретного ключа при детектировании только побочного излучения передающей станции как функция среднего числа фотонов $\overline{M}$ при различных отношениях "сигнал-шум" $\frac{\overline{M}}{\sigma_M}$ $\left(\frac{E_s}{N_{\text{noise}}}\right)$ – среднего числа фотонов к дисперсии. Параметр $\frac{\overline{M}}{\sigma_M}$ $\left(\frac{E_s}{N_{\text{noise}}}\right)$ для кривых *1–4* следующий: *1* – 0.5; *2* – 0.2; *3* – 0.1; *4* – 0.05. (b) – Длина секретного ключа при атаке на информационные состояния и активном зондировании фазового модулятора на передающей станции. Параметр μ_P для кривых *1–4*: *1* – 0.001, *2* – 0.05, *3*– 0.1, *4* – 0.25

Пусть квантовое состояние поля содержит M фотонов – бозе-частиц. Состояние имеет носитель в конечной частотной полосе Ω. В качестве одночастичных базисных состояний выберем волновые функции вытянутого сфероида $\varphi_n(\omega)$. Таких функций $N = \Omega T$. Число многочастичных ортогональных векторов состояний с M фотонами, локализованных во временном окне T, равно числу способов размещения M фотонов по N одночастичным состояниям. Число размещений M бозе-частиц (фотонов) по N состояниям равно [27] $N_M = C^M_{N-1+M} = \frac{(N-1+M)!}{(N-1)!M!}$. Отметим, что бозе-статистика возникает в различных задачах квантовой криптографии, например, при реализации квантовых генераторов случайных чисел (см. подробности в [28]). Вектор состояния, отвечающий размещению $n_1 + n_2 + \ldots + n_N = M$ (n_1 частиц в состоянии $\varphi_1(\omega_1)$, и т.д.), имеет вид

$$|\Psi_{n_1,n_2,\ldots,n_N}\rangle =$$
$$= \int_\Omega \ldots \int_\Omega d\omega_1 d\omega_2 \ldots d\omega_{n_1} \ldots d\omega_{n_1+1} d\omega_{n_1+2} \ldots$$
$$\ldots d\omega_{n_2}, d\omega_{n_{N-1}+1} d\omega_{n_{N-1}+2} \ldots d\omega_{n_N} \qquad (6)$$
$$\varphi_1(\omega_1)\varphi_1(\omega_2)\ldots\varphi_1(\omega_{n_1})\varphi_2(\omega_{n_1+1})\varphi_2(\omega_{n_1+2})\ldots$$
$$\ldots\varphi_2(\omega_{n_2})\ldots\varphi_N(\omega_{n_{N-1}+1})\varphi_N(\omega_{n_{N-1}+2})\ldots\varphi_N(\omega_{n_N})$$
$$|\omega_1,\omega_2,\ldots\omega_{n_1},\ldots\omega_{n_1+1},\omega_{n_1+2},\ldots\omega_{n_2},$$
$$\omega_{n_{N-1}+1},\omega_{n_{N-1}+2},\ldots\omega_{n_N}\rangle.$$

Консервативно в пользу Евы, максимальная энтропия источника, соответственно, максимальная утечка достигается в том случае, когда источник генерирует все C^M_{N-1+M} ортогональных различимых состояний равновероятно. Такой источник описывается матрицей плотности – квантовым ансамблем, который зависит от того, какой логический бит, 0 или 1, приготавливается передающей аппаратурой. Имеем

$$\rho_{0,1S_A} = \sum_{M=0}^{\infty} p_{0,1}(M)\frac{1}{N_M} \times$$
$$\sum_{M\in\{n_1,n_2,\ldots,n_N\}} |\Psi_{n_1,n_2,\ldots,n_N}\rangle\langle\Psi_{n_1,n_2,\ldots,n_N}|, \qquad (7)$$
$$\sum_{M=0}^{\infty} p_{0,1}(M) = 1.$$

Распределения вероятностей для 0 $p_0(M)$ и 1 $p_1(M)$ могут быть измерены в контролируемой зоне – вблизи аппаратуры передающей станции. Индексы у $\rho_{0,1S_A}$ означают 0 или 1 в канале S_A – Side Alice. С использованием аналогичных рассуждений строится состояние в побочном канале, связанном с переизлучением лавинных детекторов на приемной станции. Обозначим квантовый ансамбль как

$$\rho_{0,1S_B} = \sum_{M=0}^{\infty} q_{0,1}(M)\frac{1}{N_M} \times$$
$$\times \sum_{M\in\{n_1,n_2,\ldots,n_N\}} |\Psi_{n_1,n_2,\ldots,n_N}\rangle\langle\Psi_{n_1,n_2,\ldots,n_N}|, \qquad (8)$$
$$\sum_{M=0}^{\infty} q_{0,1}(M) = 1.$$

Аналогично (7) индексы у $\rho_{0,1S_A}$ означают 0 или 1 в канале S_B – Side Bob.

Квантовое состояние в побочном канале, связанным с активным зондированием фазового модулятора на станции Алисы, может быть представлено в виде

$$\rho_{0,1P} = |\lambda_{0,1}\rangle_{P\,P}\langle\lambda_{0,1}|. \tag{9}$$

Индекс 0 или 1 у $\rho_{0,1P}$ означает отраженное квантовое состояние, когда аппаратура Алисы приготавливает 0 или 1, индекс P – от Phase. При фазовом кодировании при приготовлении логического бита 0 или 1 к фазовому модулятору прикладывается разное напряжение, грубо говоря, и опуская подробности, изменяется оптическая длина устройства, что приводит к разным отраженным состояниям $|\lambda_{0,1}\rangle_P$, которые считаем чистыми (см. выше). Если Ева зондирует состояние фазового модулятора когерентными состояниями $|\alpha\rangle$ с известной фазой α, то отраженные состояния, в пользу Евы, также когерентные с фазой $|\alpha\rangle_{0P}$ и $|-\alpha\rangle_{1P}$, выбор фаз отраженных состояний отвечает, в пользу Евы, максимальной различимости отраженных состояний. Далее увидим, что в длину ключа входит только скалярное произведение отраженных состояний ${}_{0P}\langle\alpha|-\alpha\rangle_{1P}$.

Квантовые состояния Алиса–Ева. Построим теперь унитарную атаку на однофотонную компоненту состояний. Отметим, что для получения информации Ева вынуждена *искажать* информационные состояния в квантовом канале связи. Состояния в побочных каналах являются для нее "бонусом", их можно регистрировать непосредственно, не заботясь об их искажении после измерений. Имея ввиду протокол BB84, рассмотрим атаку на информационные состояния в одном из базисов [29]. Атака в сопряженном базисе получается унитарным поворотом информационных состояний. Имеем (см. детали в [29])

$$\begin{aligned} |0\rangle_X\otimes|0\rangle_Y \to |0\rangle_X\otimes U_{BE}(|0\rangle_Y\otimes|E\rangle_Q) = \\ = |0\rangle_X\otimes[\sqrt{1-Q}|0\rangle_Y\otimes|\Phi_0\rangle_Q + \\ + \sqrt{Q}|1^+\rangle_Y\otimes|\Theta_0\rangle_Q], \end{aligned} \tag{10}$$

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, который содержит способ атаки Евы на передаваемое в квантовом канале состояния Боба, $|E\rangle_Q$ – исходное вспомогательное состояние Евы – ancilla, $|\Phi_0\rangle_Q$ и $|\Theta_0\rangle_Q$ – искаженные состояния, возникающие из вспомогательного состояния Евы. Аналогичное выражение имеет место, когда в канал передается состояние $|1\rangle_Y$. Имеем

$$\begin{aligned} |1\rangle_X\otimes|1\rangle_Y \to |1\rangle_X\otimes U_{BE}(|1\rangle_Y\otimes|E\rangle_Q) = \\ = |1\rangle_X\otimes[\sqrt{1-Q}|1\rangle_Y\otimes|\Phi_1\rangle_Q + \\ + \sqrt{Q}|0\rangle_Y\otimes|\Theta_1\rangle_Q]. \end{aligned} \tag{11}$$

Побочные каналы утечки сводятся к добавлению к состояниям Евы квантовых состояний в побочных каналах. После измерений на стороне Боба в базисе $\{|0\rangle_Y, |1\rangle_Y\}$ возникает матрица плотности Алиса–Боб–Ева, имеем

$$\rho_{XYQS_APS_B} = \tag{12}$$

$$= \frac{1}{2}|0\rangle_{X\,X}\langle 0|\otimes\rho_{0S_A}\otimes\rho_{0P}\otimes[(1-Q)|0\rangle_{Y\,Y}\langle 0|\otimes$$

$$\otimes|\Phi_0\rangle_{Q\,Q}\langle\Phi_0|\otimes\rho_{0S_B}+Q|1\rangle_{Y\,Y}\langle 1|\otimes|\Theta_0\rangle_{Q\,Q}\langle\Theta_0|\otimes\rho_{1S_B}]+$$

$$+\frac{1}{2}|1\rangle_{X\,X}\langle 1|\otimes\rho_{1S_A}\otimes\rho_{1P}\otimes[(1-Q)|1\rangle_{Y\,Y}\langle 1|\otimes$$

$$\otimes|\Phi_1\rangle_{Q\,Q}\langle\Phi_1|\otimes\rho_{1S_B}+Q|0\rangle_{Y\,Y}\langle 0|\otimes|\Theta_1\rangle_{Q\,Q}\langle\Theta_1|\otimes\rho_{0S_B}].$$

Интерпретируем (12). Пусть Алиса посылала $|0\rangle_X$, Боб может зарегистрировать $|0\rangle_{Y\,Y}\langle 0|$ с вероятностью $1-Q$ – правильный отсчет. При этом в распоряжении Евы окажется состояние $\rho_{0S_A}\otimes\rho_{0P}\otimes$ $\otimes|\Phi_0\rangle_{Q\,Q}\langle\Phi_0|\otimes\rho_{0S_B}$, т.е. кроме искаженного состояния ancilla при атаке на состояния в квантовом канале у Евы будут состояния из побочных каналов. Если Боб зарегистрировал ошибочное состояние $|1\rangle_{Y\,Y}\langle 1|$ с вероятностью ошибки Q, то этом в случае в распоряжении Евы окажется состояние $\rho_{0S_A}\otimes\rho_{0P}\otimes$ $\otimes|\Theta_0\rangle_{Q\,Q}\langle\Theta_0|\otimes\rho_{1S_B}$. Побочные состояния у Евы ρ_{0S_B} или ρ_{1S_B} возникают в зависимости от того, какое состояние зарегистрировано у Боба – фактически какой из двух лавинных детекторов сработал. Для вычисления длины ключа нужны частичные матрицы плотности Алиса–Ева

$$\rho_{XQS_APS_B} = \tag{13}$$

$$= \frac{1}{2}|0\rangle_{X\,X}\langle 0|\otimes\rho_{0S_A}\otimes\rho_{0P}\otimes[(1-Q)|\Phi_0\rangle_{Q\,Q}\langle\Phi_0|\otimes\rho_{0S_B}+$$

$$+Q|\Theta_0\rangle_{Q\,Q}\langle\Theta_0|\otimes\rho_{1S_B}]+$$

$$+\frac{1}{2}|1\rangle_{X\,X}\langle 1|\otimes\rho_{1S_A}\otimes\rho_{1P}\otimes[(1-Q)|\Phi_1\rangle_{Q\,Q}\langle\Phi_1|\otimes\rho_{1S_B}+$$

$$+Q|\Theta_1\rangle_{Q\,Q}\langle\Theta_1|\otimes\rho_{0S_B}],$$

и матрица плотности Евы

$$\rho_{QS_APS_B} = \tag{14}$$

$$= \frac{1}{2}(1-Q)[|\Phi_0\rangle_{Q\,Q}\langle\Phi_0|\otimes\rho_{0S_A}\otimes\rho_{0P}\otimes\rho_{0S_B}+$$

$$+|\Phi_1\rangle_{Q\,Q}\langle\Phi_1|\otimes\rho_{1S_A}\otimes\rho_{1P}\otimes\rho_{1S_B}]+$$

$$+\frac{1}{2}Q[|\Theta_0\rangle_{Q\,Q}\langle\Theta_0|\otimes\rho_{0S_A}\otimes\rho_{0P}\otimes\rho_{1S_B}+$$

$$+|\Theta_1\rangle_{Q\,Q}\langle\Theta_1|\otimes\rho_{1S_A}\otimes\rho_{1P}\otimes\rho_{0S_B}].$$

Вычисляя собственные числа (13) и (14), получаем для условной энтропии фон Неймана

$$H(\rho_{XQS_APS_B}|\rho_{QS_APS_B}) = \qquad (15)$$

$$= -\frac{1}{2}\sum_{M=0}^{\infty}\left[p_0(M)\log(p_0(M)) + p_1(M)\log(p_1(M))\right] -$$

$$-\frac{1}{2}\sum_{M=0}^{\infty}\left[q_0(M)\log(q_0(M)) + q_1(M)\log(q_1(M))\right] +$$

$$+\frac{1}{2}(1-Q)\sum_{M=0}^{\infty}\Big[\lambda_+^{(1-Q)}(M)\log(\lambda_+^{(1-Q)}(M)) +$$

$$+\lambda_-^{(1-Q)}(M)\log(\lambda_-^{(1-Q)}(M))\Big] + \frac{1}{2}Q\times$$

$$\times\sum_{M=0}^{\infty}\Big[\lambda_+^{(Q)}(M)\log(\lambda_+^{(Q)}(M)) + \lambda_-^{(Q)}(M)\log(\lambda_-^{(Q)}(M))\Big].$$

Введены обозначения

$$\lambda_{\pm}^{(1-Q)} = \frac{1}{2}\times$$
$$\times[Q_{00}+Q_{11}\pm\sqrt{(Q_{00}+Q_{11})^2-4Q_{00}Q_{11}(1-\zeta^2)}], \quad (16)$$

$$\lambda_{\pm}^{(Q)} = \frac{1}{2}\times$$
$$\times[Q_{01}+Q_{10}\pm\sqrt{(Q_{01}+Q_{10})^2-4Q_{01}Q_{10}(1-\zeta^2)}], \quad (17)$$

$$Q_{ij} = p_i(M)q_j(m)\ (i,j=0,1),$$
$$\zeta = \varepsilon\eta,\ \eta = {}_P\langle\lambda_0|\lambda_1\rangle_P, \qquad (18)$$
$$\varepsilon = {}_Q\langle\Phi_0|\Phi_0\rangle_Q = {}_Q\langle\Theta_0|\Theta_0\rangle_Q = 1-2Q.$$

Для вычисления утечки информации при коррекции ошибок нужна частичная матрица плотности Алиса–Боб. Вычисляя частичный след по всем состояниям Евы в (12), получаем

$$\rho_{XY} =$$
$$= \frac{1}{2}|0\rangle_{XX}\langle 0|\otimes[(1-Q)|0\rangle_{YY}\langle 0| + Q|1\rangle_{YY}\langle 1|] +$$
$$+\frac{1}{2}|1\rangle_{XX}\langle 1|\otimes[(1-Q)|1\rangle_{YY}\langle 1| + Q|0\rangle_{YY}\langle 0|]. \quad (19)$$

Частичная матрица плотности Боба и условная энтропия фон Неймана Алиса–Боб с учетом (19) имеют вид

$$\rho_Y = \frac{1}{2}[|0\rangle_{YY}\langle 0| + |1\rangle_{YY}\langle 1|],$$
$$H(\rho_{XY}|\rho_Y) = h(Q). \qquad (20)$$

Для длины секретного ключа, принимая во внимание (1) и (15), (20), получаем

$$\ell(\{p_{0,1}, q_{0,1}, \lambda_{0,1}, Q\}) =$$
$$= H(\rho_{XQS_APS_B}|\rho_{QS_APS_B}) - h(Q). \qquad (21)$$

Формула (21) дает длину секретного ключа с учетом утечки информации по побочным каналам. Длина ключа зависит от структуры квантовых состояний в побочных каналах, от вероятностей распределений по числу фотонов ($p_{0,1}q_{0,1}$) в частотной полосе измерений, отраженного зондирующего состояния ($\lambda_{0,1}$, см. (9)), а также от наблюдаемой ошибки на приемной стороне. Канал утечки, связанный с зондированием модулятора интенсивности не дает прямой информации о передаваемых битах ключа, но влияет на оценку величины доли однофотонной компоненты состояний, что может быть учтено модифицированным Decoy State методом, развитым в [16, 17].

Предельные случаи, связь с фундаментальной величиной Холево. Формула (21) дает длину ключа с учетом всех побочных каналов утечки информации. Рассмотрим примеры отдельных каналов утечки.

Канал утечки, связанный с излучением передающей аппаратуры. Пусть Ева не вторгается в квантовый канал связи и не производит возмущение информационных состояний, а детектирует только побочное излучение передающей аппаратуры. В этом случае в формулах (12)–(14) нужно оставить только слагаемые

$$\rho_{XS_A} = \frac{1}{2}\{|0\rangle_{XX}\langle 0|\otimes\rho_{0S_A} + |1\rangle_{XX}\langle 1|\otimes\rho_{1S_A}\},$$
$$\rho_{S_A} = \frac{1}{2}\{\rho_{0S_A} + \rho_{1S_A}\}. \qquad (22)$$

В этом случае длина секретного ключа дается фундаментальной величиной Холево [30–32] для квантового ансамбля $\mathcal{E} = \{\frac{1}{2}, \rho_{0S_A}; \frac{1}{2}, \rho_{1S_A}\}$ и равна

$$\ell(\{p_{0,1}\}) = 1 - \chi(\mathcal{E}), \qquad (23)$$

$$\chi(\mathcal{E}) = H\left(\frac{\rho_{0S_A}+\rho_{1S_A}}{2}\right) - \frac{1}{2}H(\rho_{0S_A}) - \frac{1}{2}H(\rho_{1S_A}).$$

$$\chi(\mathcal{E}) = -\frac{1}{2}\sum_{M=0}^{\infty}\left\{p_0(M)\log\left(\frac{p_0(M)+p_1(M)}{2p_0(M)}\right) +\right.$$
$$\left. + p_1(M)\log\left(\frac{p_0(M)+p_1(M)}{2p_1(M)}\right)\right\}. \qquad (24)$$

Формулы (23), (24) имеют следующую интерпретацию. При детектировании только побочного излучения Ева видит с вероятностью 1/2 состояние ρ_{0S_A} и с вероятностью 1/2 состояние ρ_{1S_A}. Цель Евы – узнать какому биту Алисы, 0 или 1, отвечают данные квантовые состояния. Фактически Алиса и Ева находятся в ситуации квантово-классического канала связи. Алиса кодирует классическую информацию о секретных битах в квантовые состояния. Неформально, величина Холево есть верхняя достижимая граница классической информации (числа бит), которую можно извлечь из квантового ансамбля. Причем данная граница достигается на коллективных измерениях квантовых состояний [21–23]. Каждая позиция от Алисы несет один бит информации (первое слагаемое в правой части (23)), из этого бита Ева знает не более $\chi(\mathcal{E})$ бит (второе слагаемое в (23)), соответственно, информация недоступная для Евы (секретная часть) составляет $1-\chi(\mathcal{E})$ бит. Для иллюстрации, считая шум в побочном канале гауссовским, сумму в (15) можно заменить на интеграл, $\sum_{M=0}^{\infty} \to \int_0^{\infty} dM$, а в качестве распределений взять $p_{0,1}(M) = \frac{1}{\sqrt{2\pi\sigma_M^2}} e^{-\frac{(M-M_{0,1})^2}{2\sigma_M^2}}$, 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. На рисунке 1a приведены зависимости длины секретного ключа при различных отношениях среднего числа фотонов в состоянии к дисперсии шума $\frac{\overline{M}}{\sigma_M}$, где $\overline{M} = \frac{M_1-M_0}{2}$. В классическом случае вместо числа фотонов используется энергия сигнала в частотной полосе (E_s), аналогично дисперсия сигналов выражается через интенсивность шума в частотной полосе. В этом случае имеет место соответствие $\Omega\overline{M} \to E_s$ и $\Omega\sigma^2 \to \frac{N_{\text{noise}}}{2}$. В этих обозначениях длина ключа в (23) становится функцией $\ell\left(\frac{E_s}{N_{\text{noise}}}\right)$. Из рисунка 1a видно, что даже без атаки на информационные квантовые состояния при большом отношении сигнал/шум – хорошей различимости состояний (например, кривая 1 ($\frac{\overline{M}}{\sigma_M} = 0.5$, $\left(\frac{E_s}{N_{\text{noise}}}\right)$)) даже при малом числе фотонов в побочном состоянии $\frac{M}{\sigma_M} \approx 5$, длина ключа стремится к нулю. Подслушиватель, детектируя состояния только в побочном канале и не производя ошибок на приемной стороне, будет знать весь ключ. При малом отношении сигнал/шум (кривая *4* рис. 1a) – плохая различимость состояний позволяет можно получить ключ даже при большом среднем числе фотонов ($\frac{M}{\sigma_M} > 20$) в побочном состоянии.

Канал утечки, связанный с зондированием фазового модулятора и атакой на информационные состояния. Рассмотрим атаку Евы с активным зондированием состояния фазового модулятора и вторжением в квантовый канал связи. Оставляя в (12)–(14) соответствующие слагаемые, для условной энтропии получаем

$$H(\rho_{XQP}|\rho_{QP}) = 1 - \chi(\epsilon\eta), \tag{25}$$

$$\chi(\epsilon\eta) = -\left(\frac{1+\epsilon\cdot\eta}{2}\right)\log\left(\frac{1+\epsilon\cdot\eta}{2}\right) - \\ -\left(\frac{1-\epsilon\cdot\eta}{2}\right)\log\left(\frac{1-\epsilon\cdot\eta}{2}\right),$$

где $\epsilon = 1-2Q$ и $\eta = |{}_P\langle\lambda_0|\lambda_1\rangle_P|$. Для длины секретного ключа, принимая во внимание (1) и (25), получаем

$$\ell(\{\lambda_{0,1}, Q\}) = 1 - \chi(\epsilon\eta) - h(Q). \tag{26}$$

Проинтерпретируем результат. Зондирование состояния фазового модулятора эффективно увеличивает различимость информационных квантовых состояний, не приводя при этом к дополнительным ошибкам на приемной стороне. Фазы отраженных когерентных состояний “привязаны” к состоянию фазового модулятора – приготавливаемому информационному состоянию. В пользу Евы можно считать, что фазы когерентных состояний соответствуют фазам информационных состояний $|0\rangle_X$, $|1\rangle_X$, и отраженные состояния имеют вид: $|\lambda_0\rangle_P = |\sqrt{\mu_P}\rangle_P$, $|\lambda_1\rangle_P = |-\sqrt{\mu_P}\rangle_P$, где μ_P – среднее число фотонов в отраженных состояниях. Если в качестве зондирующего излучения используются когерентные состояния, то для η получаем $\eta = e^{-2\mu_P}$. При малых $\mu_P \ll 1$ для величины $\chi(\epsilon\eta)$ в (25) находим $\chi(\epsilon\eta) \approx h(Q(\mu_P))$, $Q(\mu_P) = Q + \mu_P$. Без зондирующего излучения и атаке только на информационные состояния в канале связи длина секретного ключа при наблюдаемой ошибке Q на приемной стороне (см. (3), (25), (26)) равна $1-2h(Q)$. С учетом зондирующего излучения длина секретного ключа оказывается равной $1-h(Q+\mu_P)-h(Q) < 1-2h(Q)$, и естественно меньше. Зависимости длины секретного ключа при атаке на информационные состояния и активном зоднировании фазового модулятора приведены на рис. 2b. Чем более интенсивные состояния отражаются от модулятора, тем меньшую длину ключа, при данной наблюдаемой ошибке, можно получить. Параметры состояний в побочных каналах должны определяться для каждой конкрентной реализации системы квантовой криптографии. Предлагаемый метод позволяет определить диапазон параметров состояний в побочных каналах, при которых гарантируется секретное распределение ключей. *Важно отметить, что в формулах (21), (23), (26) для длины секретного ключа учтены совместные коллективные измерения над квантовыми состояниями в побочных каналах и информационными квантовыми состояниями.*

Выражаю благодарность коллегам по Академии криптографии Российской Федерации за обсуждения, замечания 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. O. Bauer, *Some aspects of military line communications as deployed by the German armed forces prior to 1945. The History of Military Communications, Proceedings of the Fifth Annual Colloquium, Centre for the History of Defence Electronics, Bournemouth University, 24 September* (1999).
2. *Electromagnetic Pulse (EMP) and Tempest Protection for Facilities*, Engineer Pamphlet EP 1110-3-2, U.S. Army Corps of Engineers, Publications Depot, Hyattsville, December 31 (1990).
3. W. van Eck, Computers & Security **4**, 269 (1985).
4. P. Kocher, J. Jaffe, and B. Jun, *Differential Power Analysis*, in Advances in Cryptology, ed. by M. Wiener, CRYPTO'99, LNCS 1666, Springer (1999), p. 388.
5. P. Wright, *Spycatcher – The Candid Autobiography of a Senior Intelligence Officer*, William Heinemann Australia, Sidney (1987).
6. P. Smulders, Computers & Security **9**, 53 (1990).
7. M. G. Kuhn, *Compromising emanations: eavesdropping risks of computer displays*, Technical Report, Cambridge University, UCAM-CL-TR-577, **577** (2003).
8. C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, in *Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process.*, Bangalore, India (1984), p. 175.
9. R. Renner, arXiv/quant-ph:0512258 (2005).
10. M. Tomamichel, Ch. Ci Wen Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 1 (2012).
11. K. Tamaki, M. Curty, and M. Lucamarini, New J. Phys. **18**, 065008 (2016).
12. M. Pereira, M. Curty, and K. Tamaki, Nature Parther Journals, Quantum Information **62**, 1 (2019).
13. W. Wang, K. Tamaki, and M. Curty, New J. Phys. **20**, 083027 (2018).
14. S. N. Molotkov, Laser Phys. Lett. **17**, 015203 (2020).
15. K. S. Kravtsov and S. N. Molotkov, Phys. Rev. A **100**, 042329 (2019).
16. S. N. Molotkov and K. A. Balygin, Laser Phys. Lett. (2020), to be published.
17. С. Н. Молотков, ЖЭТФ **157**, 963 (2020).
18. F. Xu, X. Ma, Q. Zhang, H.-Kw. Lo, and J.-W. Pan, arXiv:1903.09051.
19. K. A. Balygin, A. N. Klimov, I. B. Bobrov, K. S. Kravtsov, S. P. Kulik, and S. N. Molotkov, Laser Phys. Lett. **15**, 095203 (2018).
20. К. А. Балыгин, А. Н. Климов, И.,Б. Бобров, С. Н. Молотков, М. И. Рыжкин, ЖЭТФ **157**, 195 (2020).
21. R. M. Wood, *Laser-induced damage of optical materials*, Taylor & Francis, N.Y., London (2003).
22. S. N. Molotkov, Laser Phys. Lett. **16**, 075203 (2019).
23. H. J. Landau and H. O. Pollak, Bell Syst. Techn. J. **40**, 65 (1961).
24. D. Slepian and H. O. Pollak, Bell Syst. Techn. J. **40**, 43 (1961).
25. W. H. J. Fuchs, J. Math. Anal. Appl. **9**, 317 (1964).
26. С. Н. Молотков, Письма в ЖЭТФ **11**, 608 (2020).
27. Л. Д. Ландау, Е. М. Лифшиц, *Статистическая физика*, Наука, М. (1995), т. V, ч. I.
28. С. Н. Молотков, Письма в ЖЭТФ **105**, 374 (2017).
29. С. Н. Молотков, ЖЭТФ **153**, 895 (2018).
30. A. S. Holevo, Probl. Inform. Transm. **9**, 177 (1973).
31. А. С. Холево, УМН **53** 193 (1998).
32. А. С. Холево, *Квантовые системы, каналы, информация*, МЦНМО, М. (2010).