Письма в ЖЭТФ, том 97, вып. 10, с. 693 – 699

О квантовомеханической границе на величину утечки информации по побочным каналам в квантовой криптографии

С. Н. Молотков

Академия криптографии РФ, 121552 Москва, Россия

Институт физики твердого тела РАН, 142432 Черноголовка, Россия

Факультет вычислительной математики и кибернетики, МГУ им. Ломоносова, 119991 Москва, Россия

Поступила в редакцию 11 марта 2013 г.
После переработки 15 апреля 2013 г.

Секретность криптографических ключей в системах квантовой криптографии гарантируется фундаментальными запретами квантовой механики. Квантовый канал, по которому передаются квантовые состояния, не контролируется, и подслушиватель может производить над ним любые модификации. К настоящему времени получены доказательства стойкости протоколов квантового распределения ключей [2, 3], включая реалистический случай конечной длины передаваемых последовательностей. Всегда предполагается, что подслушиватель не имеет ни прямого, ни опосредованного доступа к передающей и приемной аппаратуре. В реальности ситуация несколько иная. Приготовление и регистрация квантовых состояний происходят в соответствии со случайными последовательностями, которые генерируются на передающей и приемной станциях. Это приводит к электромагнитному излучению, регистрируя которое подслушиватель может получать дополнительную информацию о ключе. В работе установлена верхняя квантовомеханическая граница на величину информации подслушивателя о ключе, которая может быть получена через побочный канал.

DOI: 10.7868/S0370274X1310010X

Введение. Побочные каналы утечки (*side channels*) служат эффективным источником несанкционированного получения информации [1]. Источником информации может являться некоторое физическое устройство (источник акустического, механического, оптического, электромагнитного сигналов). Далее будем иметь в виду побочный канал утечки, связанный с излучением электромагнитного поля при генерации случайных чисел в квантовой криптографии. Насколько нам известно, в данном контексте этот вопрос до сих пор не обсуждался.

Для сокращения информации, которую подслушиватель может получить через побочный канал, прибегают к ослаблению и/или зашумлению исходного сигнала. В классической области нет фундаментальных запретов на копирование любого сигнала. Следовательно, любой слабый полезный сигнал путем создания множества копий может быть эффективно усилен и выделен из шума. По этой причине не существует верхней границы на величину утечки информации. Информация, которую может получить подслушиватель, зависит от технических свойств его детектирующей аппаратуры. Такая ситуация является принципиально неудовлетворительной. Никогда нельзя быть уверенным в том, что противная сторона не имеет аппаратуры с лучшими характеристиками, чем это изначально предполагалось.

Сформулируем основные вопросы. 1. Существует ли верхняя граница на величину утечки информации при заданных параметрах (например, ослаблении исходного сигнала), которая гарантировано не может быть увеличена подслушивателем при дальнейшем совершенствовании технологий? 2. Каким образом верхняя граница зависит от контролируемого легитимными пользователями ослабления сигнала, и можно ли уменьшить ее до любой наперед заданной малой величины?

Отметим принципиальное отличие подслушивания состояний в квантовом канале связи от детектирования состояний излучения в побочном канале.

А. При посылке информационных состояний в квантовый канал связи состояния контролируемым образом ослабляются так, чтобы в канал связи с приемной стороны направлялись квантовые состояния с известными свойствами. Б. На приемной стороне квантовые состояния измеряются. Цель измерений двояка: во-первых, получить информацию о передаваемом бите, а во-вторых, по наблюдаемым ошибкам оценить степень искажения квантовых состояний при передаче, а затем связать верхнюю границу информации подслушивателя о передаваемых состояниях с их наблюдаемыми искажениями. В. В дальнейшем степень искажения (верхняя граница информации подслушивателя) позволяет определить степень сжатия очищенного от ошибок ключа до финального секретного.

А. Если никак не заботиться о состояниях (обычно это даже не обсуждается), то в побочный канал, выходят состояния с неконтролируемой интенсивностью. В дальнейшем за детектированием и искажениями этих состояний легитимные пользователи не следят. Поэтому сразу необходимо ослабить состояния до такого уровня, чтобы информация о ключе, которую может получить подслушиватель, была бы сколь угодно малой. Фактически необходимо превратить классический побочный канал в квантовый. Принципиально важно, что на практике не требуется полной экранировки состояний в побочном канале, поскольку сделать это невозможно. Уровень сигнала в побочном канале позволяет выбрать такую степень сжатия ключа при которой будет полностью устранена информация подслушивателя о ключе, получаемая им из побочного канала.

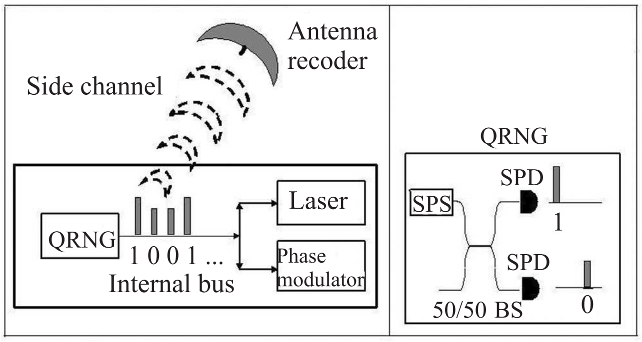
В первом случае цель подслушивателя – получить максимум информации о ключе из квантового канала и произвести минимум искажений передаваемых состояний, а во втором – получить максимум информации о состояниях из побочного канала, не заботясь о вносимых при этом искажениях.

В обоих случаях для устранения информации используется универсальное хэширование. В случае побочного канала такое хэширование не обсуждалось и не использовалось.

Неформальная постановка задачи. Уточним постановку задачи применительно к системам квантового распределения ключей. Одним из главных элементов в системах квантовой криптографии на передающей и приемной стороне являются независимые генераторы случайных чисел 0 и 1. В соответствии с этими случайными последовательностями происходят приготовление квантовых состояний на передающей стороне и выбор измерения на приемной. При этом всегда подразумевается, что последовательности случайных чисел *полностью недоступны* для подслушивателя. Не имея возможности вскрытия аппаратуры и непосредственного чтения последовательностей, подслушиватель может иметь опосредованный доступ к данным последовательностям через побочный канал.

Существует множество различных физических методов получения случайных чисел. Большое количество методов сводится к оцифровке некоторого шумового классического сигнала (например, шума тока в канале полевого транзистора). Однако если детально проанализировать физическую причину появления самого классического шума, то окажется, что истинная причина его появления на классическом уровне имеет квантовое происхождение. В классической физике истинная случайность отсутствует. Логически это связано с тем, что в классической физике эволюция системы независимо от ее сложности описывается дифференциальными уравнениями и состояние системы однозначно определяется начальными условиями. В квантовой физике ситуация принципиально иная. Даже при одинаковом приготовлении начального состояния и дальнейшей эволюции, которая также описывается дифференциальными уравнениями, квантовомеханическое измерение носит принципиально непредсказуемый результат. В этом смысле любая истинная случайность имеет квантовую природу.

Для того чтобы понять причину побочного излучения, рассмотрим пример выработки случайной последовательности. Один из способов генерации случайной последовательности 0 и 1 состоит в регистрации однофотонных состояний (реально квазиоднофотонных, однако пока это неважно) на одном из выходов волоконного светоделителя (см. рисунок). В



Схематическое представление генерации и передачи случайных чисел на передающей стороне: QRNG – квантовый генератор случайных чисел, SPS – источник однофотонных или квазиоднофотонных состояний, SPD – фотодетектор

данном методе в явном виде используется принципиальная фундаментальная неопределенность квантовомеханического исхода измерений. Если однофотонный пакет распространяется по двум различным путям, то регистрация имеет место случайно и принципиально непредсказуемо только в одном пути. Исход в одном плече светоделителя интерпретируется как логический 0, а в другом – как логическая 1.

При строго однофотонном пакете исходы измерений и возникающая последовательность 0 и 1 являются истинно случайными и равномерно распределенными. Регистрация фотона приводит к импульсу тока в одном из SPD-детекторов, который после необходимого усиления передается по внутренней шине (*internal bus*) на другие устройства управления (см. рисунок). Таким образом, случайные числа возникают *только в момент регистрации* (*измерения*) *фотона* (протекания импульса тока в фотодетекторе). До этого момента случайных чисел еще нет.

Излучение возникает уже в момент протекания тока через фотодетектор. Однако это не основной канал побочного излучения. Случайные биты 0 или 1 (импульсы тока после регистрации фотона в соответствующем фотодетекторе) по внутренней шине передаются в другие устройства (управления лазером, фазовым модулятором и т.д.). При передаче импульсов по шине логическим 0 и 1 отвечают разные уровни напряжения. Передача по проводникам внутренней шины ведет к интенсивному побочному излучению электромагнитного поля, которое может регистрироваться подслушивателем.

Квантовые состояния излучения в побочном канале. При ослаблении интенсивности классических полей неизбежно возрастает доля вакуумной компоненты, что должно приводить к увеличению ошибки различения двух состояний поля. Очевидно, что при предельно сильном ослаблении поле в основном содержит вакуумную компоненту. В отсутствие фотонов состояние поля есть просто вакуумное состояние. При квантовомеханическом рассмотрении даже "классические" квантовые состояния с макроскопически большим средним числом фотонов не являются идеально различимыми в силу присутствия вакуумной компоненты. Однако вероятность ошибки при различении таких состояний ничтожна мала. Две квантовые наблюдаемые (матрицы плотности) достоверно различимы, если они имеют носители в ортогональных подпространствах, т.е. их носители не перекрываются, $\mathrm{supp}(\rho_0) \cap \mathrm{supp}(\rho_1) = \emptyset$. В общем случае минимальная ошибка различения двух квантовых состояний, ρ_0 и ρ_1, равна (детали см. в [4])

$$Q_{\min} = \pi_0 + \sum_{\lambda_j < 0} \lambda_j, \tag{1}$$

где λ_j – собственные числа оператора $\pi_1\rho_1 - \pi_0\rho_0$, $\pi_{0,1}$ – вероятности, с которыми приготавливаются матрицы плотности $\rho_{0,1}$. Из (1) видно, что если носители матриц плотности не перекрываются, то ошибка различения равна 0. Увеличение вакуумной компоненты при ослаблении неизбежно приведет к уменьшению различимости пары состояний при измерениях.

Поскольку при приготовлении случайных чисел фиксирована только мощность сигнала, состояние излучения описывается не чистым состоянием, а матрицей плотности. Отвечающие 0 и 1 матрицы плотности электромагнитного излучения, которое может быть зарегистрировано во всех телесных углах, можно записать в виде (см., например, [5])

$$\rho^{(0,1)} = \sum_{\omega} \left(\sum_{m_\omega = 0}^{N_\omega^{(0,1)}} p_{m_\omega}^{(0,1)} |m_\omega\rangle\langle m_\omega| \right), \tag{2}$$
$$\langle m_\omega | n_{\omega'} \rangle = \delta_{m_\omega, n_{\omega'}},$$

где $|n_{\omega'}\rangle$ – фоковское состояние с числом фотонов n_ω в частотной моде ω. Условие нормировки матриц плотности имеет вид $\sum_\omega \left(\sum_{m_\omega=0}^{N_\omega^{(0,1)}} p_{m_\omega}^{(0,1)} \right) = 1$. Здесь $N_\omega^{(0,1)}$ – максимальное число фотонов в спектральной моде с частотой ω для состояний, отвечающих 0 и 1, $p_{m_\omega}^{(0,1)}$ – вероятность (доля фотонов в спектральной компоненте с частотой ω). Вакуумной компоненте поля отвечают коэффициенты $p_{m_\omega}^{(0,1)}$ с нулевыми фоковскими числами заполнения, $m_\omega = 0$.

Конкретная структура матрицы плотности излучения, возникающего при передаче импульсов напряжения, отвечающих 0 или 1, по шине данных или межмодульным соединениям, определяется видом кабеля и т.д. Она может быть получена путем решения соответствующей электродинамической задачи для данного устройства, которое дает конкретные числовые коэффициенты $p_{m_\omega}^{(0.1)}$ матрицы плотности. Последние мы будем считать известными. Их точный вид для получения общего ответа нам не потребуется.

Исходные неослабленные квантовые состояния излучения "привязаны" к случайной битовой строке $X = \{0,1\}^{N_{\text{key}}}$ (N_{key} – длина строки):

$$(|x\rangle \otimes \rho^{(x)})^{\otimes N_{\text{key}}} = (|x_{i_1}\rangle \otimes \rho^{(x_{i_1})}) \otimes (|x_{i_2}\rangle \otimes \otimes \rho^{(x_{i_2})}) \otimes \ldots \otimes (|x_{N_{\text{key}}}\rangle \otimes \rho^{(x_{N_{key}})}). \tag{3}$$

Для дальнейшего удобно поставить в соответствие классическим битам $x = 0, 1$ ортогональные достоверно различимые квантовые состояния $|x\rangle$, *доступные только легитимным пользователям.*

Пусть коэффициент ослабления спектральной компоненты за счет экранировки аппаратуры есть T_ω. Совместное состояние исходного излучения и аппаратуры до поглощения является единым квантовым состоянием. Аппаратура легитимных пользователей, в которой происходит ослабление, имеет макроскопически большое число степеней свободы, по которым происходит усреднение. Поэтому после поглощения состояние излучения описывается матрицей плотности. При экранировке каждая спектральная компонента преобразуется следующим образом (см., например, [6]):

$$|m_\omega\rangle\langle m_\omega| \to \sum_{k_\omega=0}^{m_\omega} C_{k_\omega}^{m_\omega} T_\omega^{k_\omega}(1-T_\omega)^{m_\omega-k_\omega}|k_\omega\rangle\langle k_\omega|. \quad (4)$$

Матрица плотности, доступная подслушивателю, имеет вид

$$\rho_E^{(0,1)} = \quad (5)$$

$$= \sum_\omega \left[\sum_{m_\omega=0}^{N_\omega^{(0,1)}} p_{m_\omega}^{(0,1)} \sum_{k_\omega=0}^{m_\omega} C_{k_\omega}^{m_\omega} T_\omega^{k_\omega}(1-T_\omega)^{m_\omega-k_\omega}|k_\omega\rangle\langle k_\omega| \right].$$

Фактически это означает, что доля T_ω каждой спектральной компоненты поглощается в результате экранировки и оказывается недоступной подслушивателю, а доля $1 - T_\omega$ покидает аппаратуру и становится доступной подслушивателю. При условии сильного затухания в системе, $\max_\omega\{N_\omega^{(0,1)} T_\omega\} \ll 1$, с точностью до членов, линейных по T_ω, находим

$$|m_\omega\rangle_{AA}\langle m_\omega| \to (1-T_\omega)^{m_\omega}(|\mathrm{vac}\rangle\langle\mathrm{vac}| + \\ + m_\omega T_\omega |1_\omega\rangle_{EE}\langle 1_\omega|), \quad (6)$$

где $|\mathrm{vac}\rangle$ – вектор вакуумного состояния поля, общего для всех ω. В пределе малых чисел заполнения матрица плотности (5) становится равной

$$\rho_E^{(0,1)} = \left[(1-\overline{N}^{(0,1)})|\mathrm{vac}\rangle\langle\mathrm{vac}| + \sum_\omega \overline{N}_\omega^{(0,1)} |1_\omega\rangle\langle 1_\omega| \right], \quad (7)$$

где среднее число заполнения по частотным модам $\overline{N}_\omega^{(0,1)} = \sum_{m_\omega}^{N_\omega^{(0,1)}} p_{m_\omega}^{(0,1)} m_\omega T_\omega \ll 1$, $\overline{N}^{(0,1)} = \sum_\omega \overline{N}_\omega^{(0,1)}$. Корреляция между случайной битовой строкой длины N_{key} и квантовыми состояниями подслушивателя в побочном канале дается тензорным произведением, аналогичным (3), где фигурирует матрица плотности $\rho_{XE} = \sum_{x=0,1} |x\rangle\langle x| \otimes \rho_E^{(x)}$.

Индивидуальные измерения. Для подслушивателя задача сводится к различению двух матриц плотности, $\rho_E^{(0)}$ и $\rho_E^{(1)}$. При индивидуальных измерениях состояния излучения в каждой позиции минимальная ошибка различения при равномерном распределении 0 и 1 на генераторе случайных чисел ($\pi_0 = \pi_1 = 1/2$) с учетом (7) равна

$$Q_{\min} = (1-q)/2. \quad (8)$$

Здесь q определяется отрицательными собственными числами $\rho_E^{(0)} - \rho_E^{(1)}$. С учетом (7) $q = |(1-\overline{N}^{(0)}) - (1-\overline{N}^{(1)})|$. Поскольку матрицы плотности нормированы на единицу, имеем $(1-\overline{N}^{(0)}) - (1-\overline{N}^{(1)}) = -\left[(\sum_\omega \overline{N}_\omega^{(0)}|1_\omega) - (\sum_\omega \overline{N}_\omega^{(1)}|1_\omega]\right]$. При индивидуальных измерениях состояния побочного излучения в каждой отдельной позиции подслушиватель и легитимные пользователи находятся в ситуации классического бинарного симметричного канала с вероятностью ошибки Q_{min}. Среднее количество $I(A;E)$ бит информации на одну позицию (взаимная информация) между легитимными пользователями (A) и подслушивателем (E), которые может получить подслушиватель, ограничено классической пропускной способностью [7]. Оно определяется только ошибкой $Q_{\min}$ и не превосходит

$$I(A;E) < C_{cl}(Q_{\min}) = \\ = -Q_{\min}\log Q_{\min} - (1-Q_{\min})\log(1-Q_{\min}), \quad (9)$$

причем $I(A;E)$ стремится к единице при $Q_{\min} \to 0$.

Коллективные измерения. Граница (9) не является верхней границей информации в квантовой механике, поскольку никто не ограничивает подслушивателя только индивидуальными измерениями. Квантовая механика допускает более мощные коллективные измерения. При этом подслушиватель проводит измерения сразу над всей последовательностью квантовых состояний излучения, используя квантовую память, а затем проводя измерения над ней как над единым квантовым состоянием. Тогда задача подслушивателя сводится к различению целых последовательностей квантовых состояний. В этом случае легитимные пользователи и подслушиватель находятся в ситуации квантово-классического канала связи. Верхняя граница информации, которую может извлечь подслушиватель при таких измерениях, ограничена фундаментальной величиной Холево, $\chi(\rho_E^{(0,1)})$ [4]. Последняя является достижимой при коллективных измерениях и дает верхнюю границу для классической информации, которая может быть получена из ансамбля квантовых состояний [4]. Итак, имеем

$$I(A;E) < \chi(\rho_E^{(0,1)}) = \overline{C} = \\ = H\left[(\rho_E^{(0)} + \rho_E^{(1)})/2\right] - \left[H(\rho_E^{(0)}) + H(\rho_E^{(1)})\right]/2, \quad (10)$$

где $H(\rho) = -\mathrm{Tr}\{\rho\log\rho\}$ – энтропия фон Неймана. Фундаментальная граница (10) диктуется только законами квантовой механики. Отметим, что величина (10) совпадает с *классической пропускной способностью квантово-классического канала связи*. Как было отмечено в [8], в квантовой механике в отличие от классических каналов, возможен бесконечный набор пропускных способностей $\overline{C}_n$ $(n = 1, 2, ...)$, причем $\overline{C}_1 \leq \overline{C}_2 \leq ... \leq \overline{C}$. Данный набор отличается измерениями. Величина $\overline{C}_1$ возникает, если подслушиваетль выполняет только индивидуальные измерения в каждой позиции, что дает пропускную способность за один шаг (*one shot*) $\overline{C}_1 = C_{\mathrm{cl}}(Q_{\min})$. Величина $\overline{C}_2$ возникает, если подслушиватель выполняет измерения над двумя позициями сразу, и т.д. Величина $\overline{C}$ определяется измерениями сразу над всей последовательностью и дает верхнюю границу информации доступную подслушивателю.

Вместе с тем малость взаимной информации, вообще говоря, не гарантирует того, что подслушиватель не знает отдельные биты достоверно, что неприемлемо для ключей. Данный эффект является чисто квантовомеханическим и носит название "захват информации" (*information locking*) [9]. В результате даже после ослабления побочного излучения до некоторого уровня все равно необходимо дополнительное устранение остаточной информации. Для этого требуется более "тонкая" величина, чем взаимная информация. Такой инструмент дает замечательная теорема об остатке хэширования [10].

Устранение информации подслушивателя из побочного канала. После измерения состояния излучения в побочном канале подслушиватель имеет битовую строку, которая частично коррелирована с битовой строкой легитимных пользователей. Идея состоит в том, что легитимные пользователи посредством сжатия (хэширования) исходной битовой строки, о которой подслушиватель имеет частичную информацию, получают битовую строку меньшей длины, о которой подслушиватель никакой информации не имеет (точнее, имеет сколь угодно малую информацию по желанию легитимных пользователей). *Принципиально, что такое сжатие производится в открытую, т.е. считается, что подслушиватель знает все шаги этой процедуры и саму хэш-функцию.* После этого оказывается, что расстояние до идеальной ситуации становится экспоненциально малым по параметру, который легитимные пользователи выбирают сами.

В результате измерений подслушивателем квантового состояния поля степень корреляции между битовой последовательностью $(|x\rangle\langle x|)^{\otimes n}$ и последовательностью описывается матрицей плотности $\rho_{XE}^{\otimes n}$. Если корреляции полностью отсутствуют (идеальная ситуация), то совместная матрица распадается на тензорное произведение $\rho_X^{\otimes n} \otimes \rho_E^{\otimes n}$. Степень корреляции удобно описывать следовым расстоянием до идеальной ситуации (см., например, [11]):

$$d_1(\rho_{XE}^{\otimes n}, \rho_X^{\otimes n} \otimes \rho_E^{\otimes n}) = \frac{1}{2}||\rho_{XE}^{\otimes n} - \rho_X^{\otimes n} \otimes \rho_E^{\otimes n}||_1, \quad (11)$$

где $||A||_1 = \mathrm{Tr}\{\sqrt{AA^+}\}$, A – эрмитов оператор. В нашей ситуации $\rho_X^{\otimes n} = \frac{1}{2^{N_{key}}} \sum_x (|x\rangle\langle x|)^{\otimes n}$ отвечает равномерному распределению и $\rho_E^{\otimes n} = \mathrm{Tr}_X\{\rho_{XE}^{\otimes n}\}$. Важно, что в результате любых манипуляций над последовательностью $(|x\rangle\langle x|)^{\otimes n}$ следовое расстояние не может увеличиваться, любые преобразования битовой строки $(|x\rangle\langle x|)^{\otimes n}$ приведут только к уменьшению степени корреляций.

Уменьшение корреляций может быть достигнуто посредством сжатия (хэширования) битовой строки $\{x\}_{\mathrm{key}}^N$ $((|x\rangle\langle x|)^{\otimes N_{\mathrm{key}}})$ до битовой строки $\{z\}^{N_{\mathrm{sec}}}$ $((|z\rangle\langle z|)^{\otimes N_{\mathrm{sec}}}, z = 0, 1)$ меньшей длины N_{sec}. Оно описывается отображением при помощи случайных универсальных хэш-функций второго порядка, введенных в [12]:

$$f: \quad X = \{0,1\}_{\mathrm{key}}^N \to Z = \{0,1\}^{N_{\mathrm{sec}}}, \quad (12)$$

где множество хэш-функций $f \in F$. При этом сама хэш-функция f является случайной величиной, которая открыто, случайно и равновероятно выбирается из множества F. *Таким образом, подслушиватель знает выбор функции.* Данные хэш-функции второго порядка обладают следующим свойством:

$$\mathrm{Pr}_f[f(\hat{x}) = f(x)] \leq \frac{1}{|Z|} = 2^{-N_{\mathrm{sec}}}, \quad \hat{x} \neq x, \quad (13)$$

т.е. вероятность иметь одно и то же хэш-значение при различных значениях аргумента не превышает (13). Иначе говоря, вероятность того, что разные исходные битовые строки $\{x\}^{N_{\mathrm{key}}}$ и $\{\hat{x}\}^{N_{\mathrm{key}}}$ перейдут в одну и ту же битовую строку $\{z\}^{N_{\mathrm{sec}}}$ не превышает (13). *Величина сжатия определяется сглаженной min-энтропией.* По определению min-энтропии (подробности см. в [11])

$$H_{\min}(X|E) = -\sup_{\sigma_E} \log \lambda, \quad (14)$$

где λ – минимальное число, при котором оператор $\lambda I_X \otimes \sigma_E - \rho_{XE} > 0$. Здесь σ_E и ρ_{XE} – матрицы плотности, действующие в $\mathcal{H}_E$ и $\mathcal{H}_X \otimes \mathcal{H}_E$, I_X – единичный оператор в $\mathcal{H}_X$. По определению [11] сглаженная min квантовая энтропия равна

$$H_{\min}^{\varepsilon}(X|E) = \sup_{\overline{\rho}_{XE} \in \mathcal{B}^{\varepsilon}(\rho_{XE})} H_{\min}(X|E)_{\overline{\rho}_{XE}}, \quad (15)$$

где точные верхняя и нижняя грани берутся по всем матрицам плотности $\overline{\rho}_{XE}$, находящимся в шаре $\mathcal{B}^{\varepsilon}(\rho_{XE})$ радиуса ε с центром в ρ_{XE}, $\mathcal{B}^{\varepsilon}(\rho_{XE}) = \{\overline{\rho}_{XE} : ||\rho_{XE} - \overline{\rho}_{XE}||_1 \leq \mathrm{Tr}\{\overline{\rho}_{XE}\} \cdot \varepsilon\}$. *Указанная энтропия имеет прозрачный операциональный смысл* (детали см. в [13]), *если одна из подсистем, например X, является классической битовой строкой и $\varepsilon \to 0$. Тогда $H^{\varepsilon}_{\min}(X|E)$ равна числу случайных равномерно распределенных бит, которые можно получить из строки X и которые теперь никак не коррелированы с квантовой подсистемой E.* Согласно теореме о хэшировании (теорема Leftover Hash [10]) расстояние до идеальной ситуации после сжатия становится равным

$$d_1(\rho_{ZE_z}, \rho_Z \otimes \rho_{E_z}) = \frac{1}{2}||\rho_{ZE_z} - \rho_Z \otimes \rho_{E_z}||_1 < \\ < \varepsilon + \frac{1}{2}\sqrt{2^{N_{\text{sec}} - H^{\varepsilon}_{\min}(\rho^{\otimes N_{\text{key}}}_{XE}|\rho^{\otimes N_{\text{key}}}_{E})}}, \quad (16)$$

где матрица плотности после хэширования

$$\rho_{ZE_z} = \sum_f \sum_z p_f |f\rangle\langle f| \otimes |z\rangle\langle z| \otimes \rho^z_E, \\ \rho^z_{E_z} = \sum_{x: f^{-1}(x) = z} \rho^x_E, \quad (17) \\ p_f = \frac{1}{|F|}, \quad \rho^z_{E_z} = \sum_{x, x = f^{-1}(z)} \rho^x_E.$$

Здесь $\rho_{E_z} = \mathrm{Tr}_Z\{\rho_{ZE_z}\}$ – матрица плотности подслушивателя после хэширования, ρ_Z – матрица плотности, отвечающая однородному распределению Z, аналогичная ρ_X. В (17) для удобства введены ортогональные квантовые состояния $|f\rangle$, отвечающие конкретной хэш-функции f. Один из способов реализации хэш-функции, хотя вычислительно далеко и не самый экономный (см. [14]), состоит в умножении по модулю 2 битовой строки длиной N_{key} на выбираемую открыто случайную матрицу из 0 и 1 размером $N_{\text{sec}} \times N_{\text{key}}$. В результате возникает битовая строка длины N_{sec}. Интуитивно достаточно очевидно, что поскольку в новую строку переходят примерно $2^{N_{\text{key}}}/2^{N_{\text{sec}}}$ строк, лишь частично известных подслушивателю, его информация о новой строке меньшей длины может только уменьшиться. Если длина новой сжатой битовой строки не превышает

$$N_{\text{sec}} \le H^{\varepsilon}_{\min}(\rho^{\otimes N_{\text{key}}}_{XE}|\rho^{\otimes N_{\text{key}}}_{E}) - 2\log\frac{1}{2\varepsilon}, \quad (18)$$

то расстояние до идеальной ситуации не превосходит

$$d_1(\rho_{ZE_z}, \rho_Z \otimes \rho_{E_z}) = \frac{1}{2}||\rho_{ZE_z} - \rho_Z \otimes \rho_{E_z}||_1 \le 2\varepsilon. \quad (19)$$

Для конкретных вычислений необходимо иметь оценку для сглаженной min-энтропии. Согласно [11]

$$\frac{1}{N_{\text{key}}} H^{\varepsilon}_{\min}\left(\rho^{\otimes N_{\text{key}}}_{XE}|\rho^{\otimes N_{\text{key}}}_{E}\right) \ge H(\rho_{XE}) - H(\rho_E) - \delta, \quad (20)$$

где $\delta = [2H_{\max}(\rho_X) + 3]\sqrt{\frac{\log 1/\varepsilon}{N_{\text{key}}} + 1}$, $H_{\max}(\rho_X) = \log \mathrm{rank}(\rho_X)$. Энтропии фон Неймана в (20) могут быть вычислены. Учитывая, что $\pi_0 = \pi_1 = 1/2$, находим $H(\rho_{XE}) = 1$ и

$$\rho_{XE} = \sum_{x=0,1} \pi_x |x\rangle\langle x| \otimes \rho^{(x)}_E = \\ = \frac{1}{2}\left(|0\rangle\langle 0| \otimes \rho^{(0)}_E + |1\rangle\langle 1| \otimes \rho^{(1)}_E\right),$$

$$\rho_E = \mathrm{Tr}_X\{\rho_{XE}\} = \frac{1}{2}\left(\rho^{(0)}_E + \rho^{(0)}_E\right), \quad (21)$$

$$H(\rho_E) = -\lambda_{\text{vac}}\log\lambda_{\text{vac}} - \textstyle\sum_\omega \lambda_\omega \log\lambda_\omega, \\ \lambda_{\text{vac}} = 1 - (\overline{N}^{(0)} + \overline{N}^{(1)})/2, \quad (22) \\ \lambda_\omega = (\overline{N}^{(0)}_\omega + \overline{N}^{(1)}_\omega)/2.$$

Поскольку пространство $\mathcal{H}_X$ двумерно, $\log \mathrm{rank}(\rho_X) = 1$. Соотношения (20)–(22) связывают степень сжатия исходной последовательности N_{key} до величины N_{sec} с параметрами побочного излучения. При этом расстояние ε до идеальной ситуации может быть сделано сколь угодно малым. Сжатие приводит к тому, что вероятность для подслушивателя знать сжатую строку превышает вероятность угадывания не более чем на сколь угодно малую величину 2ε.

Некоторые примеры. Пусть состояния излучения в побочном канале представляют собой чистые состояния. Такой пример является идеализированным, но делает качественную интерпретацию результатов физически прозрачной. Чистые состояния могут быть записаны в виде $\rho^{(0,1)}_E = |\varphi_{0,1}\rangle\langle\varphi_{0,1}|$, $|\varphi_{0,1}\rangle = \lambda^{(0)}_{\text{vac}}|\text{vac}\rangle + \sum_{n_\omega} \lambda^{(0,1)}_{n_\omega}|n_\omega\rangle\langle n_\omega|$. Единственным существенным параметром здесь является скалярное произведение состояний, определяющее меру неортогональности (достоверной неразличимости) состояний, $\zeta = |\langle\varphi_0|\varphi_1\rangle| = |\lambda^{(0)}_{\text{vac}}\lambda^{(1)}_{\text{vac}} + \sum_{n_\omega} \lambda^{(0)}_{n_\omega}\lambda^{(1)}_{n_\omega}|$. В этом случае формулы для информации подслушивателя принимают простой вид.

Для индивидуальных измерений взаимная информация в (9) принимает вид $I(A,E) \le C_{\text{cl}} = \frac{1}{2}[(1 + \sqrt{1-\zeta^2})\log(1+\sqrt{1-\zeta^2}) + (1-\sqrt{1-\zeta^2}) \times \log(1 - \sqrt{1-\zeta^2})]$. Для *коллективных измерений* $I(A,E) \le \chi = \overline{C} = -\left[\left(\frac{1-\zeta}{2}\right)\log\left(\frac{1-\zeta}{2}\right) + \left(\frac{1+\zeta}{2}\right)\log\left(\frac{1+\zeta}{2}\right)\right]$. При этом всегда $\overline{C} \ge C_{\text{cl}}$.

Min-энтропия. Величина min-энтропии в (20) в этом случае равна $\frac{1}{N_{\text{key}}} H^{\varepsilon}_{\min}\left(\rho^{\otimes N_{\text{key}}}_{XE}|\rho^{\otimes N_{\text{key}}}_{E}\right) \ge 1 - \overline{C} - \delta$. Таким образом, в случае чистых состояний все определяется единственной величиной $\overline{C}$ – классической пропускной способностью квантового канала $(x, \quad |x\rangle \to \rho_E^x)$ между источником случайных чисел и подслушивателем, которая совпадает с величиной Холево [4].

Заключение. Итак, величина $\overline{C}$ определяет верхнюю границу информации, которая лимитируется фундаментальными законами квантовой механики и которую можно извлечь из квантового ансамбля. Если длина случайной классической последовательности X – N_{key} $(X = \{0,1\}^{N_{\text{key}}})$, то подслушиватель в среднем *знает* не более $N_{\text{key}}\overline{C}$ бит из этой последовательности и *не знает* $N_{\text{key}}(1-\overline{C})$ бит. После сжатия этой последовательности до длины $N_{\text{sec}} \le N_{\text{key}}(1-\overline{C})$ (16), не превосходящей числа бит, неизвестных подслушивателю, расстояние до идеальной ситуации (полного отсутствия корреляции между последовательностью легитимных пользователей и последовательностью подслушивателя) в (16) становится экспоненциально малым по параметру $2^{-N_{\text{key}}[l_{\text{sec}}-(1-\overline{C})]}$. *Другими словами, длина секретной строки не может быть больше числа $N_{key}(1-\overline{C})$ бит, неизвестных подслушивателю. Последнее определяется только характеристиками побочного излучения (5), (7) и не зависит от каких-либо предположений о технических возможностях подслушивателя.*

Основным выводом настоящей работы является то, что существующие доказательства секретности протоколов квантовой криптографии должны быть снабжены дополнительным сжатием ключей для устранения информации подслушивателя о ключе, получаемой им из побочного канала. Дополнительное сжатие ключей диктуется фундаментальными ограничениями квантовой механики и определяется только интенсивностями спектральных компонент поля.

Выражаю благодарность коллегам по Академии криптографии Российской Федерации за постоянную поддержку.

1. M. G. Kuhn, *Compromising emanations: eavesdropping risks of computer displays*, Technical Report, Cambridge Ubiv., UCAM-CL-TR-577, ISSN 1476-2986, # 577, 2003.
2. M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nature Communications **3**, 634 (2011).
3. С. Н. Молотков, ЖЭТФ **142**, 19 (2012).
4. А. С. Холево, *Введение в квантовую теорию информации*, сер. *Современная математическая физика*, вып. 5, М.: МЦНМО, 2002; Успехи математических наук **53**, 193 (1998).
5. R. Loudon, *The Quantum Theory of Light*, Clarendon Press, Oxford, 1973.
6. Л. Мандель, Э. Вольф, *Оптическая когерентность и квантовая оптика*, М.: Физматлит, 2000, 895 с. [L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*, Cambridge University Press, 1995].
7. Р. Галлагер, *Теория информации и надежная связь*, М.: Сов. радио, 1974 [R. G. Gallager, *Information Theory and Reliable Communication*, Wiley, N.Y., 1968].
8. P. Shor, arXiv:quant-ph/0304102.
9. R. König, R. Renner, A. Dariska, and U. Maurer, Phys. Rev. Lett. **98**, 140502-1 (2007).
10. M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, arXiv/quant-ph: 10022436.
11. R. Renner, arXiv/quant-ph: 0512258.
12. J. L. Carter and M. N. Wegman, Journal of Computer and System Sciences **18**, 143 (1979).
13. R. König, R. Renner, and C. Schaffner, arXiv/quant-ph: 08071338.
14. C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. on Inf. Theory **41**, 1915 (1995).