ЖЭТФ, 2016, том 150, вып. 5 (11), стр. 903–916

ОДНОРАЗОВЫЙ БЛОКНОТ, СЛОЖНОСТЬ ПЕРЕБОРА КЛЮЧЕЙ И ПРАКТИЧЕСКАЯ СЕКРЕТНОСТЬ КВАНТОВОЙ КРИПТОГРАФИИ

С. Н. Молотков*

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

Академия криптографии Российской Федерации
121552, Москва, Россия

Факультет вычислительной математики и кибернетики,
Московский государственный университет им. М. В. Ломоносова
119899, Москва, Россия

Поступила в редакцию 31 мая 2016 г.

Показана прямая связь между сложностью полного перебора ключей, который является одним из основных критериев секретности в классических системах, и следовым расстоянием, используемым в квантовой криптографии. Приведены границы для минимального и максимального числа шагов перебора, за которое определяется истинный ключ.

DOI: 10.7868/S0044451016110079

1. ВВЕДЕНИЕ

Квантовая механика открыла новые возможности для вычислений [1–3]. Интерес к квантовым вычислениям возник после работы Шора [3], где было показано, что задача факторизации из класса задач с экспоненциальной сложностью по размеру входных данных (по крайней мере, для известных классических алгоритмов) переходит в разряд задач с полиномиальной сложностью. Последнее означает, что системы асимметричной криптографии с открытыми ключами, которые широко используются в информационных технологиях, оказываются не криптостойкими. Другим важным квантовым алгоритмом является алгоритм поиска Гровера [4] в неструктурированной базе данных. Число классических алгоритмов, которые ускоряются на квантовом компьютере, имеет меру нуль [5]. Позднее было показано, что квантовые алгоритмы могут быть использованы для моделирования квантовых систем [6]. На сегодняшний день существует несколько десятков квантовых алгоритмов [7].

Другим примером использования фундаментальных законов квантовой механики в теории информации является квантовая криптография — квантовое распределение ключей [8], — которая в отличие от квантовых вычислений имеет значительные практические продвижения. Если когда-то будет создан квантовый компьютер, то криптостойкость систем с открытыми ключами окажется под вопросом. Для серьезных целей используются симметричные системы шифрования с секретными ключами. Существует единственный способ шифрования, который гарантирует выживаемость даже при создании квантового компьютера — шифрование в режиме одноразового блокнота. Идея шифрования в режиме одноразового блокнота проста и является одним из немногих точно доказанных результатов в классической криптографии. Впервые идея была предложена Вернамом в 1926 г., но без доказательства (бегущие ключи — running keys) [9]. Независимо она предложена и доказана В. А. Котельниковым (19 июня 1941 г.) [10]; затем независимо — К. Шенноном в 1945 г. (опубликовано в 1949 г.) [11].

Если две стороны A и B имеют общий секретный ключ k (k — случайная битовая строка длины n), то шифрование сообщения m (m — также битовая

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

строка) на стороне A происходит по правилу

$$c = m \oplus k,$$

где c — шифр, также битовая строка. Расшифрование на стороне B происходит как

$$m = c \oplus k = m \oplus (k \oplus k).$$

Если длина ключа в битах не меньше длины сообщения и ключ используется только один раз, то такой способ шифрования не может быть дешифрован (взломан) даже теоретически при условии, что ключ идеально случайный, т. е. вероятность любого ключа есть

$$P_K(k) = \frac{1}{2^n}.$$

В этом случае вероятность появления шифра c не зависит от сообщения (ключ подслушивателю неизвестен):

$$P(c|m) = P_K(k) = \frac{1}{2^n}.$$

Это означает, что подслушиватель каждый раз видит случайную битовую строку, никак не коррелированную с сообщением.

Неформально это означает, что подслушиватель, зная только c, видит случайную строку битов длины n. При этом данный шифр-текст равновероятно может произойти из любого открытого сообщения. Фактически подслушиватель, зная c, может перепробовать все 2^n ключей, получить все сообщения и наугад выбрать любое.

Проблема шифрования в режиме одноразового блокнота состоит в постоянной генерации и распределении ключей между пространственно-удаленными пользователями и гарантировании секретности ключей. Для распределения секретных ключей нужен защищенный канал связи, для защищенного канала связи нужны секретные ключи. Возникает замкнутый круг.

Квантовая криптография разрывает этот замкнутый круг. Законы квантовой механики позволяют распределять ключи и гарантировать их секретность на уровне фундаментальных законов природы через открытый и доступный для прослушивания и модификации квантовый канал связи. В квантовой криптографии используется еще вспомогательный открытый классический канал связи. Классический открытый канал должен быть аутентичным. Аутентичность — более слабый криптографический примитив, чем общий секретный ключ, который является самым сильным криптографическим примитивом, из которого могут быть построены все остальные.

Однако реальная ситуация несколько отличается от идеальной. Ключи, которые получаются в результате квантового распределения, не являются идеально случайными[1)]. Квантовая механика гарантирует, что они являются лишь ε-секретными [12] (см. ниже). Это означает, что ключи не только не идеально случайны, но и не являются полностью неизвестными подслушивателю. ε-секретность ключей означает, что корреляции между общим ключом легитимных пользователей и «слепком» ключа подслушивателя сколь угодно малы (ε-малы в определенной метрике). Параметр секретности ε может быть выбран наперед сколь угодно малым. Сразу же возникает следующий вопрос — какой длины должен быть сырой ключ, из которого сжатием (хэширование при помощи универсальных хэш-функций второго порядка) получается секретный ключ нужной длины, чтобы обеспечить заданную величину ε. Фактически это вопрос о масштабировании ε как функции финального секретного ключа и исходного сырого ключа. Если эта зависимость степенная, то экспоненциальное приближение ε к нулю потребует экспоненциально большой длины исходного сырого ключа, что практически неприемлемо. Если экспоненциальное приближение ε к нулю потребует линейного увеличения длины сырого ключа, то приближение к идеальной ситуации при шифровании в режиме одноразового блокнота практически реализуемо с линейной сложностью.

В некотором роде данный вопрос созвучен безошибочным квантовым вычислениям с неидеальными квантовыми вентилями, хотя физически ситуации различаются. Для устранения ошибок при квантовых вычислениях требуется квантовая коррекция ошибок, которая реализуется при помощи дополнительных квантовых вентилей, и они тоже имеют свои ошибки, которые также надо исправлять при помощи новых квантовых вентилей. Если число дополнительных квантовых вентилей растет полиномиально при некотором уровне исходных ошибок, то возможно проведение безошибочных квантовых вычислений с полиномиальными затратами по числу вентилей.

На сегодняшний день скорость генерации и распределения ключей в квантовой криптографии еще недостаточна для шифрования в режиме одноразового блокнота больших потоков сообщений, хотя это ограничение является чисто технологическим. По-

[1)] Вообще говоря, ключи, полученные с любого генератора случайных чисел, включая квантовый, не являются идеально случайными.

этому один и тот же ключ может неоднократно использоваться в классических алгоритмах шифрования. Даже если использовать ключи, полученные в системе квантовой криптографии в режиме шифрования с одноразовым блокнотом для коротких сообщений, то все равно остается вопрос, в каких терминах нужно учитывать отклонение ключей от идеально случайных и полностью некоррелированных со слепком ключей у подслушивателя.

2. КРИТЕРИЙ СЕКРЕТНОСТИ КЛЮЧЕЙ В КВАНТОВОЙ КРИПТОГРАФИИ

Критерий секретности ключей в квантовой криптографии формулируется в довольно абстрактных терминах, которые заметно отличаются от критериев, принятых в классической криптографии. В результате всех стадий квантового распределения ключей (передачи, измерения квантовых состояний, коррекции ошибок в первичных ключах, сжатия очищенных ключей до финальных секретных ключей при помощи универсальных хэш-функций второго порядка) легитимные пользователи имеют общий секретный ключ x, а подслушиватель в самом общем случае имеет квантовую систему, коррелированную с данным ключом. Данная ситуация описывается матрицей плотности (см. подробности в [12])

$$\rho_{XE} = \sum_{x\in X} P_X(x)|x\rangle\langle x| \otimes \rho_E^x,$$

где состояние классического регистра с ключом x: $|x\rangle = |x_1\rangle \otimes |x_1\rangle \otimes \ldots |x_k\rangle$, $|X| = 2^k$, $x \in X = \{0,1\}^k$, и ρ_E^x — частичная матрица плотности квантовой системы подслушивателя, коррелированная с данным ключом x. Классическая информация, полученная подслушивателем, также может быть включена в ρ_E^x.

Критерий секретности в квантовой криптографии в терминах близости реальной ситуации после квантового распределения ключей, которая описывается совместной матрицей плотности после распределения ключей для легитимных пользователей и подслушивателя — ρ_{XE}, к идеальной ситуации, когда корреляции между квантовой системой подслушивателя и ключом легитимных пользователей полностью отсутствуют, и ключ легитимных пользователей идеально случайный. Такая идеальная ситуация описывается некоррелированными матрицами плотности $\rho_U \otimes \rho_E$. Расстояние между этими двумя ситуациями описывается следовым расстоянием

$$||\rho_{XE} - \rho_U \otimes \rho_E||_1 < \varepsilon, \qquad (1)$$

где следовая метрика по определению

$$||\rho||_1 = \frac{1}{2}\mathrm{Tr}\{|\rho|\} = \frac{1}{2}\mathrm{Tr}\{\sqrt{\rho^2}\},$$

$$\rho_{XE} = \sum_{x\in X} P_X(x)|x\rangle\langle x| \otimes \rho_E^x,$$

$$|x\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \ldots \otimes |x_n\rangle,$$

$$\rho_U = \frac{1}{N}\sum_{x\in X} |x\rangle\langle x|,$$

$$\rho_E = \mathrm{Tr}_X\{\rho_{XE}\} = \sum_x^N P_x(x)\rho_E^x,$$

$$\rho_X = \mathrm{Tr}_E\{\rho_{XE}\} = \sum_x^N P_x(x)|x\rangle\langle x|,$$

ρ_U — матрица плотности для однородного идеального распределения ключей.

Подслушиватель (Ева) не имеет прямого доступа к ключу x, а имеет доступ лишь к побочной информации о ключе — битовой строке $y \in Y = \{0,1\}^n$, которая коррелирована с истинным ключом x легитимных пользователей Алисы и Боба. Битовая строка y получается в результате измерений Евы над своей квантовой системой ρ_E, которая дается частичным следом от совместной матрицы плотности Алиса–Боб и Ева, описывающей корреляции ключа Алисы–Боба с квантовой системой Евы. Измерения Евы описываются разложением единицы $I_E = \sum_{y\in Y} \mathcal{M}_y$, $y \in Y = \{0,1\}^n$, где $\mathcal{M}_y$ — положительная операторно-значная мера в пространстве состояний Евы.

Ниже используем следующие обозначения для условных вероятностей: $P_{XY}(x,y)$ — совместное распределение вероятностей случайных величин x, y; $P_X(x)$ и $P_Y(y)$ — маргинальные распределения вероятностей. Условные распределения вероятностей: $P_{X|Y}(X = x|y)$ — вероятность появления y, если событие x имело место; $P_{X|Y}(x|Y = y)$ — вероятность появления x, если событие y имело место. Соответственно, формулы Байеса и правила суммирования вероятностей имеют вид

$$P_{XY}(x,y) = P_X(x)P_{X|Y}(X = x|y),$$

$$P_{XY}(x,y) = P_{X|Y}(x|Y = y)P_Y(y),$$

$$\sum_{x\in X} P_{X|Y}(x|Y = y) = \sum_{y\in Y} P_{X|Y}(X = x|y) = 1,$$

$$\sum_{x\in X} P_{XY}(x,y) = P_Y(y), \quad \sum_{y\in Y} P_{XY}(x,y) = P_X(x).$$

Условная вероятность того, что ключ Алисы–Боба есть x, а результат измерения Евы (слепок ключа x) будет y, равна

$$P_{X|Y}(X=x|y)=\mathrm{Tr}\{\mathcal{M}_y\rho_E^x\},$$

где правило суммирования условных вероятностей гласит

$$\sum_{y\in Y}P_{X|Y}(X=x|y)=1.$$

Условная вероятность того, что ключ Евы после измерений совпадает с ключом Алисы–Боба (далее для краткости — вероятность угадывания ключа Евой), есть

$$P_{X|Y}(X=x|x)=\mathrm{Tr}\{\mathcal{M}_x\rho_E^x\},\quad y=x. \tag{2}$$

Одним из фундаментальных результатов квантовой теории информации является то, что квантовая криптография гарантирует на уровне фундаментальных законов природы, что средняя по всем ключам вероятность угадывания не превышает (см. детали в [13])

$$P_{Guess}(X|E)=\max_{\mathcal{M}}\sum_{x\in X}P_X(x)\mathrm{Tr}\{\rho_E^x\mathcal{M}_x\}=$$
$$=\sum_{x\in X}P_X(x)P_{X|Y}(X=x|x)=\sum_{x\in X}P_{XY}(x,x), \tag{3}$$

где $P_{XY}(x,y)$ — совместное распределение вероятностей ключей Алисы–Боба (x) и Евы (y), и не превышает

$$P_{Guess}(X|E)=\sum_{x\in X}P_{XY}(x,x)\le\frac{1}{N}+$$
$$+\ ||\rho_{XE}-\rho_U\otimes\rho_E||_1<\frac{1}{N}+\varepsilon,\quad N=2^n, \tag{4}$$

где ε — параметр секретности, выбираемый легитимными пользователями. Заданное ε достигается сжатием сырого (очищенного) ключа.

3. РАЗЛИЧНЫЕ СИТУАЦИИ

Тот факт, что критерий секретности (1) сильно отличается от критериев, используемых в классической криптографии, вызвал бурные дискуссии в литературе [14], которые, на наш взгляд, пока ничем конструктивным не закончились. В классической криптографии одним из основных критериев практической секретности является критерий сложности перебора ключей. Поэтому для практического использования ключей, полученных в квантовой криптографии, необходимо уметь отвечать на вопрос, как связаны различные критерии криптостойкости. Точнее говоря, как, используя только следовое расстояние и не делая никаких предположений о виде распределения $P_X(x)$ и других предположений, получить другие критерии, например, критерий сложности перебора ключей.

Возможны различные ситуации использования ключей. В зависимости от ситуации возникают различные вопросы, на которые требуется ответить.

1. Сообщение зашифровано на ключе, полученном в результате квантового распределения ключей. Формально это означает, что ключ x выбран из множества $X=\{0,1\}^n$ с вероятностью $P_X(x)$. Вопросы: как неидеальность ключей изменит среднее число шагов перебора до нахождения истинного ключа по сравнению с идеальным случаем? Как число шагов перебора связано со следовым расстоянием?

2. Имеется бесконечный поток сообщений. Каждое сообщение шифруется на ключе x, выбранном с вероятностью $P_X(x)$. Для каждого сообщения подслушиватель делает M опробований ключей (M фиксировано). Вопросы: чему равно среднее число сообщений до первого нахождения истинного ключа — дешифрования сообщения? Как это число зависит от неидеальности ключей и как оно связано со следовым расстоянием до идеальной ситуации?

3. Имеется R сообщений, каждое из которых шифруется на своем ключе, полученном в результате квантового распределения. Подслушиватель для каждого сообщения делает заданное число шагов опробования ключей M. Вопрос: как вероятность того, что ни одно сообщение не будет прочитано (ключ не найден), связана со следовым расстоянием?

4. Имеется одно сообщение, зашифрованное в режиме одноразового блокнота. Вопросы: какова вероятность найти истинный ключ (прочитать сообщение), насколько данная вероятность отличается от вероятности шифрования на идеальных случайных ключах и как данная вероятность связана со следовым расстоянием?

Из законов квантовой механики логически следует лишь то, что следовое расстояние между матрицами плотности после квантового распределения ключей не превосходит ε. Принципиальный для квантовой криптографии вопрос состоит в следующем: достаточно только данной характеристики или нужны какие-то другие критерии и неравенства? На данные вопросы возможно ответить, не делая никаких предположений о детальном виде распределения $P_{XY}(x,y)$, а только используя границу для

следового расстояния между двумя ситуациями — реальной и идеальной (1).

4. СЛОЖНОСТЬ ПОЛНОГО ПЕРЕБОРА КЛЮЧЕЙ. РАБОТА ПО УГАДЫВАНИЮ

Пусть в результате квантового распределения ключей возник ключ x, который используется для шифрования по определенному алгоритму $\mathcal{F}$, который отображает открытый текст m в шифр-текст c:

$$c = \mathcal{F}(x, m).$$

Свяжем теперь следовое расстояние с работой по угадыванию (guess work). Данная величина была введена (по-крайней мере, в открытой печати) Месси [15]. Пусть имеется случайная величина x с распределением $P_X(x)$. Пусть распределение $P_X(x)$ известно. Пусть в соответствии с этим распределением выбран x. Требуется найти среднее число шагов, имея в своем распоряжении оракула, который отвечает на вопрос, угадан x или нет. Упорядочим распределение по мере убывания вероятности появления x,

$$P_X(x_1) \geq P_X(x_2) \geq \ldots \geq P_X(x_N),$$

тогда работа (среднее число шагов) по угадыванию по определению есть

$$G(X) = \sum_{i=1}^{N} i \cdot P_X(x). \tag{5}$$

Интерпретация этой величины прозрачна. На первом шаге ($i = 1$) задается вопрос оракулу: является ли величина $x = x_1$ случайной величиной? Если да, то процесс останавливается, при этом x определяется с вероятностью $P_X(x_1)$, если нет, то процесс продолжается, делается второй шаг $i = 2$ и т. д. до нахождения истинного x. Математическое ожидание числа шагов определяется выражением (5). Максимум числа шагов перебора достигается на равномерном распределении $P_X(x) = 1/N$ [16],

$$G_U(X) = \sum_{i=1}^{N} i \cdot P_U(x) = \frac{N+1}{2}.$$

Если ключ используется в каком-то алгоритме шифрования, то роль оракула может выполнять пара известный открытый текст – шифр-текст. Например, подслушиватель может «подсунуть» известный ему открытый текст m, который будет зашифрован на неизвестном ему ключе, т. е. иметь еще и шифр-текст c. Имея пару (m, c), подслушиватель может перебирать ключи k_i, сравнивая $c_i = \mathcal{F}(k_i, m)$ до совпадения c и известного ему m.

Формально роль оракула может выполнять некоторый критерий читаемости открытого текста, полученного из шифр-текста с использованием правильного или неправильного ключа.

Для $G(X)$ имеет место важная оценка [16]

$$\frac{N+1}{2} - 2N||P_X - P_U||_1 \leq G(X) \leq \\ \leq \frac{N+1}{2} - N||P_X - P_U||_1, \tag{6}$$

где следовое расстояние между классическими распределениями вероятности

$$||P_X - P_U||_1 = \frac{1}{2}\sum_{x \in X} |P_X(x) - P_U(x)|.$$

Данные границы являются плотными. Максимальное число шагов перебора до нахождения истинного ключа достигается на равномерном распределении $P_X(x) = P_U(x) = 1/N$.

5. РАБОТА ПО УГАДЫВАНИЮ ПРИ НАЛИЧИИ ПОБОЧНОЙ ИНФОРМАЦИИ

В квантовой криптографии подслушиватель не имеет непосредственного доступа к переменной x (распределению $P_X(x)$), а имеет доступ к побочной информации — переменной y, коррелированной с x. Данные корреляции описываются совместным распределением $P_{XY}(x, y)$ (см. ниже).

Уточним для дальнейшего используемые обозначения. Будем обозначать $P_{X|Y}(x_i|Y = y)$ условную вероятность получить x_i при имеющемся $Y = y$. Грубо говоря, это вероятность происхождения x_i из y, по формальным причинам удобнее именно в таком порядке, а не наоборот — происхождение y из x_i. Упорядочим условные вероятности:

$$P_{X|Y}(x_1|Y = y) \geq P_{X|Y}(x_2|Y = y) \geq \ldots \\ \ldots \geq P_{X|Y}(x_N|Y = y).$$

Правило суммирования условных вероятностей записывается в виде

$$\sum_{i=1}^{N} P_{X|Y}(x_i|Y = y) = 1,$$

оно имеет простую интерпретацию. Заданное y может переходить в разные x_i, сумма вероятностей

всех переходов равна единице — y неизбежно куда-то перейдет.

Пусть подслушиватель получил результат измерения y. При фиксированном y среднее число шагов полного перебора есть $G(X|Y=y)$. Аналогично предыдущему случаю Ева при заданном y перебирает все ключи x:

$$G(X|Y=y)=\sum_{i=1}^{N} i\cdot P_{X|Y}(x_i|Y=y). \qquad (7)$$

Для дальнейшего удобно ввести обозначения

$$P_j=P_{X|Y}(x_j|Y=y),\quad Q_i=\sum_{j=1}^{i}\left(P_j-\frac{1}{N}\right), \qquad (8)$$

$$\left\|P-\frac{1}{N}\right\|=\max_i Q_i. \qquad (9)$$

Последнее равенство является определением вариационного расстояния между двумя распределениями вероятностей, которое равно $\max_i Q_i$ и достигается при суммировании по тем индексам j в предыдущей формуле, при которых $P_j>1/N$. Кроме того, вариационное и следовое расстояния между распределениями вероятностей связаны между собой (см. подробности в [17]):

$$\left\|P-\frac{1}{N}\right\|=\left\|P-\frac{1}{N}\right\|_1, \qquad (10)$$

это следует из равенства

$$|P_X(x)-F_X(x)|=P_X(x)+F_X(x)-\\ -2\min(P_X(x),F_X(x)),$$

$$||P_X-F_X||_1=1-\sum_x \min(P_X(x),F_X(x)).$$

Дальнейшая цепочка равенств является тождественными преобразованиями, с учетом (7)–(10) имеем

$$N+1-G(X|Y=y)=\sum_{i=1}^{N}\sum_{j=1}^{i}P_{X|Y}(x_j|Y=y),$$

$$P_1+(P_1+P_2)+\ldots+(P_1+P_2+\ldots+P_N)=\\ =\sum_{i=1}^{N}(N-i+1)P_i,$$

$$G(X|Y=y)+\sum_{i=1}^{N}(N-i+1)P_i=N+1,$$

$$\sum_{i=1}^{N}Q_i=\sum_{i=1}^{N}\sum_{j=1}^{i}P_j-\frac{N+1}{2},$$

$$G(X|Y=y)=\frac{N+1}{2}-\sum_{i=1}^{N}Q_i(X|Y=y),\\ Q_i(X|Y=y)=\sum_{j=1}^{i}\left(P_{X|Y}(x_j|Y=y)-P_U(x_j)\right), \qquad (11)$$

где $P_U(x_j)=1/N,\quad \forall j$.

Величина y является функцией с распределением $P_Y(y)$. Среднее число шагов перебора по всем исходам измерений Евы (y) дается математическим ожиданием величины $G(X|Y=y)$. Иначе говоря, $G(X|Y=y)$ сама является случайной величиной, как функция y с распределением $P_Y(y)$.

Далее, по определению вариационного расстояния (variational distance, см., например, [17])

$$||P_{X|Y=y}-P_U||=Q_{max}(X|Y=y)=\\ =\max_i Q_i(X|Y=y)=\\ =\sum_{j=1,P_{X|Y}(x_j|Y=y)>P_U(x_j)}^{i}\left(P_{X|Y}(x_j|Y=y)-\right.\\ \left.-P_U(x_j)\right). \qquad (12)$$

При фиксированном y условное распределение является обычным распределением вероятности относительно x, поэтому вариационное расстояние, как и выше для маргинальных распределений, связано со следовым расстоянием [17],

$$||P_{X|Y=y}-P_U||=||P_{X|Y=y}-P_U||_1=\\ =\frac{1}{2}\sum_{j=1}^{N}|P_{X|Y}(x_j|Y=y)-P_U(x_j)|. \qquad (13)$$

6. НИЖНЯЯ ГРАНИЦА РАБОТЫ ПО УГАДЫВАНИЮ

Потребуются свойства следового расстояния между матрицами плотности. Следовое расстояние не возрастает при взятии частичного следа (в более общем виде не возрастает после применения квантовой операции [18]), имеем

$$||P_X-P_U||_1=||\rho_X-\rho_U||_1\le\\ \le||\rho_{XE}-\rho_U\otimes\rho_E||_1\le\varepsilon, \qquad (14)$$

$$\rho_X=\mathrm{Tr}_E\{\rho_{XE}\}=\sum_{x\in X}P_X(x)|x\rangle\langle x|,$$

$$\rho_U = \mathrm{Tr}_E\{\rho_U \otimes \rho_E\} = \sum_{x\in X} P_U(x)|x\rangle\langle x|,\ P_U(x) = \frac{1}{|N|}.$$

Возвращаясь к формуле (11), с учетом (12), (13) получаем, что число шагов перебора до определения истинного ключа не меньше, чем

$$G(X|Y=y) \geq \frac{N+1}{2} - \sum_{i=1}^{N} \max_i\ Q_i(X|Y=y) = \\ = \frac{N+1}{2} - 2\sum_{i=1}^{N} ||P_{X|Y=y} - P_U||_1 = \\ = \frac{N+1}{2} - N\sum_{x_i}\left|P_{X|Y}(x_i|Y=y) - \frac{1}{N}\right|,$$

где учтено, что $P_U(x_i) = 1/N$.

Теперь можно усреднить по y, находим

$$G(X|Y) = \sum_{y\in Y} P_Y(y)G(X|Y=y) \geq \frac{N+1}{2} - \\ - N\sum_{y}^{N}\sum_{x}^{N} P_Y(y)\left|P_{X|Y}(x|Y=y) - \frac{1}{N}\right| = \\ = \frac{N+1}{2} - N\sum_{y}^{N}\sum_{x}^{N}\left|P_{XY}(x,y) - \frac{P_Y(y)}{N}\right|. \quad (15)$$

7. СВЯЗЬ РАБОТЫ ПО УГАДЫВАНИЮ С КВАНТОВО-МЕХАНИЧЕСКИМИ НЕРАВЕНСТВАМИ

Для получения границ для работы по угадыванию при наличии побочной информации (y) требуется связать следовое расстояние между классическими распределениями вероятностей со следовой нормой между матрицами плотности. Удивительным свойством следового расстояния является то, что следовые расстояния для распределений $P_X(x)$ и $P_Y(y)$ связаны и оба ограничены величиной $||\rho_{XE} - \rho_U \otimes \rho_E||_1 < \varepsilon$. Связь между классическими распределениями вероятностей и матрицами плотности возникает в результате измерений. В зависимости от ситуации измерения могут конструироваться различными способами.

Для сокращения примем следующие обозначения:

$$D(\rho_{XE}, \rho_U\otimes\rho_E) = \frac{1}{2}\mathrm{Tr}\{|\rho_{XE} - \rho_U\otimes\rho_E|\} = \\ = ||\rho_{XE} - \rho_U\otimes\rho_E||_1. \quad (16)$$

Имеют место следующие неравенства (см. детали в [13]). Для любого оператора $\mathcal{M}$, $0 \leq \mathcal{M} \leq I$,

$$\mathrm{Tr}\{\mathcal{M}|\rho_{XE} - \rho_U\otimes\rho_E|\} \geq \\ \geq |\mathrm{Tr}\{\mathcal{M}(\rho_{XE} - \rho_U\otimes\rho_E)\}|, \quad (17)$$

$$D(\rho_{XE}, \rho_U\otimes\rho_E) = \\ = \max_{\mathcal{M}} \mathrm{Tr}\{\mathcal{M}(\rho_{XE} - \rho_U\otimes\rho_E)\}. \quad (18)$$

Рассмотрим измерения, которые позволяют получить оценки для средней по всем ключам вероятности угадывания (2)–(4) при наличии побочной информации. Битовая строка y получается в результате измерений, выберем измерение в виде следующего разложения единицы:

$$I = \sum_{x'\in X} \mathcal{F}_{x'}, \quad \mathcal{F}_{x'} = |x'\rangle\langle x'|\otimes\mathcal{M}_{x'}. \quad (19)$$

Принимая во внимание (16)–(19), находим максимум по всевозможным измерениям:

$$\frac{1}{2}\sum_{x\in X}|\mathrm{Tr}\{\mathcal{F}_x(\rho_{XE} - \rho_U\otimes\rho_E)\}| \leq \\ \leq \frac{1}{2}\sum_{x\in X}\mathrm{Tr}\{\mathcal{F}_x|\rho_{XE} - \rho_U\otimes\rho_E|\} = \\ = \frac{1}{2}\mathrm{Tr}\{|\rho_{XE} - \rho_U\otimes\rho_E|\} = D(\rho_{XE} - \rho_U\otimes\rho_E). \quad (20)$$

Левая часть связана с классическими распределениями вероятностей, с учетом (19) получаем

$$\frac{1}{2}\sum_{x\in X}|\mathrm{Tr}\{\mathcal{F}_x(\rho_{XE} - \rho_U\otimes\rho_E)\}| = \\ = \frac{1}{2}\sum_{x\in X}\left|\left(P_X(x)\mathrm{Tr}\{\mathcal{M}_x\rho_E^x\} - \frac{1}{N}P_Y(x)\right)\right| = \\ = \frac{1}{2}\sum_{x\in X}\left|P_X(x)P_{X|Y}(X=x|x) - \frac{P_Y(x)}{N}\right| = \\ = \frac{1}{2}\sum_{x\in X}\left|P_{XY}(x,x) - \frac{P_Y(x)}{N}\right|, \quad (21)$$

где использовано

$$P_Y(x) = \mathrm{Tr}\{\rho_E\mathcal{M}_x\}, \\ P_{X|Y}(X=x|x) = \mathrm{Tr}\{\rho_E^x\mathcal{M}_x\}, \quad (22)$$

$$P_{XY}(x,x) = P_X(x)P_{X|Y}(X=x|x). \quad (23)$$

С учетом (16), (21)–(23) получаем

$$\frac{1}{2}\sum_{x\in X}\left|P_{XY}(x,x) - \frac{P_Y(x)}{N}\right| \leq \\ \leq ||\rho_{XE} - \rho_U\otimes\rho_E||_1 < \varepsilon, \quad (24)$$

далее, используя (14), находим

$$\frac{1}{2}\sum_{x\in X}\left|P_X(x)-\frac{1}{N}\right|\le||\rho_{XE}-\rho_U\otimes\rho_E||_1<\varepsilon. \quad (25)$$

Измерение, которое рассматривалось выше (14), дает только диагональные члены для совместного распределения вероятностей $(P_{XY}(x,x))$, что недостаточно для нахождения нижней границы работы по угадыванию (15), поэтому приходится использовать другое измерение. Перейдем к его рассмотрению. Для окончательного получения нижней границы работы по угадыванию (15) требуется оценка для величины

$$\sum_y^N\sum_x^N\left|P_{XY}(x,y)-\frac{P_Y(y)}{N}\right|.$$

Имеют место следующие неравенства, основанные на неравенстве треугольника для следовой нормы:

$$\begin{aligned}\sum_y^N\sum_x^N\left|P_{XY}(x,y)-\frac{P_Y(y)}{N}\right|&=\sum_y^N\sum_x^N\left|P_{XY}(x,y)-\right.\\&\left.-P_X(x)P_Y(y)+P_X(x)P_Y(y)-\frac{P_Y(y)}{N}\right|\le\\&\le\sum_y^N\sum_x^N\left(|P_{XY}(x,y)-P_X(x)P_Y(y)|+\right.\\&\left.+\left|P_X(x)P_Y(y)-\frac{P_Y(y)}{N}\right|\right)=\\&=\sum_y^N\sum_x^N|P_{XY}(x,y)-P_X(x)P_Y(y)|+\\&+\sum_x^N\left|P_X(x)-\frac{1}{N}\right|. \quad (26)\end{aligned}$$

Далее рассмотрим измерение, описываемое разложением единицы,

$$I=\sum_{z=(x,y)}^{N\times N}|x'\rangle\langle x'|\otimes\mathcal{M}_y,\qquad\sum_{z=(x,y)}^{N^2}=\sum_y^N\sum_x^N. \quad (27)$$

Отметим, что данное измерение отвечает независимым измерениям легитимных пользователей и подслушивателя. Например, в качестве $\mathcal{M}_y$ можно взять проектор на битовую строку y — $|y\rangle_{EE}\langle y|$. Корреляция исходов измерений возникает из-за того, что квантовое состояние ρ_{XE} является запутанным. Напомним аналогию с измерениями над полностью запутанным состоянием двух кубитов (ЭПР-парой). Измерения независимы и локальны, а результаты измерений будут полностью коррелированы.

Используя (16)–(18), (26), (27), получаем требуемые неравенства, которые связывают классические распределения вероятностей в (15) со следовым расстоянием между матрицами плотности:

$$\begin{aligned}\frac{1}{2}\sum_y^N\sum_x^N|\mathrm{Tr}\left((|x'\rangle\langle x'|\otimes\mathcal{M}_y)(\rho_{XE}-\rho_X\otimes\rho_E)\right)|=\\=\frac{1}{2}\sum_y^N\sum_x^N|\mathrm{Tr}\left((P_X(x)|x\rangle\langle x|)\otimes(\rho_E^x\mathcal{M}_y)-\right.\\\left.-(P_X(x)|x\rangle\langle x|)\otimes(\rho_E\mathcal{M}_y)\right)|=\\=\frac{1}{2}\sum_y^N\sum_x^N|P_X(x)P_{X|Y}(X=x|y)-P_X(x)P_Y(y)|=\\=\frac{1}{2}\sum_y^N\sum_x^N|P_{XY}(x,y)-P_X(x)P_Y(y)|\le\\\le\frac{1}{2}\mathrm{Tr}(|\rho_{XE}-\rho_X\otimes\rho_E|)=||\rho_{XE}-\rho_X\otimes\rho_E||_1=\\=||\rho_{XE}-\rho_U\otimes\rho_E+\rho_U\otimes\rho_E-\rho_X\otimes\rho_E||_1\le\\\le||\rho_{XE}-\rho_U\otimes\rho_E||_1+||\rho_U\otimes\rho_E-\rho_X\otimes\rho_E||_1\le\\\le||\rho_{XE}-\rho_U\otimes\rho_E||_1+||\rho_X-\rho_U||_1<2\varepsilon, \quad (28)\end{aligned}$$

где учтено, что

$$P_{X|Y}(X=x|y)=\mathrm{Tr}(\rho_E^x\mathcal{M}_y),$$

$$P_X(x)=\mathrm{Tr}(P_X(x)|x\rangle\langle x|),$$

$$P_Y(y)=\mathrm{Tr}(\rho_E\mathcal{M}_y)=\mathrm{Tr}\left(\sum_{x'}^N P_X(x')\rho_E^{x'}\mathcal{M}_y\right)=$$

$$=\sum_{x'}^N P_X(x')P_{X|Y}(X=x'|y).$$

Наконец, собирая все неравенства (28), ограничиваем следовое расстояние между классическими распределениями следовой нормой из квантовой криптографии:

$$\frac{1}{2}\sum_y^N\sum_x^N\left|P_{XY}(x,y)-\frac{P_Y(y)}{N}\right|\le$$

$$\le||\rho_{XE}-\rho_U\otimes\rho_E||_1<\varepsilon. \quad (29)$$

Для нижней границы работы по перебору (15) с учетом (29) получаем

$$G(X|Y)>\frac{N+1}{2}-2N||\rho_{XE}-\rho_U\otimes\rho_E||_1>$$

$$>\frac{N(1-4\varepsilon)}{2}+\frac{1}{2}. \quad (30)$$

Как видно из (30), среднее число шагов перебора ключей до определения истинного ключа не менее, чем (30). При этом данная граница явно выражается через следовое расстояние между реальной и идеальной ситуациями и связывает абстрактный критерий секретности, используемый в квантовой криптографии, со сложностными критериями в классической криптографии.

8. ВЕРХНЯЯ ГРАНИЦА РАБОТЫ ПО УГАДЫВАНИЮ

В этом разделе получим верхнюю границу для работы по угадыванию, которая дает среднее число шагов и не более, за которое гарантированно будет найден истинный ключ. Верхняя граница возникает из следующей цепочки неравенств. Неравенство параллелограмма, которое следует из выпуклости величины Q_i (см. детали в [16])

$$\sum_{i=k}^{m} Q_i(X|Y=y) \geq$$
$$\geq \frac{Q_k(X|Y=y)+Q_m(X|Y=y)}{2}(m-k+1). \quad (31)$$

Далее

$$Q_i(X|Y=y) = P_{X|Y}(x_i|Y=y) - \frac{1}{N}, \qquad Q_N(X|Y=y) = 0, \quad (32)$$

пусть индекс l имеет такое значение, при котором

$$Q_l(X|Y=y) = \max Q_i(X|Y=y) = \left\| P_{X|Y=y} - \frac{1}{N} \right\|, \quad (33)$$

$$Q_{l-1}(X|Y=y) = Q_l(X|Y=y) - P_{X|Y}(x_l|Y=y) + \frac{1}{N}. \quad (34)$$

С учетом (11), (31)–(34) получаем

$$\frac{N+1}{2} - G(X|Y) = \sum_{i=1}^{l-1} Q_i(X|Y=y) + \sum_{i=l}^{N} Q_i(X|Y=y) \geq$$
$$\geq \frac{Q_1(X|Y=y) - Q_{l-1}(X|Y=y)}{2}(l-1) + \frac{Q_l(X|Y=y)+Q_N(X|Y=y)}{2}(N-l+1) =$$
$$= \frac{Q_l(X|Y=y)+(P_{X|Y}(x_i|Y=y)-P_{X|Y}(x_l|Y=y)}{2} \times (l-1) + \frac{Q_l(X|Y=y)}{2}(N-l+1) \geq$$
$$\geq \frac{Q_l(X|Y=y)(l-1)}{2} + \frac{Q_l(X|Y=y)(N-l+1)}{2} = \frac{NQ_N(X|Y=y)}{2} = N\left\| P_{X|Y=y} - \frac{1}{N} \right\|_1 =$$
$$= \frac{N}{2}\sum_{i=1}^{N}\left| P_{X|Y}(x_i|Y=y) - \frac{1}{N} \right|. \quad (35)$$

Далее, усредняя по всем исходам y, находим

$$G(X|Y) = \sum_{y\in Y} G(X|Y=y)P_Y(y),$$

используя неравенства (35), получаем

$$G(X|Y) \leq \frac{N+1}{2} - \frac{N}{2} \times \sum_{y}^{N}\sum_{x}^{N} P_Y(y)\left| P_{X|Y}(x|Y=y) - \frac{1}{N} \right| =$$
$$= \frac{N+1}{2} - \frac{N}{2}\sum_{y}^{N}\sum_{x}^{N}\left| P_{XY}(x,y) - \frac{P_Y(y)}{N} \right|,$$

с учетом (28) имеем

$$\sum_{y}^{N}\sum_{x}^{N}\left| P_{XY}(x,y) - \frac{P_Y(y)}{N} \right| = \mathrm{Tr}\{\mathcal{M}(\rho_{XE} - \rho_U \otimes \rho_E)\},$$

а максимум (см. (18)) равен

$$\max_{\mathcal{M}} \mathrm{Tr}\{\mathcal{M}(\rho_{XE} - \rho_U \otimes \rho_E)\} = ||\rho_{XE} - \rho_U \otimes \rho_E||_1.$$

Наконец, получаем

$$\frac{N+1}{2} - 2N||\rho_{XE} - \rho_U \otimes \rho_E||_1 \leq G(X|Y) \leq \frac{N+1}{2} - N||\rho_{XE} - \rho_U \otimes \rho_E||_1. \quad (36)$$

Данные границы являются плотными (tight bounds). Формула (36) устанавливает фундаментальную связь между абстрактным критерием секретности в квантовой криптографии (расстоянием между реальной и идеальной ситуациями — $||\rho_{XE} - \rho_U \otimes \rho_E||_1 < \varepsilon$) и трудоемкостью по перебору ключей в классических системах шифрования.

Удобно переписать нижнюю границу, определяющую минимально необходимое число шагов опробования ключа до его определения, с учетом (28) в виде

$$G(X|Y) \geq \frac{N+1}{2} - 2N\left(||\rho_{XE} - \rho_X \otimes \rho_E||_1 + ||\rho_X - \rho_U||_1\right). \quad (37)$$

Отсюда видно, что когда корреляции между системой Евы ρ_E и ключом легитимных пользователей (ρ_X, $P_X(x)$) полностью отсутствуют — $\rho_{XE} = \rho_X \otimes \otimes \rho_E$ ($||\rho_{XE} - \rho_X \otimes \rho_E||_1 = 0$), тогда минимальное число шагов перебора до установления ключа определяется отклонением функции распределения самих ключей $P_X(x)$ от идеального — равномерного распределения ключей $P_U = (||\rho_X - \rho_U||_1)/N$:

$$G(X|Y) \geq \frac{N+1}{2} - 2N||\rho_X - \rho_U||_1 > \\ > \frac{N+1}{2} - 2N\varepsilon, \quad (38)$$

при этом

$$||\rho_X - \rho_U||_1 = \left\| P_X - \frac{1}{N} \right\|_1 < \varepsilon.$$

Таким образом, из (37) видно, что следовое расстояние между матрицами плотности учитывает как корреляции между ключами и системой подслушивателя, так и неравномерность распределения самих ключей.

9. ПРИМЕР. СЛЕДОВОЕ РАССТОЯНИЕ МЕЖДУ ПОЛНОСТЬЮ КОРРЕЛИРОВАННЫМИ РАСПРЕДЕЛЕНИЯМИ

На первый взгляд, границы (36) не зависят от y и определяются только ε, поэтому для полностью коррелированного распределения $P_{XY}(x,y) = = \delta_{x,y}/N$ и, соответственно, $P_{X|Y}(x|Y = y) = = P_{Y|X}(X = x|y) = 1$, $P_X(x) = P_Y(y) = 1/N$, возможен внешний конфуз. При таком полностью коррелированном распределении побочная переменная y однозначно определяет исходный ключ x. В этом случае нахождение ключа достигается за один шаг. Однако надо иметь ввиду, что за данной ситуацией «следит» ε. В этом случае расстояние ε между реальной ситуацией (полные корреляции между x и y) $P_{XY}(x,y) = \delta_{x,y}/N$ и реальной ситуацией (полное отсутствие корреляций) $P_{XY}(x,y) = P_X(x)P_Y(y) = = P_Y(y)/N$ оказывается порядка единицы, что отвечает максимальному расстоянию между данными видами распределений (ситуациями). Действительно,

$$\rho_{XE} = \frac{1}{N} \sum_{x \in X} |x\rangle\langle x| \otimes |x\rangle_{EE}\langle x|,$$

$$\rho_E = \frac{1}{N} \sum_{x \in X} |x\rangle_{EE}\langle x|, \quad \rho_U = \frac{1}{N} \sum_{x \in X} |x\rangle\langle x|,$$

$$||\rho_{XE} - \rho_U \otimes \rho_E||_1 = \frac{1}{2} \times \\ \times \mathrm{Tr}\left\{ \sqrt{(\rho_{XE} - \rho_U \otimes \rho_E)^2} \right\} = \frac{1}{2} \times \\ \times \mathrm{Tr}\left\{ \sum_{x \in X} \left(\frac{1}{N} - \frac{1}{N^2} \right) |x\rangle\langle x| \otimes |x\rangle_{EE}\langle x| + \right. \\ \left. + \frac{1}{N^2} \times \right. \quad (39) \\ \left. \times \sum_{x_1 \in X} \sum_{x_2 \in X, x_1 \neq x_2} |x_1\rangle\langle x_1| \otimes |x_2\rangle_{EE}\langle x_2| \right\} = \\ = \frac{1}{2} \left(1 - \frac{1}{N} + \frac{(N-1)^2}{N^2} \right) \approx 1 - o\left(\frac{1}{N} \right),$$

т. е. следовое расстояние оказывается порядка единицы, $\varepsilon \approx 1$. При этом число шагов перебора, с учетом (39), тривиально:

$$G(X|Y) \leq 0.$$

Это означает, что максимальное число шагов перебора до определения ключа тривиально. Надо понимать, что выполняются неравенства, точное значение верхней и нижней границы в этом случае есть единица, т.е. ключ при переборе при полностью коррелированном распределении для x и y определяется за один шаг. В этом смысле граница становится тривиальной.

10. СРЕДНЕЕ ЧИСЛО СООБЩЕНИЙ ДО ОПРЕДЕЛЕНИЯ КЛЮЧА

Приведем оценки без учета побочной информации, поскольку учет последней в данном контексте имеет некоторую специфику. Вывод результатов с учетом побочной информации требует отдельного рассмотрения.

Пусть имеется, вообще говоря, бесконечный поток сообщений, каждое шифруется своим ключом, который легитимные пользователи получают в результате квантового распределения ключей — ключ подчиняется распределению $P_X(x)$. Число опробований ключей на каждом сообщении фиксировано и равно M.

При консервативном подходе в пользу подслушивателя будем считать, что Еве известно само распределение $P_X(x)$, но Ева не знает ключ, выбранный для шифрования конкретного сообщения. При этих предположениях в ее пользу Ева может упорядочить распределение $P_X(x_1) \geq P_X(x_2) \geq \geq \ldots \geq P_X(x_M) \geq \ldots \geq P_X(x_N)$. На каждом шаге вероятность того, что выбранный легитимными

пользователями ключ попадает в переборное множество $\{M\}$, есть

$$P_X(M) = \sum_{i=1}^{M} P_X(x_i).$$

Если ключ попадает в это множество, то сообщение будет дешифровано, так как Ева опробует все ключи из этого множества. Но эта ситуация реализуется с вероятностью $P_X(M)$. Вероятность появления такой ситуации на каждом k-м шаге равна

$$P(k, M) = (1-P_X(M))^{k-1} P_X(M), \quad k = 1, 2, \ldots, \infty.$$

Математическое ожидание числа шагов $\mathrm{Steps}(M)$ до первого появления сообщения, зашифрованного на ключе из множества $\{M\}$, есть

$$\mathrm{Steps}(M) = \sum_{k=1}^{\infty} kP(k, M) = \frac{1 - P_X(M)}{P_X(M)}.$$

Дальнейшая наша цель — связать $\mathrm{Steps}(M)$ $(P_X(M))$ со следовым расстоянием, возникающим после квантового распределения ключей. Далее, воспользовавшись тем, что

$$||P_X - P_U||_1 = ||\rho_X - \rho_U||_1 < \varepsilon,$$

и учитывая соотношение

$$||P_X - P_U|| = \left| \sum_x \max_x (P_X - P_U) \right| = ||P_X - P_U||_1,$$

оцениваем

$$\left| \sum_{i=1}^{N} \max_x \left(P_X(x_i) - \frac{1}{N} \right) \right| \le \sum_{i=1}^{N} \left| P_X(x_i) - \frac{1}{M} \right| + \sum_{i=M+1}^{N} |P_X(x_i) - \frac{1}{N}| \le \sum_{i=1}^{M} P_X(x_i) - \frac{M}{N} + \sum_{i=M+1}^{N} \left| P_X(x_i) - \frac{1}{N} \right| \le \varepsilon$$

и получаем

$$P_X(M) < \frac{M}{N} + \varepsilon.$$

Отсюда находим среднее число сообщений до первого нахождения ключа (дешифрования), когда на каждом шаге опробуются M первых наиболее вероятных ключей

$$\mathrm{Steps}(M) = \frac{1}{P_X(M)} - 1 > \frac{N}{M + N\varepsilon}, \qquad (40)$$

которое выражается через величину следового расстояния реальной ситуации до идеальной, ε.

Обсудим масштабы величин в (40). Длина ключа для блочного шифра ГОСТ 28147-89 Р составляет $n = 256$ бит, для нового стандарта шифрования («Кузнечик») ГОСТ Р 34.12-2015 длина ключа также равна 256 бит. Поэтому размер полного ключевого пространства $N = 2^{256} \approx 1.5 \cdot 10^{77}$ (напомним, что число атомов в видимой части Вселенной оценивается как 10^{77}). Число шагов перебора даже при $M = 2^{128} \approx 10^{38}$ является запредельным. Величина ε, которую можно реально достичь в системах квантовой криптографии, на сегодня имеет порядок (см. ниже) $\varepsilon = 2^{-32} \approx 2.5 \cdot 10^{-10}$. Поэтому $N\varepsilon \gg M$, в этом случае среднее число шагов до первого определения ключа — до первого сообщения, которое возможно будет дешифровано, есть

$$\mathrm{Steps}(M) \approx \frac{1}{\varepsilon} \approx 10^{10},$$

т. е., грубо говоря, из 10 миллиардов сообщений в среднем будет прочитано одно сообщение. При опробовании $M \to N$ ключей (перебираются почти все ключи для каждого сообщения) среднее число сообщений до первого прочитанного $\mathrm{Steps}(M) \approx 1$. При таких соотношениях параметров величина $\mathrm{Steps}(M)$ фактически не зависит от M, поэтому, если опробуется только первый наиболее вероятный ключ, то число шагов до первого прочитанного сообщения не меняется: $\mathrm{Steps}(M) \approx 1/\varepsilon \approx 10^{10}$.

11. ВЕРОЯТНОСТЬ НАХОЖДЕНИЯ КЛЮЧА ИЗ R СООБЩЕНИЙ

Имеется R сообщений, зашифрованных каждое на своем ключе. Подслушиватель производит M опробований ключей на каждом шаге. Найдем вероятность того, что будет прочитано хотя бы одно сообщение (соответственно не прочитано ни одного сообщения). Сообщение дешифруется, если ключ попадает в множество $\{M\}$. Вероятность события равна $P_X(M)$, соответственно, вероятность не попадания есть $1 - P_X(M)$. Для подсчета вероятностей воспользуемся простой формулой:

$$1 - P_X(M) + P_X(M)^R = \sum_{k=0}^{R} \begin{pmatrix} R \\ R-k \end{pmatrix} (1 - P_X(M))^k p_X(M)^{M-k}.$$

Вероятность того, что не будет прочитано ни одно сообщение, есть

$$P(\overline{OK},M,R)=(1-P_X(M))^R\geq$$
$$\geq\left(1-\frac{M+N\varepsilon}{N}\right)^R\approx(1-\varepsilon)^R\approx 1-R\varepsilon.$$

Соответственно, вероятность прочитать одно и более сообщений есть

$$P(OK,M)1=1-P(\overline{OK},M)\leq$$
$$\leq 1-\left(1-\frac{M+N\varepsilon}{N}\right)^R\approx R\varepsilon.$$

Как видно, результат опять выражается через следовое расстояние, фигурирующее в критерии секретности квантового распределения ключей. Опять для полностью коррелированного распределения ($\varepsilon\approx 1$) из R сообщений будут дешифрованы все.

12. ИСПОЛЬЗОВАНИЕ КЛЮЧЕЙ В РЕЖИМЕ ОДНОРАЗОВОГО БЛОКНОТА

При шифровании в режиме одноразового блокнота на идеальных случайных ключах для подслушивателя в отсутствие априорной и побочной информации имеется только одна возможность — угадать ключ или сам открытый текст, в этой ситуации это одно и то же. Данная вероятность равна $1/2^n$ (n — длина ключа, равная длине сообщения). Если шифрование в режиме одноразового блокнота происходит на ключах, полученных в результате квантового распределения ключей, относительно которых гарантируется лишь ε-секретность, то возникает вопрос, как изменится упомянутая вероятность угадывания ключа (сообщения). Фактически требуется найти максимальную вероятность угадывания ключа x при наличии побочной информации y. Теория позволяет вычислить максимальную вероятность угадывания ключа, среднюю по всем исходам y, т. е. усредненную по всем исходам побочной переменной y. Следовое расстояние является интегральной характеристикой — в среднем уклонение вероятности от равномерного распределения не превосходит ε. Работа по угадыванию позволяет получить оценку максимальной вероятности [19]. Пусть ключ x_1 имеет максимальную вероятность появления ($P_X(x_1)\geq P_X(x_2)\geq\ldots$). Согласно [19], имеем

$$P_X(x_1)\leq 1-\frac{2}{N}(G(X)-1). \qquad (41)$$

Данное неравенство справедливо для апостериорной вероятности, когда Ева не имеет доступа к ключу x, а имеет доступ к побочной информации — битовой строке y. В этом случае для условной вероятности — исход Евы есть y, а фактический ключ есть x_1 — имеем

$$P_{X|Y}(x_1|Y=y)\leq 1-\frac{2}{N}(G(X|Y=y)-1). \qquad (42)$$

Сами исходы у Евы возникают с вероятностью $P_Y(y)$. Усредняя по всем побочным исходам y, находим, что вероятность угадывания истинного ключа x_1 не превосходит

$$P_X(x_1)\leq\sum_{y\in Y}P_{X|Y}(x_1|Y=y)P_Y(y)\leq$$
$$\leq 1-\frac{2}{N}\sum_{y\in Y}(G(X|Y=y)-1)P_Y(y)=$$
$$=1-\frac{2}{N}(G(X|Y)-1), \qquad (43)$$

с учетом (36) находим

$$P_{max}=P_X(x_1)\leq\frac{1}{N}+2||\rho_{XE}-\rho_U\otimes\rho_E||_1<$$
$$<\frac{1}{N}+4\varepsilon. \qquad (44)$$

Поскольку условная вероятность $P_{X|Y}(x_1|Y=y)\leq 1$ и $P_Y(y)\leq 1$, при любом значении y величина максимальной вероятности не превышает значения (44). Например, при условии $k=2+\log_2 N$ ($\varepsilon=2^{-k}$) вероятность угадывания ключа (сообщения) только в два раза больше, чем при использовании идеальных ключей. При длинных сообщениях (длиной более 512) данная вероятность имеет масштаб обратного числа атомов в видимой части Вселенной, приблизительно равного 10^{77}.

Максимальная вероятность связана с энтропией Реньи H_∞ порядка ∞: $H_\infty(X)=-\log_2(P_{max})$. Энтропия Реньи бесконечного порядка имеет операциональную интерпретацию — она равна максимальной вероятности угадывания ключа за один шаг $P_{guess}=2^{-H_\infty(X)}$, что видно из рассуждений по вычислению трудоемкости, изложенных выше.

Нужно подчеркнуть важное различие между максимальной вероятностью угадывания и работой по угадыванию. 1) Максимальная вероятность (44) представляет собой вероятность угадывания ключа x за одну попытку. 2) Работа по угадыванию (36) представляет собой среднее число шагов перебора ключей до однозначного нахождения фактического ключа x.

13. ОЦЕНКИ ДЛИНЫ ОЧИЩЕННОГО КЛЮЧА ДЛЯ ДОСТИЖЕНИЯ ЗАДАННОГО ε

Сделаем оценки длины сырой последовательности, которая требуется для шифрования сообщения длиной k бит в режиме одноразового блокнота и при заданном параметре секретности ε. Длина секретного ключа (R_n) в битах выражается через сглаженную условную минимальную энтропию ($H^{\varepsilon}_{min}(\rho^{(n)}_{XEC}|\rho^{(n)}_{EC})$) (см. детали в [12])

$$R_n \geq H^{\varepsilon}_{min}(\rho^{(n)}_{XEC}|\rho^{(n)}_{EC}), \tag{45}$$

$$H^{\varepsilon}_{min}(\rho^{(n)}_{XEC}|\rho^{(n)}_{EC}) \geq H^{\varepsilon}_{min}(\rho^{(n)}_{XE}|\rho^{(n)}_{E}) - \mathrm{leak}_n, \tag{46}$$

где $\rho^{(n)}_{XEC}$ — матрица плотности, описывающая легитимных пользователей, подслушивателя и классическую информацию в битах (leak_n), переданную через открытый канал при коррекции ошибок. Для качественных оценок будем использовать $\rho^{(n)}_{XE} \to \rho^{\otimes n}_{XE}$, $\rho^{(n)}_{E} \to \rho^{\otimes n}_{E}$, поскольку после случайного перемешивания любая матрица плотности, которая исходно не является тензорным произведением, может быть представлена в виде линейной оболочки матриц плотности в виде тензорного произведения, что является следствием квантовой теоремы де Финетти (см. подробности в [12]). Имеем

$$H^{\varepsilon}_{min}(\rho^{\otimes n}_{XE}|\rho^{\otimes n}_{E}) \geq n\left(H(\rho_{XE}) - H(\rho_E) - \delta\right), \quad \delta = 5\sqrt{\frac{\log_2(1/\varepsilon)}{n}}, \tag{47}$$

где $H(\rho) = \mathrm{Tr}\{\rho\log_2(\rho)\}$ — энтропия фон Неймана. Величина δ фактически учитывает статистические флуктуации энтропии фон Неймана при конечных длинах последовательностей. Условная энтропия фон Неймана в (45), (46) есть случайная функция вероятностей значения бита — результата квантово-механических измерений над квантовой системой. В результате измерений над квантовой системой возникает случайное значение классической величины. Флуктуации классической случайной величины — это разброс значений по отношению к среднему, он ведет себя как $1/\sqrt{N}$ (N — число испытаний). Величина $\sqrt{1/n}$ (47) фактически отражает этот факт. Величина $\sqrt{\log_2(1/\varepsilon)}$ связывает флуктуации энтропии фон Неймана со случайной величиной — случайным битом, получаемым в результате измерения. Энтропия фон Неймана выражается через вероятности появления случайной величины.

Неформальный смысл условной энтропии фон Неймана — число битов, которых не хватает подслушивателю, имеющему в распоряжении квантовую систему ρ_E, коррелированную с битовой последовательностью легитимных пользователей x, чтобы полностью знать значение классической последовательности x. Вторжение подслушивателя в квантовый канал связи, из которого подслушиватель получает свою квантовую систему ρ_E, приводит к ошибкам на приемной стороне. Чем больше искажение информационных квантовых состояний, тем больше ошибка на приемной стороне. Поэтому условная энтропия фон Неймана связана с ошибками на приемной стороне и, соответственно, с числом битов (leak_n), расходуемых на коррекцию ошибок. Здесь примем консервативный подход в пользу подслушивателя. Будем считать, что информация подслушивателя ограничена фундаментальной величиной Холево [20] — количеством классической информации, которую можно извлечь из квантового ансамбля информационных состояний. Эта величина зависит от протокола, но никогда не превосходит единицы (в пересчете на одно состояние ансамбля). А величина leak_n есть реальное число битов для коррекции ошибок. Эта величина зависит от способа коррекции ошибок. Минимальное количество битов дается (в асимптотическом пределе) границей Шеннона [21] ($\mathrm{leak}_n \approx nh(Q)$, $h(Q)$ — бинарная энтропийная функция Шеннона).

Длина ключа, которую можно получить из n зарегистрированных отсчетов есть

$$R_n = n\left(H(\rho_{XE}) - H(\rho_E) - \delta\right) - \mathrm{leak}_n,$$

где leak_n — количество битов, расходуемых при коррекции ошибок в сыром ключе. Оцениваем информацию через величину Холево [20]

$$H(\rho_{XE}|\rho_E) = 1 - \chi(\rho_A).$$

Конкретный вид матрицы плотности ансамбля информационных состояний (ρ_A) для вычисления $\chi(\rho_A)$ не потребуется, величина $1-\chi(\rho_A)$ порядка единицы, ρ_A — матрица плотности ансамбля квантовых состояний на передающей стороне. Минимальное количество битов при исправлении ошибок есть $\mathrm{leak}_n \approx nH(Q)$.

Пусть требуется зашифровать сообщение длиной k бит. Пусть при этом выбирается $\varepsilon = 2^{-zk}$, где $z > 1$, тогда требуется n бит сырого ключа:

$$\alpha n - 5\sqrt{\frac{zk}{n}} = k, \quad \alpha = 1-\chi(\rho_A)-\mathrm{leak}, \quad \mathrm{leak} = \frac{\mathrm{leak}_n}{n},$$

где leak — доля битов на одну посылку, расходуемая при коррекции ошибок. Далее, длина последовательности сырого ключа

$$n \approx k\frac{5\sqrt{z}}{\alpha},$$

т. е. длина сырой последовательности возрастает линейно с увеличением длины сообщения, а ε приближается к нулю экспоненциально быстро по длине сообщения. Величина α порядка единицы, пусть $\alpha = 1/2$. При $z = 4$ длина сырого ключа должна быть $n = 20k$, при этом максимальная вероятность угадывания ключа (сообщения) при шифровании в режиме одноразового блокнота при длине сообщения $k = 512$ бит, составляет не более

$$\frac{1}{2^{512}} + \frac{1}{2^{2048}} \approx \frac{1}{2^{512}},$$

что практически совпадает со случаем шифрования в режиме одноразового блокнота на идеальных случайных ключах.

14. ЗАКЛЮЧЕНИЕ

Таким образом, выше простыми средствами показана прямая связь между абстрактными критериями секретности в квантовой криптографии и конструктивными практическими критериями криптостойкости в классических системах шифрования.

Автор выражает благодарность И. М. Арбекову, А. Н. Климову, С. П. Кулику, Д. А. Кронбергу, К. С. Кравцову за многочисленные и интенсивные дискуссии, а также коллегам по Академии криптографии Российской Федерации за постоянную поддержку и обсуждения. Работа выполнена при поддержке Российского научного фонда (грант № 16-12-00015).

ЛИТЕРАТУРА

1. Ю. И. Манин, *Вычислимое и невычислимое*, Советское радио, Москва (1980).

2. R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).

3. P. W. Shor, *Proc. 35th Annual Symp. on Foundations of Computer Science*, Conf. Publ. (1994), p. 124.

4. L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

5. Y. Ozhigov, Chaos Solitons and Fractals **10**, 1707 (1999).

6. C. Zalka, arXiv:quant-ph/9603026.

7. *Quantum Algorithm Zoo*, math.nist.gov/quantum/zoo/.

8. C. H. Bennett and G. Brassard, *Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces.*, Bangalore, India (1984), p. 175.

9. G. S. Vernam, J. IEEE **55**, 109 (1926).

10. В. А. Котельников, *Отчет*, 19 июня (1941).

11. C. Shannon, Bell System Tech. J. **28**, 656 (1949).

12. R. Renner, PhD Thesis, ETH Zürich (2005).

13. C. Portmann and R. Renner, arXiv:1409.3525 [quant-ph].

14. H. P. Yuen, Phys. Rev. A **82**, 062304 (2010); H. P. Yuen, arXiv:1109.1051 [quant-ph]; H. P. Yuen, arXiv:1109.2675 [quant-ph]; H. P. Yuen, arXiv: 1109.1066 [quant-ph]; R. Renner, arXiv: 1209.2423 [quant-ph].

15. J. L. Massey, *Guessing and Entropy*, IEEE Int. Symp. on Inf. Theory (1994), p. 204.

16. J. O. Pliam, PhD Thesis, Minnesota Univ. (1999).

17. T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley (1991).

18. M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, Cambridge (2000).

19. A. De Santis, A. G. Gaggia, and U. Vaccaro, IEEE Trans. Inf. Theory **47**, 468 (2001).

20. А. С. Холево, УМН **53**, 324 (1998) [A. S. Holevo, Russ. Math. Surveys **53**, 1295 (1998)].

21. C. E. Shannon, Bell System Tech. J. **27**, 379 (1948).