Письма в ЖЭТФ, том 103, вып. 5, с. 389 – 393 © 2016 г. 10 марта

О сложности перебора ключей в квантовой криптографии

С. Н. Молотков[1)]

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 2 ноября 2015 г.
После переработки 18 января 2016 г.

Доказательства секретности ключей в квантовой криптографии используют в качестве критерия секретности следовое расстояние. В ряде работ высказывались сомнения в том, что данный критерий может быть сведен к критериям, которые используются в классической криптографии. В работе дается ответ на следующий вопрос. Пусть в результате работы системы квантовой криптографии получен ε-секретный ключ, который будет использоваться неоднократно в классических алгоритмах шифрования и про который гарантируется, что $\frac{1}{2}||\rho_{XE}-\rho_U\otimes\rho_E||_1<\varepsilon$. Насколько ε-секретный ключ уменьшит число шагов (трудоемкость) перебора по сравнению с использованием идеальных ключей? 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 ограничения на минимальное и максимальное число шагов перебора, за которые определяется истинный ключ.

DOI: 10.7868/S0370274X16050118

Введение. Конечным продуктом систем квантовой криптографии являются криптографические ключи, секретность которых гарантируется фундаментальными законами квантовой механики [1]. Доказательства секретности квантового распределения ключей являются достаточно сложными и многоходовыми. Секретность ключей в квантовой криптографии выражается в терминах близости к идеальной ситуации. Метрикой близости является следовая метрика [2]. В классической криптографии секретность ключей выражается в терминах, например, сложности перебора. Тот факт, что математический аппарат при доказательстве секретности ключей в классической и квантовой криптографии существенно различен, приводит к недопониманию и эмоциональным дискуссиям (см. [3]). Поэтому необходимо уметь отвечать на вопрос о том, как связаны между собой различные критерии криптостойкости. Ниже будет показана прямая связь между следовым расстоянием в квантовой криптографии и сложностью перебора ключей в классической криптографии.

Что гарантирует квантовая криптография? 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 (подробности см. в [4])

$$\rho_{XE}=\sum_{x\in X}P_X(x)|x\rangle\langle x|\otimes\rho_E^x, \qquad (1)$$

где состояние классического регистра с ключом x : $|x\rangle=|x_1\rangle\otimes|x_1\rangle\otimes\ldots\otimes|x_k\rangle$, $|X|=2^k$, $x\in X=\{0,1\}^k$, ρ_E^x – частичная матрица плотности квантовой системы подслушивателя (Евы), коррелированная с данным ключом x. Классическая информация, полученная Евой, также может быть включена в ρ_E^x. Свою оценку y ключа Алисы–Боба Ева получает в результате измерений над своей квантовой системой. Измерения Евы описываются разложением единицы $I_E=\sum_{y\in Y}\mathcal{M}_y$, $y\in Y=\{0,1\}^k$, где $\mathcal{M}_y$ – положительная операторно-значная мера в пространстве состояний Евы.

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

$$P_{X|Y}(X=x|y)=\mathrm{Tr}\{\mathcal{M}_y\rho_E^x\}. \qquad (2)$$

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

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

$$P_{X|Y}(X = x|x) = \mathrm{Tr}\{\mathcal{M}_x \rho_E^x\}, \quad y = x. \qquad (3)$$

Здесь использованы следующие обозначения: $P_{XY}(x,y)$ – 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: $P_{XY}(x,y) = P_X(x)P_{X|Y}(X = x|y)$, $P_{XY}(x,y) = P_{X|Y}(x|Y = y)P_Y(y)$, $\sum_{x\in X} P_{X|Y}(x|Y = y) = \sum_{y\in Y} P_{X|Y}(X = x|y) = 1$, $\sum_{x\in X} P_{XY}(x,y) = P_Y(y)$, $\sum_{y\in Y} P_{XY}(x,y) = P_X(x)$. Случайная битовая строка y является побочной информацией Евы о ключе x, к которому она не имеет доступа. Средняя вероятность угадывания Евы по всем ключам равна

$$P_{\mathrm{guess}}(X|E) = \max_{\{\mathcal{M}_x\}} \sum_{x\in X} P_X(x)\mathrm{Tr}\{\mathcal{M}_x \rho_E^x\} =$$
$$= \sum_{x\in X} P_X(x)P_{X|Y}(X = x|x) = \sum_{x\in X} P_{XY}(x,x), \qquad (4)$$

где $P_X(x)$ – вероятность появления ключа x. *Квантовая криптография гарантирует* [4], *что средняя по всем ключам вероятность угадывания не превосходит*

$$P_{\mathrm{guess}}(X|E) = \sum_{x\in X} P_{XY}(x,x) \leq$$
$$\leq \frac{1}{|X|} + \frac{1}{2}||\rho_{XE} - \rho_U \otimes \rho_E||_1 = \frac{1}{2^k} + \varepsilon, \qquad (5)$$

где $||\rho_{XE} - \rho_U \otimes \rho_E||_1$ – следовое расстояние ($||\rho||_1 = \mathrm{Tr}\{|\rho|\} = \mathrm{Tr}\{\sqrt{\rho\cdot\rho^*}\}$). Вся информация об атаках Евы содержится в ρ_{XE}. Однородная матрица плотности и матрица плотности Евы: $\rho_U = \frac{1}{|X|}\sum_{x\in X}|x\rangle\langle x|$, $\rho_E = \sum_{x\in X} P_X(x)\rho_E^x$. Ключи, удовлетворяющие условию (5), называются ε-секретными [2, 4]. Это означает, что вероятность исходов при любых измерениях над матрицами плотности ρ_{XE} и $\rho_U \otimes \rho_E$ отличается не более чем на ε. Следовое расстояние интуитивно прозрачно: невозможно отличить с вероятностью, большей ε, идеальную ситуацию (подсистема Евы не коррелирована с ключами, $\rho_U \otimes \rho_E$) от реальной (имеется корреляция между ключами легитимных пользователей и квантовой системой Евы, ρ_{XE}) [4].

Трудоемкость по перебору ключей (Guess Work), полученных в квантовой криптографии. Пусть используется идеальный ключ в классическом алгоритме шифрования. Известно, что в этом случае трудоемкость (число шагов перебора до определения фактического ключа, который вставлен в алгоритм) для злоумышленника при атаке "известный открытый текст–известный зашифрованный текст" составит $N/2$ (где $N = 2^k$) шагов.

Пусть в результате работы системы квантовой криптографии получен ε-секретный ключ, про который гарантируется, что $\frac{1}{2}||\rho_{XE} - \rho_U \otimes \rho_E||_1 < \varepsilon$. Вопрос: насколько ε-секретный ключ уменьшит число шагов (трудоемкость) перебора в смысле, обсуждаемом ниже, по сравнению с идеальными ключами?

Нашей целью является установление связи между сложностными критериями в атаках на алгоритмы шифрования и критериями секретности в квантовой криптографии. Одной из таких характеристик служит трудоемкость перебора, введенная в открытой печати в работе [5], где была установлена граница на работу угадывания в терминах энтропии Шеннона. Впоследствии выяснилось [6], что энтропия Шеннона не является мерой, в терминах которой удается получить плотную границу для работы угадывания.

Для дальнейшего важно, что в классической криптографии распределение вероятностей x неизвестно (обычно x задается генератором случайных чисел). Известно только, что уклонение распределения $P_X(x)$ от равномерного $P_U(x)$ не превосходит $\frac{1}{2}||P_X - P_U||_1 < \varepsilon$. Поясним неформальный смысл трудоемкости по перебору. Данный критерий возникает в так называемой атаке с избранным открытым текстом, когда Ева может передать для шифрования свой открытый текст. После этого Еве известна пара открытый–зашифрованный текст. Неизвестен только ключ шифрования.

Классическая криптография. Для алгоритма шифрования $\mathcal{F}$ генерируется случайный ключ x, подчиняющийся распределению вероятностей $P_X(x)$. Пусть x_j – конкретный текущий ключ. В криптографии всегда используются консервативные оценки криптостойкости в пользу подслушивателя. В пользу Евы всегда считают, что ей известно распределение $P_x(x)$. Зная это распределение, Ева упорядочивает перебираемые ключи в порядке убывания вероятностей: $P_X(x_1) \geq P_X(x_2) \geq \ldots \geq P_X(x_N)$. Пусть Ева может подсунуть открытый текст $message$, который будет зашифрован на данном ключе x_j. Зашифрованный текст $cipher$ есть $cipher = \mathcal{F}(x_j, message)$ (фактически $cipher, message$ – битовые строки). Теперь Ева знает $message$ и $cipher$. *Цель – найти* ключ x_j. Ева последовательно перебирает ключи до тех пор, пока не обнаружится совпадения входа и выхода $\mathcal{F}$, начиная с ключа с максимальной вероятностью.

Вероятность того, что для шифрования был выбран ключ x_1, есть $P_X(x_1)$ – первый шаг ($i = 1$ – номер попытки проверки ключа в сумме формулы (6), см. ниже). *Тогда с вероятностью $P_X(x_1)$ ключ будет определен на первом шаге. Если нет совпадения входа и выхода, то проверяется второй ключ x_2 (индекс числа шагов $i = 2$ в формуле* (6)) *и т.д. до совпадения. Математическое ожидание числа шагов по проверке ключей и есть трудоемкость перебора. Перебирая все ключи, Ева обязательно найдет истинный ключ в среднем за $G(X)$ шагов.* Таким образом, среднее число шагов до определения ключа есть

$$G(X) = \sum_{i=1}^{N} i \cdot P_X(x_i). \tag{6}$$

Для равномерного распределения $P_U(x)$, и только для него работа по угадыванию достигает максимума:

$$G_U(X) = \sum_{i=1}^{N} i \cdot P_U(x_i) = \frac{N+1}{2}. \tag{7}$$

Для $G(X)$ имеет место важная оценка (детали см. в [6]):

$$\frac{N+1}{2} - N||P_X - P_U||_1 \le G(X) \le \le \frac{N+1}{2} - \frac{N}{2}||P_X - P_U||_1. \tag{8}$$

Средняя трудоемкость (8) дает гарантированную границу на число шагов перебора подслушивателя до определения истинного ключа: число шагов перебора не меньше, чем левая граница (8).

В квантовой криптографии подслушиватель не имеет прямого доступа к ключам x, а имеет только свой ключ y – слепок ключа x, полученный в результате измерений (см. рис. 1a). *В реальной ситуации, как и в классическом случае, Еве неизвестны распределения $P_x(x)$, $P_{X|Y}(x|y)$. Опять в пользу Евы будем считать, что распределения ей известны.*

Пусть Евой получен результат измерения y. Данный слепок ключа Евы мог произойти из любого ключа x с вероятностью $P_{X|Y}(x_1|Y = y)$ (рис. 1b). Ева может упорядочить по мере убывания условные вероятности: $P_{X|Y}(x_1|Y = y) \ge P_{X|Y}(x_2|Y = y) \ge \ge \ldots \ge P_{X|Y}(x_N|Y = y)$, $N = |X|$. Аналогично предыдущему случаю Ева при заданном y перебирает все ключи x. Среднее число шагов перебора до определения истинного ключа при имеющемся у Евы y есть

$$G(X|Y = y) = \sum_{i=1}^{N} i \cdot P_{X|Y}(x_i|Y = y). \tag{9}$$

Нижеследующие формулы получены из (9) тождественными преобразованиями:

$$G(X|Y = y) = \frac{N+1}{2} - \sum_{i=1}^{N} Q_i(X|Y = y),$$

$$Q_i(X|Y = y) = \sum_{j=1}^{i} \left[P_{X|Y}(x_j|Y = y) - P_U(x_j)\right], \tag{10}$$

где $P_U(x_j) = \frac{1}{N}$ $\forall j$.

Формулы (9), (10) *дают среднее число шагов перебора при заданном слепке ключа y, имеющемся у Евы. Величина y имеет распределение $P_Y(y)$. Поэтому 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 $P_Y(y)$. Средняя сложность перебора по всем исходам y есть*

$$G(X|Y) = \sum_{y \in Y} P_Y(y) G(X|Y = y) = \tag{11}$$

$$= \sum_{y \in Y} P_Y(y) \left[\frac{N+1}{2} - \sum_{i=1}^{N} Q_i(X|Y = y)\right] =$$

$$= \frac{N+1}{2} - \sum_{i=1}^{N}\sum_{j=1}^{i} \left[\sum_{y \in Y} P_{X,Y}(x_j, y) - P_U(x_j)\right] =$$

$$= \frac{N+1}{2} - \sum_{i=1}^{N}\sum_{j=1}^{i} [P_X(x_j) - P_U(x_j)] =$$

$$= \frac{N+1}{2} - \sum_{i=1}^{N} Q_i(X),\ Q_i(X) = \sum_{j=1}^{i} [P_X(x_j) - P_U(x_j)].$$

Далее, по определению вариационного расстояния (*variational distance*, см., например, [7])

$$||P_X - P_U|| = Q_{\max}(X) = \max_i Q_i(X) =$$

$$= \sum_{j=1, P_X(x_j) > P_U(x_j)}^{i} [P_X(x_j) - P_U(x_j)]. \tag{12}$$

Вариационное расстояние связано со следовым расстоянием [7, 8]:

$$||P_X - P_U|| = \frac{1}{2}||P_X - P_U||_1 = \frac{1}{2}\sum_{j=1}^{N} |P_X(x_j) - P_U(x_j)|. \tag{13}$$

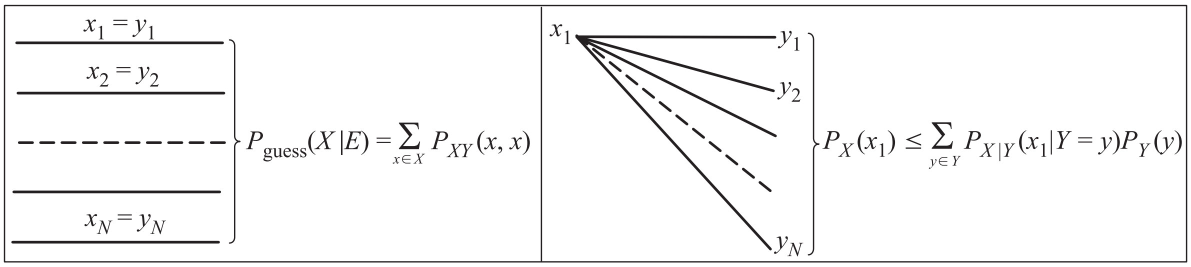

Рис. 1. (a) – Средняя по ключам вероятность угадывания. (b) – Средняя вероятность угадывания ключа по всем исходам подслушивателя

Потребуются два свойства следового расстояния между матрицами плотности. Следовое расстояние не возрастает при взятии частичного следа (в более общем виде оно не возрастает после применения квантовой операции [8]):

$$\frac{1}{2}||P_X - P_U||_1 \le \frac{1}{2}||\rho_{XE} - \rho_U \otimes \rho_E||_1 \le \varepsilon, \qquad (14)$$

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

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

Возвращаясь к формуле (11), с учетом (12)–(14) получаем, что число шагов перебора до определения истинного ключа не меньше чем

$$G(X|Y) \ge \frac{N+1}{2} - \sum_{i=1}^{N} \max_i\ Q_i(X) =$$
$$= \frac{N+1}{2} - N||P_X - P_U||_1 \ge \frac{N(1-2\varepsilon)}{2} + \frac{1}{2}. \qquad (15)$$

Аналогично получается оценка максимального числа шагов перебора, за которые можно определить истинный ключ. Окончательно трудоемкость перебора ключей при наличии побочной информации Евы, полученной из квантового и классического каналов, зажата в границах

$$\frac{N(1-2\varepsilon)}{2} + \frac{1}{2} \le G(X|Y) \le \frac{N(1-\varepsilon)}{2} + \frac{1}{2},$$
$$N = |X| = 2^k. \qquad (16)$$

Данные границы являются плотными (*tight bounds*). Формула (16) устанавливает фундаментальную связь между абстрактным критерием секретности в квантовой криптографии (расстоянием между реальной и идеальной ситуациями, $\frac{1}{2}||\rho_{XE} - \rho_U \otimes \rho_E||_1 < \varepsilon$) и трудоемкостью по перебору ключей в классических системах шифрования.

Связь между трудоемкостью перебора и максимальной вероятностью угадывания за один шаг. Следовое расстояние является интегральной характеристикой: в среднем уклонение вероятности от равномерного распределения не превосходит ε. Работа по угадыванию позволяет получить оценку на максимальную вероятность [9]. Пусть ключ x_1 имеет максимальную вероятность появления ($P_X(x_1) \ge P_X(x_2) \ge ...$). Согласно [9] имеем

$$P_X(x_1) \le 1 - \frac{2}{N}[G(X) - 1]. \qquad (17)$$

Данное неравенство выполняется 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

$$P_{X|Y}(x_1|Y=y) \le 1 - \frac{2}{N}[G(X|Y=y) - 1]. \qquad (18)$$

Сами исходы у Евы возникают с вероятностью $P_Y(y)$. Усредняя по всем побочным исходам y, находим, что вероятность угадывания истинного ключа x_1 (см. также пояснения на рис. 1b) не превосходит

$$P_X(x_1) \le \sum_{y\in Y} P_{X|Y}(x_1|Y=y)P_Y(y) \le$$
$$\le 1 - \frac{2}{N}\sum_{y\in Y}[G(X|Y=y) - 1]P_Y(y) =$$
$$= 1 - \frac{2}{N}[G(X|Y) - 1]. \qquad (19)$$

С учетом (19) получаем

$$P_{\max} = P_X(x_1) \le \frac{1}{N} + 2\varepsilon. \qquad (20)$$

Поскольку условная вероятность $P_{X|Y}(x_1|Y=y) \le 1$ и $P_Y(y) \le 1$, при любом значении y величина максимальной апостериорной вероятности не превышает значения (20). Максимальная вероятность связана с энтропией Реньи H_∞ бесконечного порядка:

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

Нужно подчеркнуть важное отличие между максимальной вероятностью угадывания и работой по угадыванию: *максимальная вероятность* (20) *представляет собой вероятность угадывания ключа x за одну попытку*, а *работа по угадыванию* (16) – *среднее число шагов перебора ключей до однозначного нахождения фактического ключа x*.

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

Выражаю благодарность И.М. Арбекову, А.Н. Климову и С.С. Назину за многочисленные обсуждения, а также коллегам по Академии криптографии Российской Федерации за постоянную поддержку.

1. C. H. Bennett and G. Brassard, *Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces.*, Bangalore, India (1984), p. 175.
2. R. Renner, *Security of Quantum Key Distribution*, PhD Thesis, ETH Zürich (2005).
3. H. P. Yuen, Phys. 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, 1209.2423 [quant-ph].
4. C. Portmann and R. Renner, arXiv: 1409.3525 [quant-ph].
5. J. L. Massey, IEEE Int. Symp. on Information Theory, 204 (1994).
6. J. O. Pliam, *Ciphers and their Products: Group Theory in Private Key Cryptography*, Doctor Philosophy Thesis, Minnesota University (1999).
7. T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley (1991).
8. M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, Cambridge (2000).
9. A. De Santis, A. G. Gaggia, and U. Vaccaro, IEEE Transactions on Information Theory **47**, 468 (2001).