ЖЭТФ, 2017, том 152, вып. 1 (7), стр. 62–78

РАЗЛИЧИМОСТЬ КВАНТОВЫХ СОСТОЯНИЙ И ТРУДОЕМКОСТЬ ПО ШЕННОНУ В КВАНТОВОЙ КРИПТОГРАФИИ

И. М. Арбеков [a], ***С. Н. Молотков*** [a,b,c*]

[a] *Академия криптографии Российской Федерации*
121552, Москва, Россия

[b] *Институт физики твердого тела Российской академии наук*
142432, Черноголовка, Московская обл., Россия

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

Поступила в редакцию 30 января 2017 г.

Доказательства секретности квантового распределения ключей являются достаточно сложными. Секретность определяется в терминах, которые отличаются от требований, предъявляемых к ключам в классической криптографии. Секретность ключей в квантовой криптографии выражается в терминах близости квантового состояния подслушивателя после распределения ключей к идеальному квантовому состоянию, которое некоррелировано с ключом легитимных пользователей. Метрикой близости двух квантовых состояний является следовая метрика. В классической криптографии секретность ключей понимается в терминах, например, сложности перебора ключей при наличии побочной информации. В квантовой криптографии побочной информацией для подслушивателя является вся совокупность информации о ключах, полученная как из квантового, так и классического каналов. Тот факт, что математический аппарат при доказательстве секретности ключей в классической и квантовой криптографии существенно разный, приводит к недопониманию и эмоциональным дискуссиям [1]. Поэтому необходимо уметь отвечать на вопрос, как связаны между собой различные критерии криптостойкости. В данной работе показана прямая связь между критерием секретности в квантовой криптографии, основанном на следовом расстоянии, определяющим различимость квантовых состояний, и критерием, использующим трудоемкость (guess work) по определению ключа при наличии побочной информации, в классической криптографии.

DOI: 10.7868/S0044451017070069

1. ВВЕДЕНИЕ

Конечным продуктом работы систем квантовой криптографии являются секретные ключи, которые впоследствии используются для шифрования информации. Секретность ключей в квантовой криптографии гарантируется фундаментальными законами квантовой механики. Математически секретность ключей формулируется в терминах различимости квантовых состояний [2, 3]. Пара квантовых состояний считается ε-неразличимой, если никакими измерениями невозможно отличить одно квантовое состояние от другого с вероятностью успеха, превышающей вероятность простого угадывания более, чем на ε.

Для секретных ключей, используемых в различных алгоритмах шифрования, предъявляются требования, которые формулируются совершенно в других терминах. Шенноном [4] был введен критерий практической секретности криптосистемы, который понимается как “the average amount of work to determine the key for a cryptogram...”. Данный критерий не был формализован, поэтому в зависимости от ситуации возможны различные критерии средней работы (трудоемкости) по определению ключа. Само понятие трудоемкости фактически связано с перебором (опробованием) ключей до определения

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

истинного ключа. Причем перебор может быть как полным — по всему пространству ключей, так и частичным — по части ключевого пространства [5]. Такой перебор может иметь место как в отсутствие побочной информации о ключе, так и при наличии дополнительной информации. Применительно к ключам, полученным в результате квантового распределения ключей, побочная информация о ключе у подслушивателя возникает при измерениях над квантовой системой, коррелированной с истинным ключом легитимных пользователей.

Необходимо четкое понимание того, как внешне совершенно разные критерии секретности в квантовой области и классической криптографии связаны между собой. Без выяснения четкой связи между различными критериями остается неясным, насколько безопасно можно использовать ключи, полученные в результате квантового распределения ключей для различных криптосистем.

В данной работе установлена прямая связь между критерием секретности, основанном на различимости пары квантовых состояний, и различными критериями, использующими понятие трудоемкости — сложности перебора — по экспоненциально большому (по длине ключа) пространству ключей в классической криптографии. Ниже будут рассмотрены различные ситуации, и по мере их возникновения будет определено понятие трудоемкости для каждой ситуации.

2. МЕРЫ РАЗЛИЧИМОСТИ КВАНТОВЫХ СОСТОЯНИЙ

В квантовой теории информации естественными и широко используемыми мерами различимости (близости) квантовых состояний являются две меры: следовое расстояние и соответствие (fidelity), которые связаны между собой [6]. Следовое расстояние между двумя квантовыми состояниями — матрицами плотности ρ и σ — по определению есть

$$D(\rho,\sigma) = ||\rho-\sigma||_1 = \frac{1}{2}\mathrm{Tr}\left\{\sqrt{(\rho-\sigma)(\rho-\sigma)^+}\right\} = \\ = \frac{1}{2}\mathrm{Tr}\left\{|\rho-\sigma|\right\}. \quad (1)$$

Следовое расстояние $D(\rho,\sigma)=0$, когда $\rho=\sigma$. Чем меньше следовое расстояние, тем менее различимы квантовые состояния. Соответствие по определению равно

$$F(\rho,\sigma) = ||\sqrt{\rho}\sqrt{\sigma}||_1 = \mathrm{Tr}\left\{\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right\}. \quad (2)$$

Когда состояния одинаковы, $\rho=\sigma$, то $F(\rho,\sigma)=1$, таким образом, чем ближе квантовые состояния, тем ближе $F(\rho,\sigma)$ к единице. Две меры различимости квантовых состояний связаны между собой полезными неравенствами [6]:

$$1-\sqrt{F(\rho,\sigma)} \le D(\rho,\sigma) \le \sqrt{1-F(\rho,\sigma)}. \quad (3)$$

Операциональный смысл следового расстояния состоит в следующем. Пусть для измерений равновероятно предъявляются состояния ρ или σ. Какова вероятность ($\mathrm{Pr}_{success}$) успешного различения квантовых состояний?

Различение квантовых состояний происходит в результате измерений. Любое измерение в квантовой механике дается разложением единицы. По сути разложение единицы является формальным описанием измерительного прибора. Пусть I — единичный оператор в пространстве состояний, где действуют матрицы плотности двух квантовых состояний ρ и σ. Для измерения с двумя исходами 0 и 1 имеем

$$I = \mathcal{M}_0 + \mathcal{M}_1, \quad (4)$$

где $\mathcal{M}_{0,1}$ — положительные операторно-значные меры. Если предъявлено состояние ρ, то вероятность результата измерения, дающего правильную интерпретацию состояния, есть

$$\mathrm{Pr}(0|\rho) = \mathrm{Tr}\{\mathcal{M}_0\rho\}. \quad (5)$$

В формуле (5) определена условная вероятность того, что было предъявлено состояние ρ и результат измерения был равен нулю. Аналогично условная вероятность правильной интерпретации состояния σ есть

$$\mathrm{Pr}(1|\sigma) = \mathrm{Tr}\{\mathcal{M}_1\sigma\}. \quad (6)$$

Учитывая равновероятное предъявление состояний и принимая во внимание, что $\mathrm{Tr}\{\rho\}=\mathrm{Tr}\{\sigma\}=1$, находим для максимальной вероятности правильного различения состояний:

$$\mathrm{Pr}_{succes} = \max_{0\le\mathcal{M}_0\le I}\left(\frac{1}{2}\mathrm{Tr}\{\mathcal{M}_0\rho\}+\frac{1}{2}\mathrm{Tr}\{\mathcal{M}_1\sigma\}\right) = \\ = \frac{1}{2}\left(1+\max_{0\le\mathcal{M}_0\le I}\mathrm{Tr}\{\mathcal{M}_0(\rho-\sigma)\}\right). \quad (7)$$

Известно, что следовое расстояние есть максимум по всем измерениям (см., например, [6]):

$$\max_{0\le\mathcal{M}_0\le I}\mathrm{Tr}\{\mathcal{M}_0(\rho-\sigma)\} = D(\rho,\sigma). \quad (8)$$

Для вероятности успешного различения одного из двух состояний с учетом (7), (8) получаем

$$\mathrm{Pr}_{succes} = \frac{1}{2}+\frac{1}{2}D(\rho,\sigma). \quad (9)$$

Если следовое расстояние $D(\rho,\sigma)=0$, то вероятность отличить одно состояние от другого равна вероятности простого угадывания — $\Pr_{success}=1/2$ — состояния неразличимы.

В контексте квантовой криптографии под матрицами плотности ρ и σ следует понимать матрицы ρ_{XE} и $\rho_U\otimes\rho_E$. В результате измерений над этими матрицами плотности возникают классические распределения вероятностей: $\rho_{XE}\to P_{XY}(x,y)$ и $\rho_U\otimes\otimes\rho_E\to P_U(x)\cdot P_Y(y)$, которые определяют трудоемкость перебора ключей (см. следующие разделы).

2.1. Различение квантовых состояний в квантовой криптографии

В квантовой криптографии после выполнения протокола легитимные пользователи имеют общую битовую строку — секретный ключ $x=(x_1,x_2,\ldots,x_n)$ ($x\in X=\{0,1\}^n$, значение бита в i-й позиции конкретного ключа x есть $x_i=0,1$), а подслушиватель в общем случае — квантовую систему ρ_E^x, коррелированную с данным ключом. Данный результат получается после выполнения всех стадий протокола квантовой криптографии: передачи и измерения квантовых состояний, согласования базисов (если это требуется по протоколу), коррекции ошибок и усиления секретности — сжатия очищенных ключей при помощи универсальных хеш-функций второго порядка [2]. В конце квантового протокола распределения ключей возникает ситуация, которую будем называть реальной ситуацией. Квантовое состояние — матрица плотности ρ_{XE} описывает реальную ситуацию в конце протокола.

Пусть вероятность распределения конкретного ключа x есть $P_X(x)$. Классической битовой строке — ключу — удобно сопоставить состояние квантовой системы: $x=(x_1,x_2,\ldots,x_n)\to|x\rangle=|x_1\rangle\otimes\otimes|x_2\rangle\otimes\ldots\otimes|x_n\rangle$. Квантовые состояния для разных ключей ортогональны, так как по построению $\langle x_i|x_j\rangle=\delta_{ij}$. Имеем

$$\rho_{XE}=\sum_{x\in X}P_X(x)|x\rangle\langle x|\otimes\rho_E^x. \tag{10}$$

Идеальной ситуацией является ситуация, когда ключи легитимных пользователей имеют равномерное распределение $P_U(x)=1/N$ ($N=2^n$). Аналогично данный набор идеальных ключей удобно описывать квантовым состоянием

$$\rho_U=\frac{1}{N}\sum_{x\in X}|x\rangle\langle x|. \tag{11}$$

В идеальной ситуации идеальные ключи полностью некоррелированы с квантовым состоянием подслушивателя ρ_E^x, и $\rho_E=\sum_{x\in X}P_X(x)\rho_E^x$, которое дается частичным следом $\rho_E=\mathrm{Tr}_X\{\rho_{XE}\}$, т. е. идеальная ситуация описывается матрицей плотности $\rho_U\otimes\rho_E$.

Ключи, полученные в результате квантового распределения, являются ε-секретными [2, 3], если два квантовых состояния ρ_{XE} и $\rho_U\otimes\rho_E$, описывающие реальную и идеальную ситуации, различимы с вероятностью успеха, превышающей вероятность простого угадывания не более, чем на ε — следовое расстояние между двумя квантовыми состояниями не превосходит ε:

$$D(\rho_{XE},\rho_U\otimes\rho_E)=||\rho_{XE}-\rho_U\otimes\rho_E||_1<\varepsilon. \tag{12}$$

Таким образом, секретность ключей в квантовой криптографии дается в терминах различимости двух квантовых состояний ρ_{XE} и $\rho_U\otimes\rho_E$, описывающих соответственно реальную и идеальную ситуации. Неформально это означает, что подслушиватель не может отличить с вероятностью большей, чем ε, ключи, полученные в реальной ситуации, от ключей в идеальной ситуации, когда какая-либо корреляция между ключами легитимных пользователей, которые являются идеально случайными и равнораспределенными, и квантовой системой подслушивателя полностью отсутствует.

3. ТРУДОЕМКОСТЬ ПО ШЕННОНУ — СЛОЖНОСТЬ ПЕРЕБОРА КЛЮЧЕЙ

Рассмотрим кратко некоторые критерии секретности криптосистемы в классической криптографии, основанные на трудоемкости по Шеннону. Возможны различные варианты использования ключей. В разных ситуациях понятие трудоемкости может быть разным.

Отклонение распределения ключей от идеального равномерного ($P_X(x)\neq P_U(x)$), а также побочная информация подслушивателя о ключах могут уменьшить число шагов перебора (трудоемкость — guess work) для нахождения истинного ключа [5, 7, 8] при различных атаках на алгоритм шифрования (атаки с известным открытым текстом, с избранным открытым текстом и т. д.).

Рассмотрим следующий пример. Для алгоритма шифрования $\mathcal{F}$ генерируется случайный ключ x, подчиняющийся распределению вероятностей $P_X(x)$. В криптографии всегда используются консервативные оценки криптостойкости в пользу подслушивателя. Всегда считается, что подслушивателю известно распределение $P_X(x)$. Зная

распределение, подслушиватель упорядочивает перебираемые ключи в порядке убывания вероятностей: $P_X(x_1) \geq P_X(x_2) \geq \ldots \geq P_X(x_N)$. Консервативно считаем, что известны открытый текст, который зашифрован на ключе $\overline{x}$, и шифр-текст (*message–cypher*). Зашифрованный текст есть $cypher = \mathcal{F}(\overline{x}, message)$ ($cypher, message$ — битовые строки). Теперь подслушиватель знает $message$ и $cypher$, а цель — найти ключ $\overline{x}$. Подслушиватель опробует последовательно ключи до тех пор, пока не будет совпадения входа и выхода $\mathcal{F}$, начиная с ключа с максимальной вероятностью. При полном переборе истинный ключ будет найден с вероятностью успеха, равной единице.

Здесь неявно считаем, что алгоритм шифрования настолько хорош, что неизвестны другие эффективные алгоритмы определения истинного ключа, кроме полного перебора. Хотя перебор ключей может использоваться в любой другой ситуации.

Возможны ситуации, когда подслушиватель перебирает только часть наиболее вероятных ключей. При этом вероятность успеха — нахождения истинного ключа — будет меньше единицы. Вероятность успеха может быть фиксирована заранее какими-то требованиями. Возможны следующие ситуации.

1. Один и тот же ключ $\overline{x}$ генерируется в соответствии с распределением вероятностей $P_X(x)$ и используется в алгоритме шифрования многократно. Подслушиватель знает распределение вероятностей $P_X(x)$, но не знает конкретный ключ и не имеет побочной информации о нем. Подслушиватель может осуществлять полный или частичный перебор ключей.

2. Каждое сообщение шифруется на новом ключе $\overline{x}$, ключи подчиняются распределению вероятностей $P_X(x)$. Подслушиватель не имеет побочной информации о ключе. Аналогично предыдущему пункту подслушиватель может осуществлять полный или частичный перебор ключей.

3. Ключ $\overline{x}$ используется для шифрования неоднократно. Подслушиватель обладает побочной информацией о ключе в виде случайной битовой строки $y \in Y = \{0,1\}^n$, которая коррелирована с ключом и получается в результате измерений подслушивателя над квантовой системой $\rho_E^{\overline{x}}$ (см. (10)). Корреляции между ключами x и побочной переменной y даются совместным распределением вероятностей $P_{XY}(x,y)$, которое считается известным подслушивателю.

4. Аналогично пункту 2 каждое сообщение шифруется на своем ключе. Подслушиватель обладает побочной информацией о ключе. В этой ситуации перебор ключей может быть полным или частичным.

В первой и второй ситуациях естественной мерой трудоемкости является среднее число шагов полного или частичного перебора ключей до определения истинного ключа [5]. При полном переборе трудоемкость обычно называется работой по угадыванию (guess work) $G(X)$ [7,9]. Решение о совпадении опробоваемого и истинного ключей может происходить по некоторому критерию читаемости текста либо с использованием атаки с известным открытым текстом (см. пример выше). Критерий читаемости означает, что ключ опробования x_{test} дает осмысленное сообщение m_{test} из зашифрованного c: $m_{test} = \mathcal{F}^{-1}(x_{test}, c)$. Определение ключа позволяет читать все последующие сообщения, зашифрованные на данном ключе.

Во второй ситуации $G(X)$ будет означать среднее число шагов перебора до определения ключа — прочтения одного данного сообщения, зашифрованного на данном ключе.

В третьей и четвертой ситуациях подслушиватель имеет дополнительную побочную информацию об истинном ключе, которая возникает при измерениях над квантовой системой при квантовом распределении ключей и которая может уменьшить трудоемкость по определению ключа.

При полном переборе по всему пространству ключей ключ определяется с вероятностью единица. Можно ослабить данное требование и интересоваться числом шагов (трудоемкостью), когда ключ определяется с некоторой заданной вероятностью успеха π_0.

Из сказанного видно, что мера трудоемкости может быть разной в зависимости от ситуации. Ниже рассмотрим меры трудоемкости в различных ситуациях. Данные меры будут выражаться через следующие распределения вероятностей: $P_X(x)$ — распределение истинных ключей, $P_Y(y)$ — распределение побочной переменной y (битовой строки), $P_{XY}(x,y)$ — их совместное распределение.

Ниже будет показано, что все данные меры трудоемкости в классическом случае могут быть выражены через меру различимости квантовых состояний, а именно, следовое расстояние (12). Тем самым будет установлена прямая связь между критерием секретности в квантовой криптографии и различными критериями секретности в классической криптографии.

4. НИЗКАЯ РАЗЛИЧИМОСТЬ КВАНТОВЫХ СОСТОЯНИЙ ГАРАНТИРУЕТ БОЛЬШУЮ ТРУДОЕМКОСТЬ ПЕРЕБОРА КЛЮЧЕЙ

Основной целью следующих разделов будет доказательство того, что низкая различимость квантовых состояний ρ_{XE} и $\rho_U \otimes \rho_E$ (эквивалентно, ε-секретность ключей) гарантирует большую трудоемкость в различных ситуациях.

Из следующих разделов будет видно, что верхние и нижние границы для различных типов трудоемкости в классической криптографии выражаются через следовое расстояние между классическими распределениями,

$$D\left(P_{XY}, \frac{P_Y}{N}\right) = \\ = \frac{1}{2}\sum_{y\in Y}\sum_{x\in X}\left|P_{XY}(x,y) - \frac{P_Y(y)}{N}\right|, \quad (13)$$

причем сами классические распределения ключей x и побочной переменной y возникают и зависят от квантовомеханических измерений подслушивателя над квантовыми состояниями (10).

Будет показано, что следовое расстояние (13) между классическими распределениями мажорируется следовым расстоянием между двумя матрицами плотности ρ_{XE} и $\rho_U \otimes \rho_E$ (см. выше). Это будет означать, что критерия секретности в квантовой криптографии, основанном на различимости квантовых состояний, достаточно для критериев секретности, основанных на различных видах трудоемкости по Шеннону в классической криптографии.

4.1. Связь измерений с классическими распределениями вероятностей

В этом разделе покажем, что две меры (12) и (13) связаны между собой через квантовомеханические измерения, которые проводит подслушиватель над своей квантовой системой ρ_E^x (см. формулу (10)), и в результате которых получает побочную переменную — битовую строку y длиной n.

В дальнейшем для мажорирования следового расстояния (13) нам потребуется следующее равенство:

$$D(\rho_{XE}, \rho_U\otimes\rho_E) = \\ = \max_{\{0\le\Lambda\le I_{XE}\}} \mathrm{Tr}_{XE}\{\Lambda(\rho_{XE} - \rho_U\otimes\rho_E)\}, \quad (14)$$

где Λ — любой положительный оператор $0 \le \Lambda \le I_{XE}$ (I_{XE} — единичный оператор в пространстве состояний XE). Матрицы плотности переходят в распределения вероятностей после измерений. Любое измерение в квантовой механике дается разложением единицы. Рассмотрим разложение единицы специального вида. Поскольку оператор

$$\rho_{XE} - \rho_U\otimes\rho_E = \sum_{x\in X}|x\rangle\langle x|\otimes\left(P_X(x)\rho_E^x - \frac{\rho_E}{N}\right) \quad (15)$$

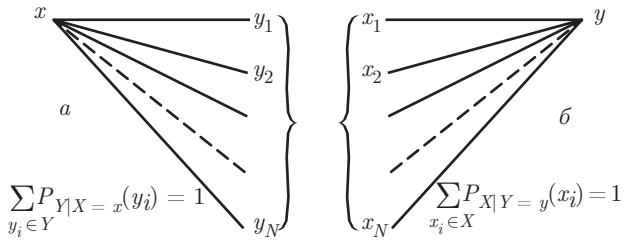
является квантово-классическим, максимум в правой части (14) достигается на измерениях, имеющих такую же квантово-классическую структуру, так как операторы $P_X(x)\rho_E^x - \rho_E/N$ при разных x действуют в ортогональных подпространствах. Обратим внимание, что операторная мера $\mathcal{M}_y$ не зависит от x.

Вычисляя (14), в качестве оператора Λ возьмем единичный оператор $\Lambda = I_{XE}$, описывающий измерение, разложение которого имеет квантово-классический вид:

$$I_{XE} = \sum_{y\in Y}\sum_{x\in X}|x\rangle\langle x|\otimes\mathcal{M}_y = \sum_{x\in X}\sum_{y\in Y}\mathcal{F}_{x,y}, \\ \mathcal{F}_{x,y} = |x\rangle\langle x|\otimes\mathcal{M}_y. \quad (16)$$

Здесь $\mathcal{M}_y$ — положительная операторно-значная мера, явный вид которой нам не потребуется.

Такой выбор измерений отвечает фактически следующей ситуации. Воспользуемся статистической интерпретацией квантового состояния — ансамбля, который описывается матрицей плотности (10). Пусть проведено квантовое распределение ключей, в итоге возник конкретный ключ x_1, а подслушиватель имеет квантовую систему $\rho_E^{x_1}$. При этом такая ситуация реализуется с вероятностью $P_X(x_1)$. Далее проводится в тех же условиях следующее квантовое распределение ключей — возникает ключ x_2 и квантовая система у подслушивателя $\rho_E^{x_2}$, и т. д. Выбор измерения в виде (16) отвечает индивидуальным измерениям над квантовыми системами подслушивателя $\rho_E^{x_1}\otimes\rho_E^{x_2}\otimes\ldots\otimes\rho_E^{x_n}$ с целью различить $\rho_E^{x_i}$, а значит, и x_i, после каждого i-го сеанса распределения ключей. В принципе возможны и коллективные измерения (проекции на запутанные состояния) сразу над всей последовательностью $\rho_E^{x_1}\otimes\rho_E^{x_2}\otimes\ldots\otimes\rho_E^{x_n}$, что может дать подслушивателю дополнительный выигрыш. Данный вопрос требует отдельного рассмотрения. Забегая вперед, заметим, что и в этом случае следового расстояния (12) оказывается достаточно для вычисления различных типов трудоемкостей.



Пояснение обозначений для условных вероятностей

Для первого слагаемого в правой части (14) находим

$$\begin{aligned}\mathrm{Tr}_{XE}\{I_{XE}\ \rho_{XE}\} &= \\ &= \mathrm{Tr}_{XE}\left\{\left(\sum_{y\in Y}\sum_{x\in X}|x\rangle\langle x|\otimes\mathcal{M}_y\right)\times\right. \\ &\left.\times\left(\sum_{x'\in X}P_X(x')|x\rangle\langle x'|\otimes\rho_E^{x'}\right)\right\} = \\ &= \sum_{y\in Y}\sum_{x\in X}P_X(x)P_{Y|X=x}(y) = \\ &= \sum_{y\in Y}\sum_{x\in X}P_{XY}(x,y). \quad (17)\end{aligned}$$

В (17) учтено, что по формуле Байеса условное и совместное распределения вероятностей связаны соотношением

$$\begin{aligned}P_{XY}(x,y) &= P_X(x)P_{Y|X=x}(y) = \\ &= P_Y(y)P_{X|Y=y}(x), \quad (18)\\ P_{Y|X=x}(y) &= \mathrm{Tr}\{\mathcal{M}_y\rho_E^x\}.\end{aligned}$$

Здесь $P_{Y|X=x}(y)$ — условная вероятность того, что в результате измерений (16) будет получено значение побочной переменной y, при условии, что истинный ключ легитимных пользователей есть x. Соответственно, условие нормировки для $P_{X|Y=y}(x)$ имеет вид

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

Неформально условная вероятность $P_{Y|X=x}(y)$ вместе с условием нормировки интерпретируется следующим образом: данная битовая строка x обязательно перейдет в какую-то битовую строку y.

Поскольку обозначения условных вероятностей, используемые в различных статьях, отличаются друг от друга, во избежание путаницы необходимо пояснить обозначения, см. рисунок. На рис. *а* показаны условные вероятности $P_{Y|X=x}(y)$ — каждый x может при измерениях перейти в разные y. В дальнейшем потребуется условное распределение вероятностей $P_{X|Y=y}(x)$. Для наглядности различие между двумя условными распределениями показана на рис. *б*. Соответственно условие нормировки $P_{X|Y=y}(x)$ имеет вид

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

Далее для второго слагаемого в правой части (14) находим

$$\begin{aligned}&\mathrm{Tr}_{XE}\{I_{XE}\ \rho_U\otimes\rho_E\} = \\ &= \mathrm{Tr}_{XE}\left\{\left(\sum_{y\in Y}\sum_{x\in X}|x\rangle\langle x|\otimes\mathcal{M}_y\right)\times\right. \\ &\left.\times\left(\frac{1}{N}\sum_{x''\in X}|x''\rangle\langle x''|\right)\left(\sum_{x'\in X}P_X(x')\rho_E^{x'}\right)\right\} = \quad (19)\\ &= \sum_{y\in Y}\sum_{x\in X}\frac{P_Y(y)}{N},\\ &P_Y(y) = \mathrm{Tr}\{\mathcal{M}_y\rho_E\}, \quad \rho_E = \sum_{x\in X}P_X(x)\rho_E^x.\end{aligned}$$

Далее нам еще потребуются некоторые важные соотношения. Воспользуемся связью вариационного и следового расстояний (см. [7, 10]). Пусть $P_1(a)$ и $P_2(a)$ — пара распределений вероятностей ($a \in \overline{A} = A + A^c$), тогда

$$\begin{aligned}||P_1(a) - P_2(a)||_1 &= \frac{1}{2}\sum_{a\in(A+A^c)}|P_1(a) - P_2(a)| = \\ &= \frac{1}{2}\left(\sum_{a\in A}(P_1(a)-P_2(a)) + \sum_{a\in A^c}(P_2(a)-P_1(a))\right) = \\ &= \frac{1}{2}(P_1(A) - P_2(A) + P_2(A^c) - P_1(A^c)) = \\ &= \frac{1}{2}(P_1(A)-P_2(A)+1-P_2(A)-1+P_1(A)) = \\ &= P_1(A) - P_2(A) = \\ &= \sum_{a:(P_1(a)-P_2(a))>0}(P_1(a) - P_2(a)). \quad (20)\end{aligned}$$

В формуле (20) суммирование идет по подмножествам, где $P_1(a) - P_2(a) > 0$, т. е. A — набор подмножеств, где $P_1(a) > P_2(a)$, соответственно A^c — дополнительное множество, где $P_2(a) > P_1(a)$, и

$$P_{1,2}(A) = \sum_{a\in A}P_{1,2}(a), \quad P_{1,2}(A^c) = \sum_{a\in A^c}P_{1,2}(a).$$

Нашей целью будет показать, что для любых измерений имеет место соотношение

$$\left\|P_{XY}-\frac{P_Y}{N}\right\|_1 = \sum_{(x,y)\in(X,Y);P_{XY}(x,y)-\frac{P_Y(y)}{N}>0}\left(P_{XY}(x,y)-\frac{P_Y(y)}{N}\right)\leq \leq D(\rho_{XE},\rho_U\otimes\rho_E)<\varepsilon. \quad (21)$$

Используя спектральное разложение разности операторов $\rho_{XE}-\rho_U\otimes\rho_E$, находим (см. детали, например, в [6])

$$\rho_{XE}-\rho_U\otimes\rho_E = R_+ - R_-,\quad R_+=\sum_{\xi_i>0}\xi_i|\xi_i\rangle\langle\xi_i|,\quad R_-=-\sum_{\xi_i\leq 0}\xi_i|\xi_i\rangle\langle\xi_i|. \quad (22)$$

Здесь ξ_i — собственные числа $\rho_{XE}-\rho_U\otimes\rho_E$, $|\xi_i\rangle$ — собственные векторы, $\langle\xi_i|\xi_J\rangle=\delta_{ij}$. Далее пусть

$$P_+=\sum_{\xi_i>0}|\xi_i\rangle\langle\xi_i|,\quad P_-=\sum_{\xi_i\leq 0}|\xi_i\rangle\langle\xi_i| \quad (23)$$

— проекторы на подпространства, отвечающие положительным и отрицательным собственным числам, тогда

$$D(\rho_{XE},\rho_U\otimes\rho_E)=\frac{1}{2}\mathrm{Tr}\{|\rho_{XE}-\rho_U\otimes\rho_E|\}= =\frac{1}{2}\left(\mathrm{Tr}\{R_+\}+\mathrm{Tr}\{R_-\}\right), \quad (24)$$

и так как $\mathrm{Tr}\{\rho_{XE}-\rho_U\otimes\rho_E\}=0$, то

$$\mathrm{Tr}\{R_+\}=\mathrm{Tr}\{R_-\},\quad \mathrm{Tr}\{|R_+-R_-|\}=\mathrm{Tr}\{R_+\}+\mathrm{Tr}\{R_+\}. \quad (25)$$

С учетом изложенного выше находим

$$\mathrm{Tr}\{P_+(\rho_{XE}-\rho_U\otimes\rho_E)\}=\mathrm{Tr}\{R_+\}= =D(\rho_{XE},\rho_U\otimes\rho_E) \quad (26)$$

и, наконец,

$$\mathrm{Tr}\{\Lambda(\rho_{XE}-\rho_U\otimes\rho_E)\}=\mathrm{Tr}\{\Lambda(R_+-R_-)\}\leq \leq\mathrm{Tr}\{\Lambda R_+\}\leq\mathrm{Tr}\{R_+\}=D(\rho_{XE},\rho_U\otimes\rho_E). \quad (27)$$

Из формул (24)–(27) для любого оператора ($0\leq\Lambda\leq I_{XE}$) следует цепочка неравенств:

$$|\mathrm{Tr}\{\Lambda(\rho_{XE}-\rho_U\otimes\rho_E)\}|=|\mathrm{Tr}\{\Lambda(R_+-R_-)\}|\leq \leq\mathrm{Tr}\{\Lambda(R_+-R_-)\}=\mathrm{Tr}\{\Lambda|\rho_{XE}-\rho_U\otimes\rho_E|\}. \quad (28)$$

Учитывая (16)–(19), (28) и в качестве Λ выбирая $\Lambda=\mathcal{F}_{x,y}$, получаем

$$\left\|P_{XY}-\frac{P_Y}{N}\right\|_1=\frac{1}{2}\sum_{x\in X}\sum_{y\in Y}\left|P_{XY}(x,y)-\frac{P_Y(y)}{N}\right|= =\frac{1}{2}\sum_{x\in X}\sum_{y\in Y}|\mathcal{F}_{x,y}(\rho_{XE}-\rho_U\otimes\rho_E)|\leq \leq\frac{1}{2}\sum_{x\in X}\sum_{y\in Y}\mathrm{Tr}\{\mathcal{F}_{x,y}|\rho_{XE}-\rho_U\otimes\rho_E|\}= =\frac{1}{2}\mathrm{Tr}\{|\rho_{XE}-\rho_U\otimes\rho_E|\}= =D(\rho_{XE},\rho_U\otimes\rho_E)<\varepsilon, \quad (29)$$

что приводит нас к нужному неравенству (21).

Для дальнейшего выведем связь соответствия между классическими распределениями вероятностей со следовым расстоянием. С учетом выражений (3), (29) получаем

$$1-\sqrt{F(\rho_{XE},\rho_U\otimes\rho_E)}\leq D(\rho_{XE},\rho_U\otimes\rho_E)\leq \leq\sqrt{1-F(\rho_{XE},\rho_U\otimes\rho_E)}, \quad (30)$$

принимая во внимание (14), находим

$$1-\sqrt{F\left(P_{XY},\frac{P_Y}{N}\right)}\leq D\left(P_{XY},\frac{P_Y}{N}\right)\leq \leq\sqrt{1-F\left(P_{XY},\frac{P_Y}{N}\right)}. \quad (31)$$

Таким образом, верхняя граница следового расстояния между классическими распределениями вероятностей мажорируется следовым расстоянием между двумя матрицами плотности ρ_{XE} и $\rho_U\otimes\rho_E$, описывающими реальную и идеальную ситуации после квантового распределения ключей.

4.2. Средняя вероятность угадывания по пространству ключей

Из результатов предыдущего раздела можно получить среднюю вероятность угадывания подслушивателя по всем ключам. Пусть подслушиватель имеет в своем распоряжении побочную переменную y, коррелированную с истинным ключом x. Условная вероятность получить при измерениях y, если истинный ключ x, равна

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

где $x\in X=\{0,1\}^n$ и $y\in Y=\{0,1\}^n$ — множества битовых строк. Пусть множества строк перенумерованы одинаковым способом, тогда между $y=x\in Y$ и $x\in X$ возникает взаимно однозначное соответствие.

Средняя по всем ключам x вероятность угадывания равна

$$\Pr_{key\ guess} = \sum_{x\in X} P_X(x)P_{Y|X=x}(x) = \sum_{x\in X} P_{XY}(x,x). \quad (32)$$

Найдем верхнюю границу для (32). Учитывая (21), выводим, что для любых измерений имеет место следующая цепочка неравенств:

$$\begin{aligned}
&\sum_{(x,y)\in(X,Y)} \left(P_{XY}(x,y) - \frac{P_Y(y)}{N}\right) \le \sum_{(x,y)\in(X,Y):\left(P_{XY}(x,y)-\frac{P_Y(y)}{N}\right)>0} \left(P_{XY}(x,y) - \frac{P_Y(y)}{N}\right) \le \\
&\le D(\rho_{XE}, \rho_U \otimes \rho_E) < \varepsilon, \\
&\sum_{x\in X} \left(P_{XY}(x,x) - \frac{P_Y(x)}{N}\right) \le \sum_{x\in X:\left(P_{XY}(x,x)-\frac{P_Y(x)}{N}\right)>0} \left(P_{XY}(x,x) - \frac{P_Y(x)}{N}\right) \le \\
&\le \sum_{(x,y)\in(X,Y):\left(P_{XY}(x,y)-\frac{P_Y(y)}{N}\right)>0} \left(P_{XY}(x,y) - \frac{P_Y(y)}{N}\right) \le D(\rho_{XE}, \rho_U \otimes \rho_E) < \varepsilon, \\
&\Pr_{key\ guess} = \sum_{x\in X} P_{XY}(x,x) \le \frac{1}{N} + D(\rho_{XE}, \rho_U \otimes \rho_E) < \frac{1}{N} + \varepsilon.
\end{aligned} \quad (33)$$

Отметим, что аналогичная (33) верхняя граница для средней по ключам вероятности угадывания была получена в работе [3], но другим методом. Однако для оценки криптостойкости систем средней вероятности угадывания по всем ключам недостаточно и требуются другие критерии криптостойкости, которые будут рассмотрены ниже.

4.3. Трудоемкость полного перебора без побочной информации о ключе

Выясним теперь, как трудоемкость полного перебора ключей, полученных в результате квантового распределения, связана со следовым расстоянием между классическими распределениями вероятностей и следовым расстоянием, определяющим различимость квантовых состояний. Рассмотрим сначала случай без побочной информации.

В пользу подслушивателя считаем, что он знает распределение вероятностей ключей, но не имеет к ним доступа и не обладает побочной информацией о ключах. В этом случае удобной характеристикой трудоемкости является работа по угадыванию (перебору) ключей, которая была введена в открытой печати в работе [9].

Зная распределение вероятностей ключей, подслушиватель может упорядочить ключи в порядке убывания вероятностей:

$$P_X(x_1) \ge P_X(x_2) \ge \ldots \ge P_X(x_n).$$

Среднее число шагов перебора — трудоемкость — определяется следующим образом. Опробуется первый наиболее вероятный ключ. Вероятность того, что ключ x_1 был выбран для шифрования, есть $P_X(x_1)$. Номер шага опробования i соответствует первому шагу (формула (34) ниже). Тогда с вероятностью $P_X(x_1)$ ключ будет определен на первом шаге. Если нет совпадения входа и выхода, например, известный открытый текст — шифр-текст, то опробуется второй ключ x_2 (индекс числа шагов $i = 2$ в формуле (34)), и т. д. до нахождения истинного ключа. Математическое ожидание числа шагов по опробованию ключей есть трудоемкость полного перебора. Перебирая все ключи, подслушиватель с вероятностью единица найдет истинный ключ в среднем за $G(X)$ шагов [7]. Таким образом, среднее число шагов до определения ключа записывается как

$$G(X) = \sum_{i=1}^{N} iP_X(x_i). \quad (34)$$

Для равномерного распределения $P_U(x)$ и только для него работа по угадыванию достигает максимума [5, 7, 10]

$$G_U(X) = \sum_{i=1}^{N} iP_U(x_i) = \frac{N+1}{2}. \quad (35)$$

Для $G(X)$ имеет место важная оценка (см. детали в [7]). Формула (34) может быть записана в виде

$$G(X) = \frac{N+1}{2} - \sum_{i=1}^{N} Q_i(X),$$
$$Q_i(X) = \sum_{j=1}^{i} \left(P_X(x_j) - P_U(x_j)\right). \quad (36)$$

Далее, учитывая, что следовое расстояние есть максимум вариационного расстояния (см. формулу (20)), находим

$$||P_X - P_U||_1 = \max_i Q_i(X) = \max_i \sum_{j=1}^{i} \left(P_X(x_j) - \frac{1}{N}\right) =$$
$$= \sum_{j=1, P_X(x_j) \geq P_U(x_j)}^{i} (P_X(x_j) - P_U(x_j)) < \varepsilon. \quad (37)$$

С учетом формул (20), (36), (37) для нижней границы находим

$$\frac{N+1}{2} - N||P_X - P_U||_1 \leq G(X) \leq \frac{N+1}{2} - \frac{N}{2}||P_X - P_U||_1. \quad (38)$$

Средняя трудоемкость (34), (38) дает гарантированную границу для числа шагов перебора подслушивателя до определения истинного ключа. Отметим, что ключ при полном переборе определяется с вероятностью единица, причем среднее число шагов полного перебора не менее нижней границы (38).

Поскольку следовое расстояние не возрастает при взятии частичного следа от квантового состояния ($\rho_X = \mathrm{Tr}_E\{\rho_{XE}\}$), имеем

$$||P_X - P_U||_1 \leq ||\rho_X - \rho_U||_1 \leq ||\rho_{XE} - \rho_U \otimes \rho_E||_1 < \varepsilon, \quad (39)$$

где

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

Тогда минимальное среднее число шагов полного перебора оценивается снизу как

$$G(X) \geq \frac{N+1}{2} - N||\rho_{XE} - \rho_U \otimes \rho_E||_1 > \frac{N(1-2\varepsilon)+1}{2}. \quad (40)$$

Формула (40) определяет связь нижней границы трудоемкости полного перебора без побочной информации со следовым расстоянием в квантовой криптографии, которое дает вероятность различения пары квантовых состояний ρ_{XE} и $\rho_U \otimes \rho_E$. Отметим, что вероятность успеха определения истинного ключа $\pi_0 = 1$.

4.4. Трудоемкость полного перебора при наличии побочной информации о ключе

Рассмотрим трудоемкость полного перебора при наличии побочной информации подслушивателя. Данная ситуация возникает в конце квантового распределения ключей. Легитимные пользователи имеют общий ключ x, а подслушиватель в результате своих финальных измерений над квантовой системой имеет побочную информацию — битовую строку y, коррелированную с истинным ключом x. Корреляции между x и y заключены в совместной и условной функциях распределения вероятностей $P_{XY}(x,y)$ и $P_{X|Y=y}(x)$ (см. также рис. *б*). Фактически случайную величину y можно рассматривать как побочную информацию о ключе x, к которому подслушиватель не имеет доступа. В пользу подслушивателя считаем, что ему известно условное распределение вероятностей $P_{X|Y=y}(x)$ и само распределение $P_X(x)$ и, естественно, распределение побочной случайной величины $P_Y(y)$.

Цель подслушивателя заключается в том, чтобы, имея побочную случайную величину y после квантового распределения ключей, найти истинный ключ x, осуществляя полный перебор. При этом вероятность успеха — нахождения истинного ключа — равна $\pi_0 = 1$.

При заданном y подслушиватель упорядочивает условные вероятности в порядке убывания:

$$P_{X|Y=y}(x_{1(y)}) \geq \geq P_{X|Y=y}(x_{2(y)}) \geq \ldots \geq P_{X|Y=y}(x_{N(y)}), \quad \sum_{i=1}^{N} P_{X|Y=y}(x_{i(y)}) = 1, \quad (41)$$

и опробует ключи $x_{i(y)}$ $(i = 1, 2, \ldots, N)$ до определения истинного ключа. Подчеркнем, что упорядочение условных вероятностей по ключам $x_{i(y)}$ зависит от y, $i(y)$ — порядковый номер упорядочения. При другом значении y' упорядочение (41) по ключам будет другим, т. е. номера $i(y)$ ключей $x_{i(y)}$ зависят от y.

Среднее число шагов перебора при заданном y равно

$$G(X|Y=y) = \sum_{i=1}^{N} iP_{X|Y=y}(x_{i(y)}), \quad (42)$$

а среднее число шагов перебора по всевозможным значениям побочной переменной y, соответственно, равно

$$G(X|Y) = \sum_{y \in Y} P_Y(y) G(X|Y=y). \quad (43)$$

Используя результаты предыдущего раздела (формула (38)), а также [7,8], получаем для средней трудоемкости полного перебора при заданном y:

$$\frac{N+1}{2} - N\left\|P_{X|Y=y} - \frac{1}{N}\right\|_1 \le G(X|Y=y) \le \le \frac{N+1}{2} - \frac{N}{2}\left\|P_{X|Y=y} - \frac{1}{N}\right\|_1, \quad (44)$$

$$\left\|P_{X|Y=y} - \frac{1}{N}\right\|_1 = \frac{1}{2}\sum_{x\in X}\left|P_{X|Y=y}(x) - \frac{1}{N}\right|.$$

Усредняя по y неравенства (44), получаем

$$\frac{N+1}{2} - N\left\|P_{XY} - \frac{P_Y}{N}\right\|_1 \le G(X|Y) \le \le \frac{N+1}{2} - \frac{N}{2}\left\|P_{XY} - \frac{P_Y}{N}\right\|_1, \quad (45)$$

$$\left\|P_{XY} - \frac{P_Y}{N}\right\|_1 = \frac{1}{2}\sum_{y\in Y}P_Y(y)\sum_{x\in X}\left|P_{X|Y=y}(x) - \frac{1}{N}\right| = = \frac{1}{2}\sum_{y\in Y}\sum_{x\in X}\left|P_{XY}(x,y) - \frac{P_Y(y)}{N}\right|,$$

где $P_{XY}(x,y) = P_{X|Y=y}(x)P_Y(y)$ — совместное распределение вероятностей.

Окончательно находим

$$G(X|Y) \ge \frac{N+1}{2} - N||\rho_{XE} - \rho_U\otimes\rho_E||_1 > > \frac{N(1-2\varepsilon)+1}{2}. \quad (46)$$

Как следует из (46), нижняя граница средней трудоемкости полного перебора ключей при наличии побочной информации также определяется следовым расстоянием (12), определяющим меру различимости пары квантовых состояний ρ_{XE} и $\rho_U\otimes\rho_E$. Вероятность успеха определения истинного ключа в этом случае равна $\pi_0 = 1$.

4.5. Дополнительные неравенства для трудоемкости полного перебора при наличии побочной информации о ключе

В предыдущем разделе верхняя и нижняя границы полного перебора выражались через следовое расстояние между классическими распределениями вероятности. Приведем еще одно неравенство, основанное на соответствии между распределениями вероятности. Согласно [11] имеем

$$\frac{1}{(1+\log_2 N)^\rho}\sum_{y\in Y}P_Y(y)\times \times\left[\sum_{x\in X}P_{X|Y=y}(x)^{1/(1+\rho)}\right]^{1+\rho} \le G(X|Y) \le \le \sum_{y\in Y}P_Y(y)\left[\sum_{x\in X}P_{X|Y=y}(x)^{1/(1+\rho)}\right]^{1+\rho}. \quad (47)$$

Когда параметр $\rho = 1$, тогда верхняя и нижняя границы превращаются в

$$\frac{1}{1+\log_2 N}N\sum_{y\in Y}P_Y(y)\left[F\left(P_{X|Y=y},\frac{1}{N}\right)\right]^2 \le \le G(X|Y) \le N\sum_{y\in Y}P_Y(y)\left[F\left(P_{X|Y=y},\frac{1}{N}\right)\right]^2, \quad (48)$$

где

$$F\left(P_{X|Y=y},\frac{1}{N}\right) = \sum_{x\in X}\sqrt{\frac{P_{X|Y=y}(x)}{N}}. \quad (49)$$

С учетом того, что

$$1 - \sqrt{F\left(P_{X|Y=y},\frac{1}{N}\right)} \le D\left(P_{X|Y=y},\frac{1}{N}\right) \le \le \sqrt{1 - F\left(P_{X|Y=y},\frac{1}{N}\right)}, \quad (50)$$

получаем для трудоемкости полного перебора:

$$\frac{1}{1+\log_2 N}N\sum_{y\in Y}P_Y(y)\left(1 - D\left(P_{X|Y=y},\frac{1}{N}\right)\right) \le \le G(X|Y) \le N\sum_{y\in Y}P_Y(y)\times \times\left(1 + D\left(P_{X|Y=y},\frac{1}{N}\right)\right). \quad (51)$$

Поскольку

$$D\left(P_{XY},\frac{P_Y}{N}\right) = \sum_{y\in Y}P_Y(y)D\left(P_{X|Y=y},\frac{1}{N}\right), \quad (52)$$

окончательно получаем

$$\frac{1}{1+\log_2 N}N\left(1 - D\left(P_{XY},\frac{P_Y}{N}\right)\right) \le G(X|Y) \le \le N\left(1 + D\left(P_{XY},\frac{P_Y}{N}\right)\right). \quad (53)$$

Из сравнения с границами трудоемкости предыдущего раздела (46) видно, что данные неравенства

являются менее плотными. Учитывая (12), для нижней границы получаем

$$G(X|Y) \geq \frac{1}{1+\log_2 N} N\,(1-\|\rho_{XE}-\rho_U\otimes\rho_E\|_1) \geq \\ \geq \frac{1}{1+\log_2 N}\,N(1-\varepsilon). \quad (54)$$

В данном случае границы трудоемкости полного перебора также выражаются через следовое расстояние между квантовыми состояниями. Отметим, что нижняя граница для трудоемкости в предыдущем разделе (формулы (45), (46)) является более плотной — более точной.

4.6. Трудоемкость частичного перебора без побочной информации о ключе при заданной вероятности успеха

Важной характеристикой трудоемкости является число опробуемых ключей до первого дешифрованного сообщения (см. детали в работе [5]). Пусть каждое сообщение шифруется своим ключом, полученным в результате квантового распределения ключей. Пусть опробуются только M первых наиболее вероятных ключей. Вероятность того, что ключи лежат в опробуемом множестве M есть

$$\pi(M) = \sum_{i=1}^{M} P_X(x_i), \\ P_X(x_1) \geq P_X(x_2) \geq \ldots \geq P_X(x_N), \\ 1 \leq M \leq N. \quad (55)$$

Ключ определяется, если он попадает в переборное множество. Вероятность определения ключа на $(k+1)$-м шаге ($(k+1)$-м сообщении) подчиняется геометрическому распределению

$$P_K(k) = (1-\pi(M))^k \pi(M), \quad \sum_{k=0}^{\infty} P_K(k) = 1. \quad (56)$$

Среднее число сообщений до первого определения ключа — дешифрования сообщения — равно

$$\mathbf{E}(k) = \sum_{k=0}^{\infty} k P_K(k) = \frac{1-\pi(M)}{\pi(M)}. \quad (57)$$

Усредненная по полному количеству шифр-сообщений трудоемкость — число опробуемых ключей — дается следующей формулой [5]:

$$G(X,M) = \sum_{k=0}^{\infty} G(X,M,k) P_K(k) = \\ = \sum_{k=0}^{\infty} \left(k\ M + \sum_{m=1}^{M} m \frac{P_X(x_m)}{\pi(M)} \right) P_K(k) = \\ = \frac{(1-\pi(M))M}{\pi(M)} + \sum_{m=1}^{M} m \frac{P_X(x_m)}{\pi(M)} = \\ = \frac{\left(1 - \sum\limits_{m=1}^{M} P_X(x_m)\right) M + \sum\limits_{m=1}^{M} m P_X(x_m)}{\sum\limits_{m=1}^{M} P_X(x_m)}. \quad (58)$$

Интерпретация данной формулы достаточно прозрачна. Первое слагаемое в сумме дает число шагов перебора, если истинный ключ в k испытаниях нигде не попал в опробуемое множество M. Второе слагаемое отвечает за число шагов частичного перебора, если ключ на $(k+1)$-м шаге попал в переборное множество первых M наиболее вероятных ключей. При этом распределение вероятностей ключей уже в переборном множестве имеет вид $P_X(x_m)/\pi(M)$. Данная трудоемкость имеет комбинированный характер. Когда $M = N$, т. е. полный перебор на каждом шаге, тогда величина (58) совпадает с работой по угадыванию при полном переборе — ключ определяется на каждом сообщении с вероятностью успеха, равной единице, $\pi_0 = 1$.

Рассмотрим трудоемкость частичного перебора, когда задана вероятность успеха π_0 [5]. Точнее говоря, перебор осуществляется только по множеству наиболее вероятных первых ключей, для которых $\{M : \pi(M) > \pi_0\}$. Полагаем

$$Q(X,\pi_0) = \min_{M:\pi(M)>\pi_0} G(X,M). \quad (59)$$

Для удобства введем обозначение

$$\delta = \left\| P_X - \frac{1}{N} \right\|_1 = \frac{1}{2} \sum_{m=1}^{N} \left| P_X(x_m) - \frac{1}{N} \right|. \quad (60)$$

Отметим здесь, что величина δ неизвестна из квантовой криптографии, известно лишь, что $\delta \leq \varepsilon$.

Сделаем оценку $\pi(M)$; используя (55), находим

$$\pi(M) = \sum_{m=1}^{M} P_X(x_m) = \\ = \frac{M}{N} + \sum_{m=1}^{M} \left(P_X(x_m) - \frac{1}{N} \right). \quad (61)$$

С учетом (55), (60), (61) получаем

$$\frac{M}{N} - 2\delta \leq \pi(M) \leq \frac{M}{N} + 2\delta. \quad (62)$$

Согласно (61), (62), имеют место включения

$$\{M:\pi(M)\geq\pi_0\}\subseteq\left\{M:\frac{M}{N}+2\delta\geq\pi_0\right\}=$$
$$=\left\{M:\frac{M}{N}\geq\pi_0-2\delta\right\}. \quad (63)$$

При условии $\pi_0-2\delta>0$ в указанной области имеет место неравенство

$$\frac{N}{M}\leq\frac{1}{\pi_0-2\delta}.$$

Далее получаем следующую цепочку неравенств:

$$\frac{1}{\pi(M)}\geq\frac{1}{\frac{M}{N}+2\delta}=\frac{1}{\frac{M}{N}\left(1+2\delta\frac{N}{M}\right)}\geq$$
$$\geq\frac{1}{\frac{M}{N}\left(1+2\delta(\pi_0-2\delta)^{-1}\right)}\geq\left(1-\frac{2\delta}{\pi_0}\right)\frac{N}{M}. \quad (64)$$

Далее

$$(1-\pi(M))M\geq\left(1-\frac{M}{N}-2\delta\right)M. \quad (65)$$

Оценка второго слагаемого в (58) дает

$$\sum_{m=1}^{M}mP_X(x_m)=\sum_{m=1}^{M}m\left(\frac{1}{N}+P_X(x_m)-\frac{1}{N}\right)=$$
$$=\frac{M(M+1)}{2N}+\sum_{m=1}^{M}m\left(P_X(x_m)-\frac{1}{N}\right)\geq$$
$$\geq\frac{M(M+1)}{2N}-\sum_{m=1}^{M}m\left|P_X(x_m)-\frac{1}{N}\right|\geq$$
$$\geq\frac{M(M+1)}{2N}-2\delta M. \quad (66)$$

Учитывая неравенства (63)–(65), получаем

$$\frac{(1-\pi(M))M+\sum\limits_{m=1}^{M}mP_X(x_m)}{\pi(M)}\geq\left(1-\frac{2\delta}{\pi_0}\right)\times$$
$$\times\frac{N}{M}\left(\left(1-\frac{M}{N}-2\delta\right)M+\frac{M(M+1)}{2N}-2\delta M\right)\geq$$
$$\geq\left(1-\frac{2\delta}{\pi_0}\right)\left(\frac{2N-M-8N\delta+1}{2}\right). \quad (67)$$

Окончательно для нижней границы трудоемкости частичного перебора имеем

$$Q(X,\pi_0)=\min_{\{M:\pi(M)\geq\pi_0\}}G(X,M)\geq$$
$$\geq\min_{\left\{M:\frac{M}{N}\geq\pi_0-2\delta\right\}}G(X,M)=$$
$$=\min_{\left\{M:\frac{M}{N}\geq\pi_0-2\delta\right\}}\frac{(1-\pi(M))M+\sum\limits_{m=1}^{M}P_X(x_m)}{\pi(M)}\geq$$
$$\geq\min_{\left\{M:\frac{M}{N}\geq\pi_0-2\delta\right\}}\left(1-\frac{2\delta}{\pi_0}\right)\left(\frac{2N-M-8\delta N+1}{2}\right)\geq$$
$$\geq\left(1-\frac{2\delta}{\pi_0}\right)\left(\frac{N(1-8\delta)+1}{2}\right)>$$
$$>\left(1-\frac{2\varepsilon}{\pi_0}\right)\left(\frac{N(1-8\varepsilon)+1}{2}\right), \quad (68)$$

где учтено, что $\delta\leq||\rho_{XE}-\rho_U\otimes\rho_E||_1<\varepsilon$.

Как видно из (68), трудоемкость в рассмотренном случае также выражается через следовое расстояние (12), отвечающее за различимость пары квантовых состояний ρ_{XE} и $\rho_U\otimes\rho_E$. В пределе $\varepsilon\to0$ (и $\pi_0=1$) формула (68) переходит в формулу для случая полного перебора (38). Отметим, что нижняя граница в (39) является более плотной $\left(\frac{N(1-2\varepsilon)+1}{2}\right)$, чем (68) $\left((1-2\varepsilon)\frac{N(1-8\varepsilon)+1}{2}\right)$. Данный факт связан с тем обстоятельством, что при выводе (38) неравенство для следового расстояния (12) используется однократно, а при выводе (68) — несколько раз (см. (64)–(67)).

4.7. Трудоемкость частичного перебора при наличии побочной информации о ключе при заданной вероятности успеха

Рассмотрим следующую ситуацию. Каждое сообщение шифруется на своем ключе x_i, который генерируется в соответствии с распределением $P_X(x)$. Подслушиватель не имеет доступа к ключам, но имеет побочную информацию о ключе — случайную величину (битовую строку) y_i $(i=1,2,\ldots,N)$, коррелированную с данным ключом. Например, величина y_i получена в результате подслушивания при квантовом распределении ключей при измерениях над квантовой системой (10) ρ_E^x, коррелированной с данным ключом. Пусть исходное множество ключей каким-то образом упорядочено, например, в лексикографическом порядке.

Подслушиватель, имея побочную информацию y_i, для каждого шифр-сообщения опробует $1\leq M\leq N$ первых наиболее вероятных ключей. Пусть в пользу подслушивателя ему известны сами распределения вероятностей $P_{XY}(x,y)$, $P_{X|Y=y}(x)$, $P_Y(y)$.

Подслушиватель при данном y_i упорядочивает первые M ключей в порядке убывания условных вероятностей. Кроме того, задается вероятность успеха π_0 (см. ниже). Пусть упорядочение условных вероятностей при заданном y_i есть

$$P_{X|Y=y_i}(x_{1(y_i)}) \geq \\ \geq P_{X|Y=y_i}(x_{2(y_i)}) \geq \ldots \geq P_{X|Y=y_i}(x_{M(y_i)}). \quad (69)$$

Номера исходных ключей $m(y_i)$ при упорядочивании вероятностей зависят от y_i — $x_{m(y_i)}$ (где $1(y_i)$, $2(y_i), \ldots, N(y_i)$ является перестановкой номеров исходных ключей). Задача состоит в вычислении среднего числа опробований до первого удачного вскрытия шифра — определения истинного ключа. Опробуются первые M ключей для первого сообщения, если ключ найден, то процесс завершен (успех). Если ключ после M опробований не найден, ожидается второе сообщение, и т. д. до определения истинного ключа.

Пусть последовательность побочной переменной у подслушивателя в серии испытаний имеет вид

$$\mathbf{y} = (y_1, y_2, \ldots, y_i, \ldots). \quad (70)$$

Здесь индекс i нумерует сообщения, этот же индекс нумерует побочную переменную — битовую строку y_i, полученную вместе с i-м сообщением. Пусть соответствующая последовательность переборных множеств первых M наиболее вероятных ключей, привязанных к каждому y_1, $y_2, \ldots, y_N$, есть

$$\mathbf{K} = (\mathcal{K}_1, \mathcal{K}_2, \ldots, \mathcal{K}_i, \ldots). \quad (71)$$

Здесь каждое множество $\mathcal{K}_i$ зависит от значения y_i:

$$\mathcal{K}_i = \left\{x_{1(y_i)}, x_{2(y_i)}, \ldots, x_{M(y_i)}\right\}.$$

Условная вероятность последовательности длины j до первого определения ключа равна

$$P(j|Y=y) = \pi(M, y_{j+1}) \prod_{i=0}^{j} (1 - \pi(M, y_i)), \\ \pi(M, y_i) = \sum_{\{x_{m(y_i)} \in \mathcal{K}_i\}} P_{X|Y=y_i}(x_{m(y_i)}). \quad (72)$$

Напомним еще раз, что последовательность переборных множеств и упорядочение условных вероятностей в них на каждом шаге определяется значением побочной переменной y_i на данном шаге. Имеем

$$\mathcal{K}_i = \{x_{m(y_i)} : P_{X|Y=y_i}(x_{1(y_i)}) \geq \\ \geq P_{X|Y=y_i}(x_{2(y_i)}) \geq \ldots \geq P_{X|Y=y_i}(x_{M(y_i)}); \\ m(y_i) = 1, \ldots, M\}, \quad (73)$$

т. е. упорядочение в $\mathcal{K}_i$ зависит однозначно от побочной переменной y_i. Другими словами, расстановка индексов $m(y_i)$ и условных вероятностей в множестве X задается побочной переменной y_i.

Средняя трудоемкость по всем побочным переменным, которые при разных j независимы, в соответствии с (58)

$$G(M, X|Y) = \mathbf{E}\left(G(M, X|\mathbf{y})\right) = \\ = \mathbf{E}\left(M \sum_{j=0}^{\infty} \left(j\pi(M, y_{j+1}) \prod_{i=0}^{j} (1 - \pi(M, y_i))\right) + \right. \\ + \sum_{j=0}^{\infty} \sum_{m=1}^{M} \left(m \frac{P_{X|Y=y_{j+1}}(x_{m(y_{j+1})})}{\pi(M, y_{j+1})} \pi(M, y_{j+1}) \times \right. \\ \left.\left. \times \prod_{i=0}^{j} (1 - \pi(M, y_i))\right)\right) = \\ = \mathbf{E}\left(M \sum_{j=0}^{\infty} \left(j\pi(M, y_{j+1}) \prod_{i=0}^{j} (1 - \pi(M, y_i))\right) + \right. \\ + \sum_{j=0}^{\infty} \sum_{m=1}^{M} \left(m P_{X|Y=y_{j+1}}(x_{m(y_{j+1})}) \times \right. \\ \left.\left. \times \prod_{i=0}^{j} (1 - \pi(M, y_i))\right)\right) = \\ = M \sum_{j=0}^{\infty} \left(j\mathbf{E}\left(\pi(M, y_{j+1})\right) \prod_{i=0}^{j} (1 - \mathbf{E}\left(\pi(M, y_i)\right))\right) + \\ + \sum_{j=0}^{\infty} \sum_{m=1}^{M} \left(m\mathbf{E}\left(P_{X|Y=y_{j+1}}(x_{m(y_{j+1})})\right) \times \right. \\ \left. \times \prod_{i=0}^{j} (1 - \mathbf{E}(\pi(M, y_i)))\right), \quad (74)$$

где $\mathbf{E}(\ldots)$ — среднее по всем независимым реализациям y_i,

$$\mathbf{E}(\ldots) = \sum_{y_1 \in Y} P_Y(y_1) \times \\ \times \sum_{y_2 \in Y} P_Y(y_2) \ldots \sum_{y_i \in Y} P_Y(y_i) \ldots (\ldots). \quad (75)$$

Индекс $m(y_j)$ определяет шаг опробования ключей и принимает следующее значение при фиксированном y_j:

$$\{m(y_j) = 1(y_j), 2(y_j), \ldots, M(y_j)\}.$$

Данная запись символизирует тот факт, что при данном y_j осуществляется перестановка ключей таким образом, что для первого ключа $x_{1(y_j)}$ условная

вероятность максимальна. Для второго $x_{2(y_j)}$ соответственно

$$P_{X|Y=y_j}(x_{1(y_j)}) \geq P_{X|Y=y_j}(x_{2(y_j)})$$

и т. д.

Вычислим средние в формуле (74); с учетом (75) имеем

$$\pi(M) = \mathbf{E}\left(\pi(M, y_j)\right) = \\ = \sum_{y_J \in Y} P_Y(y_j) \sum_{x_m(y_j) \in \mathcal{K}_j} P_{X|Y=y_j}(x_{m(y_j)}). \quad (76)$$

Далее

$$\sum_{m=1}^{M} m\mathbf{E}\left(P_{X|Y=y_j}(x_{m(y_j)})\right) = \\ = \sum_{m=1}^{M} m \sum_{y_j \in Y} P_Y(y_j) P_{X|Y=y_j}(x_{m(y_j)}). \quad (77)$$

4.7.1. Прямое вычисление средних

Введем обозначение

$$p(m) = \sum_{y_i \in Y} P_Y(y_i) P_{X|Y=y_i}(x_{m(y_i)}),$$

$$\pi(M) = \sum_{m=1}^{M} p(m) = \\ = \sum_{m=1}^{M} \sum_{y_i \in Y} P_Y(y_i) P_{X|Y=y_i}(x_{m(y_i)}), \quad (78)$$

вероятность $p(m)$ зависит только от номера шага m опробования ключей. С учетом (78) для среднего в (74) находим

$$\sum_{m=1}^{M} m \sum_{y_i \in Y} P_Y(y_i) P_{X|Y=y_i}(x_{m(y_i)}) = \\ = \sum_{m=1}^{M} mp(m). \quad (79)$$

Формально перестановка сумм является законной, но требует пояснений. Если бы не было упорядочения условных вероятностей (78), которое зависит от y_i, то перестановка сумм в (78) была бы самоочевидной. Для демонстрации законности перестановки порядка суммирования в (78) выпишем явно выражения с переставленным порядком суммирования и без него (ниже m — индекс опробования). Находим

$$\pi(M) = \sum_{m=1}^{M} p(m) = \\ = \sum_{m=1}^{M} \sum_{y_i \in Y} P_Y(y_i) P_{X|Y=y_i}(x_{m(y_i)}) = \\ (m=1) \quad = \big(P_Y(y_1)P_{X|Y=y_1}(x_{1(y_1)}) + P_Y(y_2) \times \\ \times P_{X|Y=y_2}(x_{1(y_2)}) + \ldots + P_Y(y_2)P_{X|Y=y_N}(x_{1(y_N)})\big) + \\ (m=2) \quad + \big(P_Y(y_1)P_{X|Y=y_1}(x_{2(y_1)}) + P_Y(y_2) \times \\ \times P_{X|Y=y_2}(x_{2(y_2)}) + \ldots + P_Y(y_2)P_{X|Y=y_N}(x_{2(y_N)})\big) + \\ \ldots + \\ (m=M) \quad + \big(P_Y(y_1)P_{X|Y=y_1}(x_{M(y_1)}) + P_Y(y_2) \times \\ \times P_{X|Y=y_2}(x_{M(y_2)}) + \ldots + P_Y(y_2) \times \\ \times P_{X|Y=y_N}(x_{M(y_N)})\big). \quad (80)$$

Вычисление $\pi(M)$ по формуле (78) с переставленными суммами дает

$$\pi(M) = \sum_{y_i \in Y} P_Y(y_i)\pi(M, y_i) = \\ = \sum_{y_i \in Y} P_Y(y_i) \sum_{x_{m(y_i)} \in \mathcal{K}_i} P_{X|Y=y_i}(x_{m(y_i)}) = \\ (y=y_1) \quad = \big(P_Y(y_1)P_{X|Y=y_1}(x_{1(y_1)}) + P_Y(y_1) \times \\ \times P_{X|Y=y_1}(x_{2(y_1)}) + \ldots + P_Y(y_1)P_{X|Y=y_1}(x_{M(y_1)})\big) + \\ (y=y_2) \quad + \big(P_Y(y_2)P_{X|Y=y_2}(x_{1(y_2)}) + P_Y(y_2) \times \\ \times P_{X|Y=y_2}(x_{2(y_2)}) + \ldots + P_Y(y_2)P_{X|Y=y_2}(x_{M(y_2)})\big) + \\ \ldots + \\ (y=y_N) \quad + \big(P_Y(y_N)P_{X|Y=y_N}(x_{1(y_N)}) + P_Y(y_N) \times \\ \times P_{X|Y=y_N}(x_{2(y_N)}) + \ldots + P_Y(y_N) \times \\ \times P_{X|Y=y_N}(x_{M(y_N)})\big). \quad (81)$$

Из сравнения формул (80) и (81) следует равенство сумм после изменения порядка суммирования в (74). Аналогично проверяется равенство (77). Кроме того, из (79) следует, что

$$\sum_{m=1}^{N} p(m) = 1, \quad (82)$$

т. е. $p(m)$ — распределение вероятностей.

С учетом (78), (79), (82) получаем

$$G(M, X|Y) = \frac{(1-\pi(M))M}{\pi(M)} + \sum_{m=1}^{M} m\frac{p(m)}{\pi(M)} = \\ = \frac{\left(1 - \sum\limits_{m=1}^{M} p(m)\right) M + \sum\limits_{m=1}^{M} mp(m)}{\sum\limits_{m=1}^{M} p(m)}. \quad (83)$$

Остается оценить фигурирующие в (83) величины через следовое расстояние, находим

$$\frac{1}{2}\sum_{m=1}^{N}\left|p(m)-\frac{1}{N}\right| =$$

$$=\frac{1}{2}\sum_{m=1}^{N}\left|\sum_{y\in Y}P_Y(y)P_{X|Y=y}(x_{m(y)})-\frac{1}{N}\right| =$$

$$=\frac{1}{2}\sum_{m=1}^{N}\left|\sum_{y\in Y}P_{XY}(x_{m(y)},y)-\frac{1}{N}\right| \le$$

$$\le D\left(P_{XY},\frac{P_Y}{N}\right)\le ||\rho_{XE}-\rho_U\otimes\rho_E||_1<\varepsilon. \quad (84)$$

Суммы после второго и третьего знаков равенства совпадают, поскольку результаты суммирования по всему множеству $x\in X$ и $x_{m(y)}\in X$ совпадают, так как $x_{m(y)}$ есть перестановка битовых строк в одном и том же множестве X.

С учетом оценок, приведенных выше, фактически приходим к задаче, рассмотренной в предыдущем разделе (см. формулу (68)), в итоге получаем

$$Q(X|Y,\pi_0)=\min_{\{M:\pi(M)\ge\pi_0\}}G(X|Y,M)\ge$$

$$\ge\left(1-\frac{2\varepsilon}{\pi_0}\right)\frac{N(1-8\varepsilon)+1}{2}. \quad (85)$$

Таким образом, трудоемкость частичного перебора при наличии побочной информации (85) также выражается через следовое расстояние (12), дающее величину различимости квантовых состояний.

4.7.2. Вычисление средних через неравенства

Возможно вычисление средних в (76), (77) при использовании следового расстояния на более раннем этапе, что приводит к тем же результатам. Для цельности картины приведем эти оценки средних. Для вычисления средних в (76), (77) потребуются оценки для величин, входящих в эти выражения; находим

$$\pi(M)=\sum_{y\in Y}P_Y(y)\pi(M,y)=$$

$$=\sum_{y\in Y}P_Y(y)\left(\sum_{x\in\mathcal{K}_y}P_{X|Y=y}(x)\right)=$$

$$=\sum_{y\in Y}P_Y(y)\left(\frac{M}{N}+\sum_{x\in\mathcal{K}_y}\left(P_{X|Y=y}(x)-\frac{1}{N}\right)\right)\le$$

$$\le\frac{M}{N}+\sum_{y\in Y}P_Y(y)\sum_{x\in\mathcal{K}_y}\left|P_{X|Y=y}(x)-\frac{1}{N}\right|\le$$

$$\le\frac{M}{N}+\sum_{y\in Y}P_Y(y)\sum_{x\in X}\left|P_{X|Y=y}(x)-\frac{1}{N}\right|=$$

$$=\frac{M}{N}+D\left(P_{XY},\frac{P_Y}{N}\right)\le\frac{M}{N}+2\varepsilon. \quad (86)$$

Было учтено, что

$$D(P_{XY},\frac{P_Y}{N})=\sum_{y\in Y}P_Y(y)\sum_{x\in X}\left|P_{X|Y=y}(x)-\frac{1}{N}\right|=$$

$$=\sum_{y\in Y}\sum_{x\in X}\left|P_{XYy}(x,y)-\frac{P_Y(y)}{N}\right|<\varepsilon. \quad (87)$$

Для оценки нижней границы аналогично (86) получаем

$$\pi(M)=\sum_{y\in Y}P_Y(y)\pi(M,y)=$$

$$=\sum_{y\in Y}P_Y(y)\left(\sum_{x\in\mathcal{K}_y}P_{X|Y=y}(x)\right)=$$

$$=\sum_{y\in Y}P_Y(y)\left(\frac{M}{N}+\sum_{x\in\mathcal{K}_y}\left(P_{X|Y=y}(x)-\frac{1}{N}\right)\right)\ge$$

$$\ge\frac{M}{N}-\sum_{y\in Y}P_Y(y)\sum_{x\in\mathcal{K}_y}\left|P_{X|Y=y}(x)-\frac{1}{N}\right|\ge$$

$$\ge\frac{M}{N}-\sum_{y\in Y}P_Y(y)\sum_{x\in X}\left|P_{X|Y=y}(x)-\frac{1}{N}\right|=$$

$$=\frac{M}{N}-D\left(P_{XY},\frac{P_Y}{N}\right)\ge\frac{M}{N}-2\varepsilon. \quad (88)$$

Оценка (77) дает

$$\sum_{y\in Y} P_Y(y)\left(\sum_{x\in\mathcal{K}_y} mP_{X|Y=y}(x_m)\right) = \frac{M(M+1)}{2N} +$$
$$+\sum_{y\in Y} P_Y(y)\left(\sum_{x\in\mathcal{K}_y} m\left(P_{X|Y=y}(x_m)-\frac{1}{N}\right)\right) \geq$$
$$\geq \frac{M(M+1)}{2N} - \sum_{y\in Y} P_Y(y)\times$$
$$\times\left(\sum_{x\in\mathcal{K}_y} m\left|P_{X|Y=y}(x_m)-\frac{1}{N}\right|\right) \geq$$
$$\geq \frac{M(M+1)}{2N} - M\sum_{y\in Y} P_Y(y)\times$$
$$\times\sum_{x_m\in X}\left|P_{X|Y=y}(x_m)-\frac{1}{N}\right| \geq \frac{M(M+1)}{2N}-2M\varepsilon. \quad (89)$$

С учетом оценок в (80)–(89) фактически приходим к задаче, рассмотренной в предыдущем разделе, и в итоге получаем формулу (85).

5. НЕКОТОРЫЕ ПРИМЕРЫ

Малость следового расстояния — ε-близость реальной ситуации после квантового распределения ключей к идеальной — означает ε-близость трудоемкости к максимальному значению $\max G(X|Y) = (N+1)/2$. Это утверждение работает и в обратную сторону. Поскольку верхняя и нижняя границы для трудоемкости полного перебора (45) являются плотными по величине ε, близость $G(X|Y)$ к максимальному значению $\max G(X|Y) = (N+1)/2$ означает ε-близость расстояния между идеальной и реальной ситуациями — ε-различимость квантовых состояний ρ_{XE} и $\rho_U\otimes\rho_E$.

Кроме того, ε-малость следового расстояния означает, что распределение самих ключей $P_X(x)$ ε-близко к равновероятному распределению $P_X(x) = 1/N$, и они лишь ε-коррелированы с побочной переменной y.

Уточним, что понимается под малостью параметра ε. Рассмотрим сложность перебора без побочной информации для распределения вероятностей ключей вида

$$P_X(x_1) = \frac{1}{2}, \quad P_X(x_i) = \frac{1}{2(N-1)}, \quad 1 < i \leq N. \quad (90)$$

Трудоемкость перебора приблизительно равна

$$G(X) \approx \frac{N}{4} \quad (91)$$

вместо максимального значения $G(x) \approx N/2$. Такое уклонение следует считать большим, так как изменение трудоемкости $\Delta(G(X)) = G(X)/2$ равно половине значения самой величины $\max G(X)$. При этом следовое расстояние между данным распределением и идеальным распределением ключей

$$\left\|P_X - \frac{1}{N}\right\|_1 \approx 1, \quad (92)$$

т. е. не является малым. При таком распределении ключей каждое второе сообщение будет дешифровано. Малость ε гарантирует близость трудоемкости перебора к максимальной, приблизительно равной $N/2$, и наоборот — близость трудоемкости к $N/2$ гарантирует малость следового расстояния. Аналогичная ситуация имеет место и для трудоемкости при наличии побочной информации.

Интересно обсудить масштабы величин. Среднее число опробований до первого нахождения ключа — дешифрования сообщений, когда на каждом шаге опробуется M первых наиболее вероятных ключей, не менее (см. (62))

$$\frac{1-\pi(M)}{\pi(M)} > \frac{N}{M+N\varepsilon}. \quad (93)$$

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 256 бит. Поэтому размер полного ключевого пространства $N = 2^{256} \approx \approx 1.5\cdot 10^{77}$ (напомним, что число атомов в видимой части Вселенной оценивается как 10^{77}). Число шагов перебора даже при $M = 2^{128} \approx 10^{38}$ является запредельно большим. Величина ε, которую можно реально достичь в системах квантовой криптографии на сегодня, имеет порядок $\varepsilon = 2^{-32} \approx 2.5\cdot 10^{-10}$. Поэтому $N\varepsilon \gg M$, в этом случае среднее число шагов опробования ключей до первого определения ключа — до первого сообщения, которое, возможно, будет дешифровано, приблизительно равно

$$\frac{1}{\varepsilon} \approx 10^{10}, \quad (94)$$

т. е., грубо говоря, из 10 миллиардов сообщений в среднем, возможно, будет прочитано одно сообщение.

На данные оценки можно взглянуть под другим углом. Пусть криптосистема производит сообщения длиной 256 бит каждую секунду, каждое сообщение шифруется в режиме одноразового блокнота ε-секретным ключом длиной 256 бит. За 100 лет система произведет приблизительно $3\cdot 10^9$ сообщений.

Пусть имеется идеальный критерий читаемости дешифрованного сообщения. Для каждого сообщения осуществляется частичный перебор по M первым наиболее вероятным ключам. Тогда примерно через 100 лет, возможно, будет дешифровано (прочитано) одно сообщение.

При опробовании $M \to N$ ключей (перебираются почти все ключи для каждого сообщения) среднее число сообщений до первого прочитанного ≈ 1, но при этом среднее число опробований ключей приблизительно равно

$$\frac{N(1-\varepsilon)}{2} \approx \frac{N}{2}.$$

При таких соотношениях параметров число шагов фактически не зависит от M, поэтому если опробуется только первый наиболее вероятный ключ, то число шагов до первого прочитанного сообщения не меняется: $1/\varepsilon \approx 10^{10}$.

6. ЗАКЛЮЧЕНИЕ

Главный вывод из приведенного выше рассмотрения состоит в том, что следовое расстояние, которое дает степень различимости пары квантовых состояний, отвечающих реальной и идеальной ситуациям, является адекватной и достаточной характеристикой, которая позволяет найти нижние границы трудоемкости (сложности) перебора ключей в различных ситуациях их использования.

Выражаем благодарность А. Н. Климову, С. П. Кулику за многочисленные и интенсивные дискуссии, а также коллегам по Академии криптографии Российской Федерации за обсуждения и постоянную поддержку.

Работа выполнена при поддержке РНФ (грант № 16-12-00015).

ЛИТЕРАТУРА

1. 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].

2. R. Renner, PhD Thesis, ETH Zürich, December (2005).

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

4. C. E. Shannon, Bell Systems Techn. J. **28**, 656 (1948).

5. И. М. Арбеков, Матем. вопр. криптогр. **7**(1), 39 (2016).

6. M. M. Wilde, arXiv:1106.1445 [quant-ph].

7. J. O. Pliam, PhD Thesis, Minnesota Univ., 1999.

8. С. Н. Молотков, ЖЭТФ **150**, 903 (2016).

9. J. L. Massey, IEEE Int. Symp. Inf. Theory, 204 (1994).

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

11. E. Arikan, IEEE Trans. Inf. Theory **42**, 99 (1996).