ЖЭТФ, 2018, том 154, вып. 4 (10), стр. 738–750 

# О КОНКАТЕНАЦИИ КЛЮЧЕЙ В КВАНТОВОЙ КРИПТОГРАФИИ: КАК КВАНТОВАЯ ЗАПУТАННОСТЬ «ДОТЯГИВАЕТСЯ» ДО КЛАССИЧЕСКИХ УСТРОЙСТВ

***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 26 апреля 2018 г.

Квантовая механика допускает коллективные измерения, связанные с проекцией на запутанные состояния и позволяющие извлечь больше классической информации из ансамбля квантовых состояний по сравнению с индивидуальными измерениями. В связи с этим возникает принципиальный вопрос для секретности ключей в квантовой криптографии. Должен ли критерий секретности формулироваться с учетом всех ключей, распределенных как в прошлых, так и в будущих сеансах квантового распределения ключей (КРК), или достаточно гарантировать секретность ключей только в отдельном сеансе КРК? Исследованию этого вопроса посвящена данная работа.

**DOI:** 10.1134/S004445101810005X

## 1. ВВЕДЕНИЕ

Явление квантовой запутанности, в отличие от суперпозиции, не имеет классического аналога. Запутанные квантовые состояния являются информационным ресурсом и возникают в различных задачах передачи и обработки информации [1]. Вопрос о запутанных состояниях возник в работе Шредингера [2] (известный пример с кошкой (Katze) Шредингера). В работе Эйнштейна – Подольского – Розена [3] (известный ЭПР-парадокс) был поставлен вопрос о полноте квантовой механики и возможности описания квантового явления запутанности на языке теорий со скрытыми параметрами. Разрешение ЭПР-парадокса было дано в работах Белла [4], где постановка вопроса о полноте квантовой теории и скрытых параметрах была математически формализована и доведена до экспериментально проверяемых неравенств (знаменитые неравенства Белла). Впоследствии, начиная с работы Аспекта [5], данные неравенства были неоднократно проверены экспериментально. Было показано, что правильным описанием запутанных состояний является квантовомеханическое описание, и теории со скрытыми параметрами не дают адекватного описания экспериментальной ситуации, которая проявляется в нарушении неравенств Белла.

Намного позднее было осознано, что квантовая запутанность может быть использована для решения вполне практических задач, например, секретного распределения криптографических ключей — протокол квантовой криптографии Экерта [6]. Явление квантовой телепортации — перенос неизвестного состояния с одной квантовой системы на другую при помощи ЭПР-пары и классических сообщений — также использует квантовую запутанность [7]. Сверхплотное кодирование, которое позволяет передавать два бита классической информации, манипулируя только одной частицей в ЭПР-паре [8], также не имеет классических аналогов. Работа квантовых повторителей, использующая переброс запутанности (entanglement swapping), также основана на запутанных состояниях [9]. Эффективность квантовых алгоритмов для ряда вычислительно слож-

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

ных задач для классического компьютера достигается за счет запутанных состояний [9].

Верхняя граница для классической информации, которую можно извлечь из ансамбля квантовых состояний — фундаментальная граница Холево [1] — достигается на коллективных измерениях. Неформально говоря, она достигается на измерениях, связанных с проекцией на запутанные состояния, при этом не обязательно ортогональные. Коллективные измерения с использованием запутанных состояний позволяют извлечь больше классической информации из квантового ансамбля состояний, чем индивидуальные измерения [1], даже если квантовые состояния в отдельных актах генерируются источником независимо. Сжатие квантовых состояний (кодирование Шумахера [10]) также использует проекции последовательностей независимых квантовых состояний на запутанные состояния.

Энтропийные соотношения неопределенностей для составных квантовых систем имеют фундаментальное значение в квантовой криптографии [11,12]. Нижняя граница энтропийных соотношений неопределенностей для составных систем также достигается на запутанных состояниях. Применительно к квантовой информатике энтропийные соотношения неопределенностей имеют более фундаментальное значение, чем стандартные соотношения неопределенностей Гейзенберга – Робертсона [13,14], поскольку определяют величину «перекачки» информации между подсистемами — в квантовой криптографии между легитимными пользователями и подслушивателем [11].

Целью квантовой криптографии является распределение секретных ключей по доступным для прослушивания квантовым каналам связи. Секретность ключей, полученных в результате квантового распределения ключей (КРК), гарантируется фундаментальными законами квантовой механики. Оптимальные атаки на квантовое распределение ключей включают в себя коллективные измерения — проекции на запутанные состояния [1]. Оптимальность для подслушивателя понимается в смысле максимума извлечения информации из передаваемых квантовых состояний при минимуме их возмущения.

## 2. НЕФОРМАЛЬНАЯ ПОСТАНОВКА ЗАДАЧИ

Неформально вопрос, на который собираемся получить ответ в работе, звучит следующим образом. Пусть проведено несколько независимых сеансов квантового распределения ключей. В результате каждого сеанса получается свой секретный ключ. Далее с ключами возможны различные манипуляции, например, отдельные ключи или их части конкатенируются (объединяются) в единый ключ. При этом возникает вопрос: достаточно ли секретности ключей в каждом отдельном сеансе, чтобы гарантировать секретность производных ключей, в том числе и составных? Этот вопрос связан с тем, что подслушиватель после каждого сеанса может хранить в квантовой памяти систему, коррелированную с ключами, а затем делать коллективные измерения сразу над всей квантовой памятью для разных сеансов, что даст ему больше информации о составном ключе, чем измерения в каждом отдельном сеансе.

Рассмотрим отдельный сеанс квантового распределения ключей. Наиболее общая атака подслушивателя на передаваемые квантовые состояния состоит в использовании своего вспомогательного квантового состояния (ancilla). Во время передачи квантовых состояний в каждой независимой посылке подслушиватель приводит во взаимодействие свое состояние и передаваемое состояние. В результате возникает запутанное состояние. Искаженное информационное состояние подслушиватель направляет на приемную сторону, а свое вспомогательное искаженное состояние сохраняет в квантовой памяти. Из-за запутанности информационного состояния и вспомогательного состояния подслушивателя измерения на приемной стороне над искаженным информационным состоянием приводят к корреляции результатов измерений на приемной стороне и квантовым состоянием подслушивателя. Иначе говоря, состояние в квантовой памяти подслушивателя определяется исходом измерений на приемной стороне. Оказывается, что наилучшая стратегия подслушивателя состоит в том, чтобы не измерять сразу свое квантовое состояние в памяти, а дождаться последней стадии протокола. Только после того как легитимные пользователи согласуют базисы, проведут коррекцию ошибок в первичных ключах, проведут сжатие (усиление секретности) очищенных ключей, можно проводить коллективные измерения.

Для каждой посылки в квантовой памяти подслушивателя находится квантовое состояние. В итоге имеется регистр независимых квантовых состояний, над которыми в конце проводится коллективное измерение, — неформально, проекция на запутанные состояния. Именно на таких коллективных измерениях достигается фундаментальная граница Холево [1], дающая верхнюю границу классической

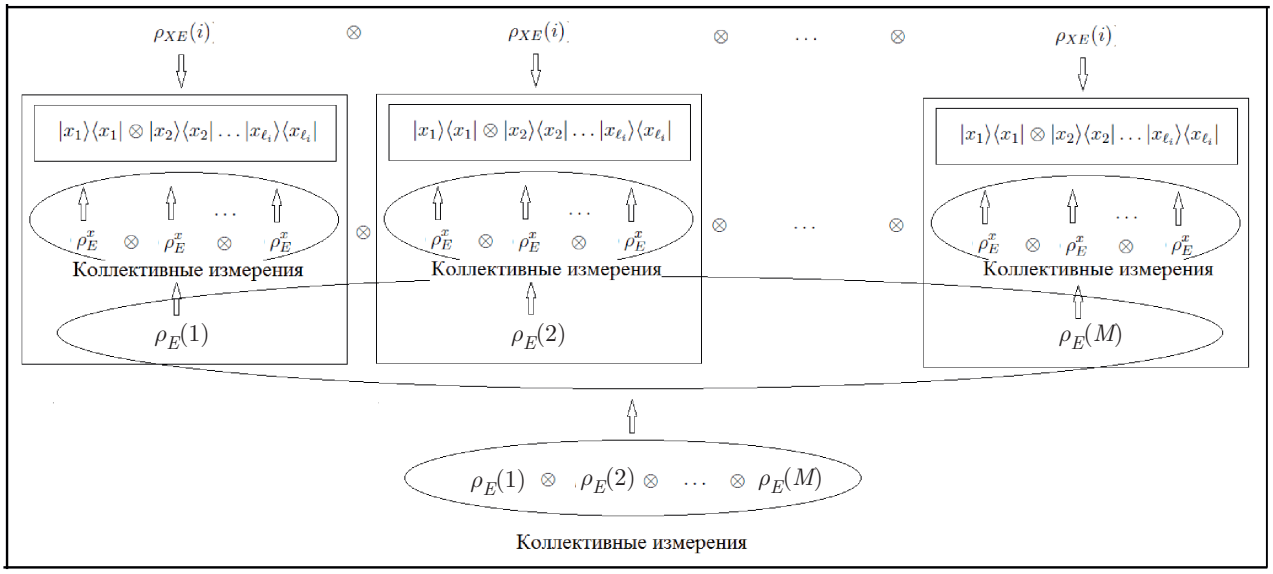


Иллюстрация коллективных измерений подслушивателя в каждом сеансе КРК и коллективных измерений после всех сеансов КРК

информации, которую можно получить из ансамбля независимых квантовых состояний, в данном случае — из регистра квантовой памяти. Это связано со свойством супераддитивности квантовой информации — коллективные измерения над состояниями сразу из всех посылок дают больше классической информации (большее число битов), чем сумма информаций, полученных при индивидуальных измерениях над квантовыми состояниями в каждой отдельной посылке. Данное явление также не имеет классического аналога, поскольку запутанность отсутствует в классической области.

В конце сеанса КРК легитимные пользователи имеют одинаковую битовую строку — общий секретный ключ. У подслушивателя после коллективных измерений возникает битовая строка («слепок ключа») коррелированная с ключом легитимных пользователей (более точные формулировки см. ниже). Такая ситуация имеет место для одного сеанса КРК. Ситуация поясняется на рисунке.

Рассмотрим теперь ситуацию с несколькими независимыми сеансами КРК. Подслушиватель после каждого сеанса в самом общем случае имеет в своей квантовой памяти квантовые системы, каждая из которых коррелирована с ключом легитимных пользователей в отдельном независимом сеансе. Однако никто не обязывает подслушивателя делать коллективные измерения над своей квантовой памятью после каждого сеанса КРК (см. рисунок), чтобы получить битовую строку («слепок ключа») после каждого сеанса. Подслушиватель может сохранять в квантовой памяти состояния после всех независимых сеансов КРК и делать коллективные измерения над квантовой памятью сразу после всех сеансов. При этом подслушиватель получит больше классической информации, чем при индивидуальных измерениях внутри каждого сеанса (см. рисунок). Это означает, что битовая строка подслушивателя после всех сеансов — составной «слепок всех ключей» легитимных пользователей — будет сильнее коррелирована с ключами легитимных пользователей. В результате ключи легитимных пользователей могут оказаться менее секретными (уточнение формулировок будет дано ниже). Таким образом, квантовая запутанность через коллективные измерения «дотягивается» до классических систем — классической битовой строки — секретного ключа (см. рисунок).

Далее, ключи, полученные в различных независимых сеансах, используются для различных целей. Ключи могут комбинироваться, конкатенироваться — из более коротких ключей получаться составные ключи, ключи могут расширяться — из одного ключа преобразованиями получаются производные ключи и т. д. Принципиальный и вполне прагматический вопрос можно сформулировать следующим образом. Достаточно ли критерия секретности для одного сеанса, чтобы гарантировать секретность ключей, полученных в различных независимых сеансах? Или необходим критерий секретности

на все сеансы, т. е. нужно помнить, в каких сеансах и какие ключи были получены? В последнем случае было бы практически невозможно хранить всю историю ключей.

## 3. ФОРМАЛИЗАЦИЯ ПОСТАНОВКИ ЗАДАЧИ

Уточним теперь на формальном уровне постановку задачи. После финальной стадии КРК — процедуры усиления секретности — легитимные пользователи (Алиса и Боб) в $i$-м сеансе имеют одинаковый секретный ключ $x \in X = \{0,1\}^{n_i}$ длиной $n_i$, а подслушиватель (Ева) имеет квантовую систему $E$. Данная ситуация описывается матрицей плотности $\rho_{XE}(i)$. Под словами «секретный ключ» понимается секретность по определенному критерию. Одним из принятых критериев секретности является критерий, основанный на следовом расстоянии. По определению ключ является $\varepsilon$-секретным [15], если

$$||\rho_{XE}(i) - \rho_U(i) \otimes \rho_E(i)||_1 \leq \varepsilon, \tag{1}$$

$$\rho_U(i) = \frac{1}{2^{n_i}} \times \\ \times \sum_{x_1,x_2,\ldots,x_{n_i}=0,1} |x_1\rangle\langle x_1| \otimes |x_2\rangle\langle x_2| \ldots |x_{n_i}\rangle\langle x_{n_i}|,$$

$$\rho_E(i) = \mathrm{Tr}_X\{\rho_{XE}(i)\},$$

где $||\rho||_1 = 1/2\,\mathrm{Tr}\{|\rho|\}$, $\rho_E(i)$ — матрица плотности квантовой системы Евы после сжатия очищенных ключей в $i$-м сеансе, $\rho_U(i)$ — матрица плотности, отвечающая идеальным случайным равнораспределенным ключам, $\rho_{XE}(i)$ — матрица плотности в $i$-м сеансе, описывающая корреляции между общим ключом легитимных пользователей и квантовой системой Евы, хранящейся в квантовой памяти. Стандартная интерпретация критерия секретности (1), основанного на следовом расстоянии, сводится к следующему [16, 17]. Реальная ситуация после квантового распределения ключей дается матрицей плотности $\rho_{XE}(i)$. Идеальная ситуация, когда ключи случайные и равнораспределенные и квантовая система подслушивателя некоррелирована с ключами легитимных пользователей, описывается матрицей плотности $\rho_U(i) \otimes \rho_E(i)$. Значок тензорного произведения означает полную независимость (полное отсутствие корреляций) между квантовой системой Евы и ключами Алисы и Боба.

Неравенство (1) дает расстояние между двумя ситуациями (квантовыми состояниями): реальной и идеальной. Никакие ключи в критерии (1) явно не фигурируют. Величина $\varepsilon$ интерпретируется как превышение вероятности различения двух ситуаций над вероятностью простого угадывания.

Под независимостью сеансов КРК понимается следующее. Легитимные пользователи передают серию квантовых состояний, проводят измерения на приемной стороне, определяют уровень ошибок, исправляют их, сжимают очищенный ключ до длины $n_i$ в $i$-м сеансе. Длина исходной передаваемой серии определяется таким образом, чтобы после сжатия обеспечить нужный уровень секретности, требуемую величину $\varepsilon$. В результате возникает матрица плотности $\rho_{XE}(i)$ (соответственно, $\rho_U(i)$ и $\rho_E(i)$) и т. д. Пусть для простоты все $M$ серий проводятся в одинаковых условиях, хотя это не принципиально. В итоге возникает квантовое состояние, описывающее реальную ситуацию после $M$ серий, $\rho_{XE}(M) = \rho_{XE}^{\otimes M}(i)$, аналогично состояние, отвечающее идеальной ситуации,

$$\rho_U(M) \otimes \rho_E(M) = \rho_U^{\otimes M}(i) \otimes \rho_E^{\otimes M}(i).$$

Теперь расстояние между ситуациями после всех сеансов дается следовым расстоянием:

$$||\rho_{XE}(M) - \rho_U(M) \otimes \rho_E(M)||_1 = \\ = ||\rho_{XE}^{\otimes M} - \rho_U^{\otimes M} \otimes \rho_E^{\otimes M}||_1 < M\varepsilon.$$

Неизвестна лучшая оценка, хотя и не слишком плотная, чем оценка, основанная на субаддитивности следового расстояния, т. е. фактически на неравенстве треугольника. При такой оценке ситуация оказывается $M\varepsilon$-секретной, если каждый сеанс был $\varepsilon$-секретен.

Если отдельный сеанс в смысле критерия секретности (1) является $\varepsilon$-секретным, то после $M$ сеансов ситуация оказывается уже лишь $M\varepsilon$-секретной.

Если ключи из различных сеансов конкатенируются, то формально можно обеспечить любой заданный уровень секретности, выбирая $\varepsilon$ в каждом сеансе таким образом, чтобы суммарное $\varepsilon$ имело нужную величину.

Например, решение работы [16] было следующим. Для обеспечения заранее заданного уровня секретности $\varepsilon$ для составного ключа при большом (возможно даже бесконечном) числе сеансов нужно, чтобы для каждого последующего сеанса генерировался более длинный очищенный ключ. Этот ключ сжимается до ключа заданной длины, для которого параметр секретности имеет меньшее значение, чем $\varepsilon$. Рост длины очищенного ключа с номером сеанса оказывается линейным (разд. 2.4 в [16]).

Поскольку ключей генерируется большое количество, фактически нужно помнить все предыдущие сеансы и знать количество будущих сеансов, что неприемлемо.

Как будет показано ниже, данная ситуация возникает из-за того, что критерий секретности (1) не относится напрямую к ключам, а относится к вероятности различения двух ситуаций. Было бы более естественно формулировать критерий секретности, в котором ключи фигурируют явно. Одним из таких критериев является средняя вероятность угадывания по ключам легитимных пользователей. Вообще говоря, два данных критерия разные, но, как будет показано ниже, оба критерия выражаются через величину $\varepsilon$.

## 4. ДВА КРИТЕРИЯ СЕКРЕТНОСТИ

Ниже рассмотрим два критерия секретности ключей, затем установим связь между ними.

### 4.1. Различимость реальной и идеальной ситуаций как критерий секретности КРК: критерий 1)

Рассмотрим критерий 1), основанный на различимости двух ситуаций. Идеальная ситуация дается матрицей плотности, когда ключ $x$ (ему отвечает матрица плотности идеально равнораспределенных ключей $\rho_U$) некоррелирован с квантовой системой подслушивателя $\rho_E$. Реальная ситуация после распределения ключей дается матрицей плотности $\rho_{XE}$. Квантовое состояние для идеальной ситуации $\rho_U \otimes \rho_E$.

Критерий секретности дается в абстрактных терминах — малости расстояния между двумя ситуациями (квантовыми состояниями). Критерий секретности 1) [15, 16] гласит

$$D(\rho_{XE}, \rho_U \otimes \rho_E) = ||\rho_{XE} - \rho_U \otimes \rho_E||_1 < \varepsilon. \qquad (2)$$

При этом часто произносятся слова, что ключи, полученные в таком протоколе, являются $\varepsilon$-секретными, что может приводить к путанице. Правильнее говорить, что реальная ситуация после протокола $\varepsilon$-секретна. Параметр секретности $\varepsilon$ выбирается легитимными пользователями «административно». Данное значение $\varepsilon$ достигается сжатием очищенных ключей до финального ключа $x$ нужной длины. Очищенные ключи возникают после передачи квантовых состояний, измерений над ними и исправления ошибок в исходной битовой последовательности. Чем меньше $\varepsilon$, тем большей длины нужен очищенный ключ, соответственно, большее число исходно переданных квантовых состояний.

За критерием (2) стоит вероятность различения двух квантовых состояний. Мерой различимости двух ситуаций (квантовых состояний) является следовое расстояние. Пусть для различения равновероятно предъявляются квантовые состояния $\rho$ и $\sigma$. Измерения должны наилучшим образом различать две ситуации ($\rho$ и $\sigma$), поэтому результат измерения должен содержать два исхода. Неважно, как их нумеровать, например 0 и 1. При наступлении исхода 0 считается, что было состояние $\rho$, при наступлении исхода 1 считается, что было состояние $\sigma$. Какова максимальная вероятность успешного различения ($\Pr_{Guess}(\rho, \sigma)$) по всевозможным измерениям? Известно, что максимальная вероятность успеха (различения) выражается через следовое расстояние (см., например, [17, 18]). Любое измерение в квантовой механике дается разложением единицы. Разложение единицы представляет собой формальное описание измерительного прибора. Пусть $I$ — единичный оператор в пространстве состояний, где действуют матрицы плотности двух квантовых состояний $\rho$ и $\sigma$. Для измерения с двумя исходами 0 и 1 имеем

$$I = \mathcal{M}_0 + \mathcal{M}_1, \qquad (3)$$

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

$$\Pr(0|\rho) = \mathrm{Tr}\{\mathcal{M}_0\rho\}. \qquad (4)$$

Формула (4) дает условную вероятность того, что было предъявлено состояние $\rho$ и результат измерения был 0. Аналогично, условная вероятность правильной интерпретации состояния $\sigma$ есть

$$\Pr(1|\sigma) = \mathrm{Tr}\{\mathcal{M}_1\sigma\}. \qquad (5)$$

С учетом равновероятного предъявления состояний и, принимая во внимание, что $\mathrm{Tr}\{\rho\} = \mathrm{Tr}\{\sigma\} = 1$, находим для максимальной вероятности правильного различения состояний (ситуаций):

$$\Pr_{success} = \max_{0\le\mathcal{M}_0\le I}\left(\frac{1}{2}\,\mathrm{Tr}\{\mathcal{M}_0\rho\}+\frac{1}{2}\,\mathrm{Tr}\{\mathcal{M}_1\sigma\}\right) = \\ = \frac{1}{2}\left(1+\max_{0\le\mathcal{M}_0\le I}\mathrm{Tr}\{\mathcal{M}_0(\rho-\sigma)\}\right). \qquad (6)$$

Известно, что следовое расстояние есть максимум по всем измерениям (см., например, [18]):

$$\max_{0\le\mathcal{M}_0\le I} \mathrm{Tr}\{\mathcal{M}_0(\rho-\sigma)\} = D(\rho,\sigma). \quad (7)$$

Для вероятности успешного различения одного из двух состояний с учетом (4)–(7) получаем

$$\mathrm{Pr}_{success} = \frac{1}{2}(1 + D(\rho,\sigma)). \quad (8)$$

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

В контексте квантовой криптографии под матрицами плотности $\rho$ и $\sigma$ следует понимать матрицы $\rho_{XE}$ и $\rho_U \otimes \rho_E$.

Сеанс КРК считается $\varepsilon$-секретным (соответственно, ключ считается $\varepsilon$-секретным) [15], если гарантируется, что следовое расстояние между двумя ситуациями (квантовыми состояниями) после сеанса КРК не более $\varepsilon$:

$$D(\rho_{XE}, \rho_U \otimes \rho_E) = ||\rho_{XE} - \rho_U \otimes \rho_E||_1 = \\ = \frac{1}{2}\,\mathrm{Tr}\{|\rho_{XE} - \rho_U \otimes \rho_E|\} < \varepsilon. \quad (9)$$

При этом подразумевается, может и неявно, что подслушиватель будет делать измерение с двумя исходами. Из (8) следует, что $\rho_{XE}$ и $\rho_U \otimes \rho_E$, описывающие реальную и идеальную ситуации, различимы с вероятностью успеха, превышающей вероятность простого угадывания не более, чем на $\varepsilon/2$,

$$\mathrm{Pr}_{Guess}(\rho_{XE}, \rho_U \otimes \rho_E) = \\ = \frac{1}{2} + \frac{1}{2}||\rho_{XE} - \rho_U \otimes \rho_E||_1 < \frac{1}{2}(1+\varepsilon). \quad (10)$$

Если было проведено $M$ независимых сеансов распределения ключей и в каждом был получен $\varepsilon$-секретный ключ, то после конкатенации всех ключей в единый составной ключ составной ключ по критерию (1) будет уже только $M\varepsilon$-секретным, поскольку вероятность различения двух ситуаций $\rho_{XE}^{\otimes M}$ и $\rho_U^{\otimes M} \otimes \rho_E{}^{\otimes M}$ будет

$$\mathrm{Pr}_{Guess}(\rho_{XE}^{\otimes M}, \rho_U^{\otimes M} \otimes \rho_E^{\otimes M}) = \\ = \frac{1}{2} + \frac{1}{2}||\rho_{XE}^{\otimes M} - \rho_U^{\otimes M} \otimes \rho_E^{\otimes M}||_1 < \frac{1}{2}(1 + M\varepsilon), \quad (11)$$

т. е. с точки зрения подслушивателя реальная и идеальная ситуации становятся более различимыми — далекими друг от друга. Превышение над вероятностью простого угадывания теперь $M\varepsilon/2$.

### 4.2. Критерий секретности, основанный непосредственно на вероятности угадывания ключей: критерий 2)

Предыдущий критерий дается в абстрактных терминах различения двух ситуаций, и ключи в нем явно никак не фигурируют.

Для формулировки критерия 2) требуется уточнить ситуацию после КРК. После сеанса КРК можно выделить следующие стадии.

В результате сеанса КРК у легитимных пользователей возникает общий ключ — битовая строка $x \in \{0,1\}^n$ длиной $n$. Подслушиватель имеет в своем распоряжении квантовую систему, коррелированную с этим ключом, которую подслушиватель сохраняет в квантовой памяти. У подслушивателя еще нет никакой битовой строки, коррелированной с истинным ключом, а имеется квантовая система $\rho_E$ [15–17].

Далее, подслушиватель после окончания сеанса КРК может либо сразу делать измерения над своей квантовой системой $\rho_E$, либо сохранять ее в квантовой памяти до следующих сеансов, а только затем делать коллективные измерения сразу над всеми системами в квантовой памяти.

Если подслушиватель делает измерения после окончания каждого сеанса, то в результате получается конкретная для данного сеанса КРК битовая строка $y \in Y = \{0,1\}^n$, коррелированная с истинным ключом $x$. На данной стадии возникает совместное классическое распределение вероятностей $P_{XY}(x,y)$. Рассмотрим величину $\sum_{x\in X} P_{XY}(x,x)$, которую можно интерпретировать как среднюю вероятность угадывания по всем ключам.

Критерий секретности 2) может быть сформулирован в виде

$$\sum_{x\in X} P_{XY}(x,x) < \delta, \quad (12)$$

где $\delta$ — параметр секретности, который задается «руками» и отличен от $\varepsilon$ и с которым он, из общих соображений, связан некоторой функциональной зависимостью. Связь параметров секретности для критериев 1) и 2) будет дана ниже.

Важно подчеркнуть следующее. В рамках критерия 1) слова о различимости двух ситуаций — реальной и идеальной — с операциональной точки зрения подразумевают измерение с двумя исходами. Вероятность одного исхода относится к успеху — правильному различению ситуаций (состояний), вероятность второго исхода — к ошибке различения.

В критерии 2) фигурирует средняя вероятность угадывания по всем ключам. С операциональной

точки зрения для определения ключей после сеанса подслушиватель должен делать другие измерения, чем в критерии 1). Такие измерения имеют $2^n$ исходов ($n$ — длина битовой строки Алисы и Боба). В каждом исходе с вероятностью $P_Y(y)$ возникает $y$ — «слепок» истинного ключа $x$.

Для того чтобы более явно и наглядно проиллюстрировать разницу между измерениями в критерии 1) и критерии 2), рассмотрим простой пример.

Рассмотрим для простоты ситуацию, когда в результате КРК получен один $\varepsilon$-секретный бит по критерию 1). Матрица плотности, описывающая реальную ситуацию, имеет вид

$$\rho_{XE}=\frac{1}{2}|0\rangle\langle 0|\otimes\rho_E^0+\frac{1}{2}|1\rangle\langle 1|\otimes\rho_E^1. \qquad (13)$$

Для того чтобы не загромождать выкладки, считаем, что 0 и 1 появляются у легитимных пользователей равновероятно, хотя для анализа это не принципиально. Соответственно, для $\rho_U$ и $\rho_E$ имеем

$$\rho_U=\frac{1}{2}|0\rangle\langle 0+\frac{1}{2}|1\rangle\langle 1|,\quad \rho_E=\frac{1}{2}\rho_E^0+\frac{1}{2}\rho_E^1. \qquad (14)$$

Теперь рассмотрим критерий 2). Цель подслушивателя — наилучшим образом отличить не матрицы плотности $\rho_{XE}$ и $\rho_U\otimes\rho_E$, а сам ключ, в данном примере 0 или 1, т. е. наилучшим образом отличить матрицы плотности $\rho_E^0$ и $\rho_E^1$, которые коррелированы со значениями ключа 0 и 1. С точки зрения подслушивателя, ему предъявляется равновероятно одно из состояний в квантовой памяти — $\rho_E^0$ или $\rho_E^1$. Максимальная вероятность различения данных состояний, соответственно значений битов ключа 0 или 1, равна

$$\Pr_{Guess}(\rho_E^0,\rho_E^1)=\frac{1}{2}+\frac{1}{2}||\rho_E^0-\rho_E^1||_1, \qquad (15)$$

$$||\rho_E^0-\rho_E^1||_1=\frac{1}{2}\operatorname{Tr}\{|\rho_E^0-\rho_E^1|\}=$$
$$=\frac{1}{2}\operatorname{Tr}\left\{\sqrt{(\rho_E^0-\rho_E^1)^+(\rho_E^0-\rho_E^1)}\right\}.$$

Хотя вероятность угадывания в критерии 2) и выражается через следовое расстояние, но это расстояние между другими матрицами плотности по отношению к критерию 1).

Если бы состояния $\rho_E^0$ и $\rho_E^1$ или, по-крайней мере, следовое расстояние между ними было известно, то задачу можно было бы считать решенной. Однако ни сами состояния, ни следовое расстояние между ними после сеанса КРК явно неизвестны. Максимумы вероятности угадывания ситуаций $\Pr_{Guess}(\rho_{XE},\rho_U\otimes\rho_E)$ и вероятности угадывания непосредственно битов ключа $\Pr_{Guess}(\rho_E^0,\rho_E^1)$ достигаются на разных измерениях.

Можно, конечно, мажорировать следовое расстояние $||\rho_E^0-\rho_E^1||_1$ через следовое расстояние $||\rho_{XE}-\rho_U\otimes\rho_E||_1$, однако максимумы достигаются на разных измерениях.

Поэтому оценка вероятности $\Pr_{Guess}(\rho_E^0,\rho_E^1)$ через измерения, на которых достигается

$$\max_{Meas}\left\|P_{XY}-\frac{P_Y}{N}\right\|_1=||\rho_{XE}-\rho_U\otimes\rho_E||_1,$$

логически необоснована и может давать любой результат, как завышающий реальную верхнюю границу для $\Pr_{Guess}(\rho_E^0,\rho_E^1)$, так и занижающий ее. Выяснить этот вопрос можно только, построив измерения, которые дают границу для коллективных измерений для всех сеансов.

Максимальная вероятность угадывания одного бита по критерию 2) есть

$$\Pr_{Guess}(\rho_E^0,\rho_E^1)=\frac{1}{2}(1+\delta'),\quad \delta'=||\rho_E^0-\rho_E^1||_1. \qquad (16)$$

Как увидим в следующих разделах, оценка, основанная непосредственно на максимизации средней вероятности угадывания по ключам по критерию 2), дает

$$\Pr_{Guess}(\rho_E^0,\rho_E^1)<e^{-(1-\varepsilon)}. \qquad (17)$$

Заметим, что вероятность различения ситуаций по критерию 1) (см. выше) есть

$$\Pr_{Guess}(\rho_{XE},\rho_U\otimes\rho_E)<\frac{1}{2}(1+\varepsilon). \qquad (18)$$

Уже на данном этапе видна структурная разница критериев 1) и 2). Критерий 2), по сути, сводится к извлечению подслушивателем классической информации из квантового ансамбля

$$\mathcal{E}=\left\{(\rho_E^0,\rho_E^1),\left(P(0)=P(1)=\frac{1}{2}\right)\right\},$$

верхняя граница этой информации дается фундаментальной величиной (информацией) Холево [1]. Ниже будет установлена связь следового расстояния в критерии 1) с критерием 2) и фундаментальной границей Холево.

### 4.3. Связь между критериями 1) и 2)

Тот факт, что в следовом расстоянии в критерии 1) в явном виде ключи не фигурируют, привел к дискуссиям [19]. Поэтому необходимо рассмотреть

другие возможные критерии секретности, которые явно содержат информацию о ключах, например, критерий, который гарантирует малость средней вероятности угадывания по всем ключам (критерий 2)). Поскольку в задаче нет другого параметра кроме $\varepsilon$, любой критерий, по-видимому, должен функционально выражаться через следовое расстояние в критерии 1).

В результате дискуссий появился критерий для средней вероятности угадывания по ключам [17] (см. также [20]), который для одного сеанса выглядит как

$$\sum_{x\in X} P_{XY}(x,x) < \frac{1}{2^n} + \varepsilon. \tag{19}$$

Этот вывод базируется на следующих посылках (см. ниже). Строится измерение с $2^n$ исходами, каждый исход дает битовую строку подслушивателя $y$ длиной $n$. Принципиальный момент (см. ниже), что такие измерения строятся так, чтобы максимизировать следовое расстояние, построенное на классических распределениях вероятностей, возникающих в данных измерениях. Поскольку следовое расстояние между матрицами плотности (ситуациями) является верхней границей, берется такое измерение, на котором достигается равенство

$$\left\| P_{XY} - \frac{P_Y}{N} \right\|_1 = ||\rho_{XE} - \rho_U \otimes \rho_E||_1 < \varepsilon, \qquad N = 2^n. \tag{20}$$

В этом месте возникает логический изъян. Когда есть скрытый логический изъян, он может всплыть в небезобидной форме в дальнейшем. Логический изъян состоит в следующем. По критерию 2) логически правильно максимизировать по всем измерениям с $2^n$ исходами непосредственно величину средней вероятности успешного угадывания подслушивателя по всем ключам,

$$\max_{Meas} \sum_{x\in X} P_{XY}(x,x), \tag{21}$$

а не по измерениям с $2^n$ исходами, которые максимизируют следовое расстояние,

$$\max_{Meas} ||P_{XY} - \frac{P_Y}{N}||_1 = ||\rho_{XE} - \rho_U \otimes \rho_E||_1. \tag{22}$$

При этом измерения, максимизирующие следовое расстояние и среднюю вероятность успешного угадывания по ключам, принципиально разные. Выше на примере одного бита в сеансе была явно показана данная разница.

На первый взгляд, если не подозревать о данном логическом изъяне, можно было бы остановиться на этом месте, рассуждая таким образом. Если вероятность угадывания для одного отдельного сеанса ограничена величиной $1/2^n + \varepsilon$, а сеансы независимы, то вероятность угадывания для $M$ сеансов будет ограничена величиной $(1/2^n + \varepsilon)^M$ и экспоненциально убывать с ростом числа сеансов. Этим можно было бы удовлетвориться, если бы данная оценка была получена как результат максимизации непосредственно средней вероятности угадывания $\max_{Meas} \sum_{x\in X} P_{XY}(x,x)$. Однако данная оценка получена как результат максимизации совсем другой величины — следового расстояния $\max_{Meas} ||P_{XY} - P_Y/N||_1$. Далее, невозможно ответить на вопрос: как изменится оценка, если подслушиватель будет делать коллективные измерения над своими квантовыми системами сразу для всех сеансов, поскольку они позволяют получить большее количество информации, и при этом проводить максимизацию непосредственно самой средней вероятности угадывания по ключам во всех сеансах КРК? Максимизация следового расстояния для классических распределений может как завышать, так и занижать оценку вероятности успеха для угадывания ключей.

На наш взгляд, более правильный подход должен состоять в максимизации непосредственно средней вероятности угадывания по ключам сразу для $M$ сеансов, это позволит сравнить результаты, которые получаются для двух разных критериев секретности.

Существует фундаментальная граница классической информации, извлекаемой из квантового ансамбля, — это граница Холево, которая достигается на коллективных измерениях [1]. Если явно известны квантовые состояния в ансамбле, то величина Холево также может быть явно вычислена. Однако после сеанса квантового распределения ключей квантовые состояния подслушивателя явно не известны. Известно лишь, что следовое расстояние до идеальной ситуации не превышает $\varepsilon$. При этом заранее не очевидно, можно ли связать границу Холево со следовым расстоянием.

## 5. ВЕРОЯТНОСТЬ ОШИБКИ ПРИ ОПРЕДЕЛЕНИИ КЛЮЧЕЙ ПОДСЛУШИВАТЕЛЕМ В ОДНОМ СЕАНСЕ КРК: МАКСИМИЗАЦИЯ ПО КРИТЕРИЮ 1)

В этом разделе покажем, как возникает оценка (19), когда измерения устроены так, что они макси-

мизируют величину следового расстояния для классических распределений:

$$\max_{Meas}\left\|P_{XY}-\frac{P_Y}{N}\right\|_1=||\rho_{XE}-\rho_U\otimes\rho_E||_1<\varepsilon.$$

Удобнее это сделать в общем виде для $n$ битов, а не для одного бита в сеансе, как было дано в примере выше.

Приведем простой и явный вывод вероятности (19). Подслушиватель не имеет прямого доступа к ключам, а имеет в распоряжении квантовую систему, коррелированную с ключом. Побочную информацию о ключе подслушиватель получает в результате измерений над своей квантовой системой. Любое измерение в квантовой механике дается разложением единицы, имеем

$$I_{XE}=\sum_{x\in X}\sum_{y\in Y}\mathcal{F}_{xy},\quad \mathcal{F}_{xy}=|x\rangle\langle x|\otimes\mathcal{M}_y, \qquad (23)$$

где $I_{XE}$ — единичный оператор. Измерение (23) имеет $2^n$ исходов. Результатом измерений является битовая строка $y\in Y=\{0,1\}^n$, коррелированная с ключом. В результате измерений возникает совместное распределение вероятностей $P_{XY}(x,y)$.

Следующая ниже процедура как раз и есть выбор измерений, которые максимизируют следовое расстояние для классических распределений вероятности, вместо прямой максимизации средней вероятности угадывания по ключам $\max_{Meas}\sum_{x\in X}P_{XY}(x,x)$.

Для любого оператора $0\le\Lambda\le I_{XE}$ имеет место [18] соотношение

$$D(\rho_{XE},\rho_U\otimes\rho_E)=\max_{\{0\le\Lambda\le I_{XE}\}}\mathrm{Tr}\{\Lambda(\rho_{XE}-\rho_U\otimes\rho_E)\}. \qquad (24)$$

Выбирая $\Lambda=I_{XE}$ (внутренняя структура $I_{XE}$ отвечает за выбор измерения), получаем

$$\left\|P_{XY}-\frac{P_Y}{N}\right\|_1=\frac{1}{2}\sum_{x\in X}\sum_{y\in Y}\left|P_{XY}(x,y)-\frac{P_Y(y)}{N}\right|=$$
$$=\sum_{(x,y)\in(X,Y):(P_{XY}(x,y)-\frac{P_Y(y)}{N})>0}\left(P_{XY}(x,y)-\frac{P_Y(y)}{N}\right)\le$$
$$\le D(\rho_{XE},\rho_U\otimes\rho_E)<\varepsilon. \qquad (25)$$

Здесь

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

В формуле (25) учтена известная связь следового расстояния с вариационным [21]. Выберем измерение, которое максимизирует вероятность успеха подслушивателя. Найдем эту вероятность с учетом (23)–(25), получаем

$$\mathrm{Pr}_{Guess}=\sum_{x\in X}P_{XY}(x,x)=\mathrm{Tr}\{\Lambda\rho_{XE}\}+$$
$$+\mathrm{Tr}\{\Lambda\rho_U\otimes\rho_E\}=\frac{1}{2^n}+D(\rho_{XE},\rho_U\otimes\rho_E)=$$
$$=\frac{1}{2^n}+\frac{1}{2}\sum_{x\in X}\sum_{y\in Y}\left|P_{XY}(x,y)-\frac{P_Y(y)}{N}\right|<\frac{1}{2^n}+\varepsilon.$$

Верхняя граница для вероятности успеха может быть получена и непосредственно из (25), имеем

$$\sum_{x\in X}\left(P_{XY}(x,x)-\frac{P_Y(x)}{N}\right)\le$$
$$\le\sum_{x\in X:\left(P_{XY}(x,x)-\frac{P_Y(x)}{N}\right)>0}\left(P_{XY}(x,x)-\frac{P_Y(x)}{N}\right)<$$
$$<\varepsilon, \qquad (26)$$

$$\mathrm{Pr}_{Guess}<\frac{1}{2^n}+\varepsilon,\quad \overline{\mathrm{Pr}}_{Guess}=1-\mathrm{Pr}_{Guess}>$$
$$>1-\left(\frac{1}{2^n}+\varepsilon\right). \qquad (27)$$

Такой же результат был получен в работе [17], но другим способом.

Как видно из (27), средняя вероятность угадывания по ключам превосходит вероятность простого угадывания не более, чем на $\varepsilon$. Однако данная оценка получена логически непоследовательным способом — путем максимизации другой величины. Максимизация следового расстояния для классических распределений может привести к любому парадоксальному значению для средней вероятности угадывания по ключам: как большему, так и меньшему значению по сравнению с истинным.

## 6. ЗАПУТАННЫЕ КОЛЛЕКТИВНЫЕ ИЗМЕРЕНИЯ И ГРАНИЦА ХОЛЕВО ДЛЯ $M$ СЕАНСОВ КРК. ПРЯМАЯ МАКСИМИЗАЦИЯ ПО КРИТЕРИЮ 2)

В этом разделе будет получена верхняя граница средней вероятности угадывания по ключам путем прямой максимизации величины $\sum_{x\in X}P_{XY}(x,x)$ по критерию 2) для $M$ сеансов с учетом коллективных

измерений. Данная вероятность определяется величиной Холево, для которой потребуется ее связь со следовым расстоянием, поскольку сами состояния в явном виде неизвестны.

Всего битовых последовательностей существует $2^{Mn}$. Неформально величина Холево $\chi$ говорит о том, что из полного числа последовательностей $2^{Mn}$ можно различить не более $2^{M\chi}$ последовательностей с вероятностью ошибки, стремящейся к нулю. При этом подслушиватель использует коллективные измерения — неформально проекции на запутанные состояния. Если окажется, что величина $\chi \ll n$, то подслушиватель даже при коллективных измерениях сможет различить лишь небольшую часть последовательностей, соответственно, малое число всех составных ключей. Здесь сразу возникает другая проблема. После КРК известна лишь граница для следового расстояния в одном сеансе. Поэтому ответ на вопрос (положительный или отрицательный) сводится к установлению связи между величиной Холево и следовым расстоянием. Знание величины Холево позволит вычислить вероятность ошибки по всем битовым последовательностям по критерию 2).

После $M$ сеансов подслушиватель находится в ситуации квантово-классического канала связи. Классический источник в каждом акте генерирует с вероятностью $P_X(x)$ символ классического алфавита $x \in X = \{0,1\}^n$, которому сопоставляется квантовое состояние $\rho_E^x$, доступное для измерений подслушивателю. Источник используется $M$ раз. Цель подслушивателя, имея в своем распоряжении квантовые состояния, различить максимально возможное число последовательностей классических символов — ключей длиной $Mn$.

Всего имеется $2^{Mn}$ последовательностей, с которыми ассоциированы последовательности квантовых состояний. Каждый ключ возникает с вероятностью $P_X(x)$. Пусть выбрана определенная случайная кодовая таблица. Неформально это означает, что каждой битовой последовательности сопоставлена последовательность квантовых состояний,

$$\hat{x}^l = (x^l_{i_1}, x^l_{i_2}, \ldots, x^l_{i_M}) \to (\rho_E^{x^l_{i_1}}, \rho_E^{x^l_{i_2}}, \ldots, \rho_E^{x^l_{i_M}}).$$

Средняя ошибка различения по всем кодовым словам в данной таблице определяется как

$$\overline{\Pr}_{Guess}(M,l) = 1 - \frac{1}{2^{Mn}} \sum_{j=1}^{2^{Mn}} \mathrm{Tr}\{\rho_{\hat{E}}^{\hat{x}^l} \mathcal{M}_j^l\}, \qquad \hat{x}^l = (x^l_{i_1}, x^l_{i_2}, \ldots, x^l_{i_M}), \tag{28}$$

где измерение дается разложением единицы $I_{\hat{E}} = \sum_{j=1}^{2^{Mn}} \mathcal{M}_j^l$. Средняя ошибка по всем случайным кодовым таблицам, сгенерированным в соответствии с распределением вероятностей $P_X(x)$, есть (см. детали в [22], идея вычисления ошибки восходит к работам Шеннона, Галлагера, Аримото для классических каналов [23, 24], затем идея была перенесена на квантовые каналы)

$$\overline{\Pr}_{Guess}(M) = \mathbf{E}\left(\overline{\Pr}_{Guess}(M,l)\right), \tag{29}$$

$$\mathbf{E}(\ldots) = \sum_{x_{i_1}\in X} \sum_{x_{i_2}\in X} \ldots \sum_{x_{i_M}\in X} P_X(x_{i_1}) \times \times P_X(x_{i_2}) \ldots P_X(x_{i_M})(\ldots),$$

где усреднение проводится по распределению вероятностей $P_X(x)$. Для ошибки может быть получено неравенство — сильное обращением теоремы кодирования (см. детали в [22]):

$$\overline{\Pr}_{Guess}(M) > 1 - \exp\{-M(-sn + E_0(s, P_X))\}, \tag{30}$$

$$E_0(s, P_X) = -\log_2 \left( \mathrm{Tr} \left( \sum_{x\in X} P_X(x) (\rho_E^x)^{1/(s+1)} \right)^{s+1} \right),$$

где параметр $s$ — произвольное число в интервале $-1 < s < 0$. Из (30) следует, что

$$E_0(0, P_X) = 0, \quad \left.\frac{\partial E_0(s, P_X)}{\partial s}\right|_{s=0} = S(\overline{\rho}_E) - \sum_{x\in X} P_X(x) S(\rho_E^x) = \chi(\mathcal{E}), \tag{31}$$

где $S(\rho) = -\mathrm{Tr}\{\rho \log_2(\rho)\}$ — энтропия фон Неймана, $\chi(\mathcal{E})$ — величина Холево для квантового ансамбля $\mathcal{E} = \{P_X(x), \rho_E^x\}$. Для дальнейшего продвижения требуется установить связь между следовым расстоянием и границей Холево $\chi(\mathcal{E})$.

## 7. СЕКРЕТНОСТЬ КЛЮЧЕЙ В СМЫСЛЕ СЛЕДОВОГО РАССТОЯНИЯ ДЛЯ ОДНОГО СЕАНСА КРК ПО КРИТЕРИЮ 1) ГАРАНТИРУЕТ СЕКРЕТНОСТЬ ДЛЯ ЛЮБОГО ЧИСЛА СЕАНСОВ КРК ПО КРИТЕРИЮ 2)

В этом разделе покажем, что критерия секретности в смысле следового расстояния для одного сеанса КРК оказывается достаточно для произвольного числа сеансов КРК. Данный вывод будет следовать из прямой максимизации вероятности угадывания

по критерию 2), поскольку величина Холево ограничивается следовым расстоянием в одном сеансе (критерий 1)). При этом окажется, что критерий 1), основанный на следовом расстоянии, завышает вероятность успешного угадывания по всем ключам. Иначе говоря, критерий 2), основанный на прямой максимизации вероятности угадывания по ключам, дает более плотную оценку, чем критерий 1).

Сначала покажем, что следовое расстояние мажорирует информацию Холево, $\chi(\mathcal{E}) < 2\varepsilon n$. Из этого факта будет следовать, что из полного числа $2^{Mn}$ последовательностей подслушиватель сможет различить не более $2^{Mn2\varepsilon}$ битовых последовательностей, т. е. лишь их экспоненциально малую долю $2^{-Mn(1-2\varepsilon)}$ по длине полной битовой последовательности (составного ключа) для всех $M$ сеансов.

Нам потребуется несколько вспомогательных величин, связанных с асимметричной относительной квантовой энтропией (см. детали в работах [25, 26]). Введем отображение для положительных операторов $\Lambda_\rho(\sigma)$:

$$\Lambda_\rho(\sigma) = \frac{d}{dt}\log_2(\rho+\sigma t)|_{t=0} = \\ = \int\limits_0^\infty ds(\rho+sI)^{-1}\sigma(\rho+sI)^{-1}, \quad \Lambda_\rho(\rho) = I, \quad (32)$$

производная понимается в смысле Фреше. Определим полуторалинейную форму, которая может рассматриваться как метрика:

$$M_\rho(\sigma,\tau) = \mathrm{Tr}\{\sigma\Lambda_\rho(\tau)\}, \quad M_\rho(\sigma,\sigma) \geq 0. \quad (33)$$

Дифференциал от асимметричной относительной энтропии

$$D_\alpha(\rho||\sigma) = \alpha\,\mathrm{Tr}\{\rho\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\rho-\sigma)\} = \\ = -\alpha\frac{d}{d\alpha}S(\rho||\alpha\rho+(1-\alpha)\sigma). \quad (34)$$

Здесь относительная энтропия $S(\rho||\sigma)$ и асимметричная энтропия $S_\alpha(\rho||\sigma)$ [25, 26] соответственно равны

$$S(\rho||\sigma) = \mathrm{Tr}\{\rho(\log_2(\rho)-\log_2(\sigma))\}, \quad (35)$$

$$S_\alpha(\rho||\sigma) = -\frac{1}{\log_2(\alpha)}S(\rho||\alpha\rho+(1-\alpha)\sigma).$$

В отличие от относительной энтропии, асимметричная энтропия является непрерывной и связана с дифференциалом:

$$S_\alpha(\rho||\sigma) = -\frac{1}{\log_2(\alpha)}\times \\ \times \int\limits_0^{-\log_2(\alpha)} D_\alpha(\rho||\sigma)d(-\log_2(\alpha')). \quad (36)$$

С учетом (34)–(36) дифференциальная энтропия ограничивается сверху следовым расстоянием

$$D_\alpha(\rho||\sigma) = \alpha\,\mathrm{Tr}\{\rho\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\rho-\sigma)\} = \\ = \alpha\,\mathrm{Tr}\{(\rho-\sigma)\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\rho)\} \leq \\ \leq \alpha\,\mathrm{Tr}\{(\rho-\sigma)_+\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\rho)\} \leq \\ \leq \alpha\,\mathrm{Tr}\{(\rho-\sigma)_+\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\alpha\rho+(1-\alpha)\sigma)\} = \\ = \mathrm{Tr}\{(\rho-\sigma)_+\} = \delta(\rho,\sigma), \quad (37)$$

где $(\rho-\sigma)_+$ — проекция на подпространство, отвечающая положительным собственным числам.

Выразим величину Холево через относительную энтропию, а относительную энтропию через дифференциальную энтропию, последняя ограничена следовым расстоянием. Величина Холево по определению [1] имеет вид

$$\chi(\mathcal{E}) = S(\overline{\rho}_E) - \sum_{x\in X}P_X(x)S(\rho_E^x), \\ \overline{\rho}_E = \sum_{x\in X}P_X(x)\rho_E^x. \quad (38)$$

Окончательно для величины Холево находим

$$\chi(\mathcal{E}) = \sum_{x\in X}P_X(x)S(\rho_E^x||\overline{\rho}_E) = \\ = -\sum_{x\in X}P_X(x)\log_2(P_X(x))S_{P_X(x)}(\rho_E^x||\overline{\rho}_E^x) \leq \\ \leq -\sum_{x\in X}P_X(x)\log_2(P_X(x))\delta(\rho_E^x,\overline{\rho}_E^x) \leq \\ \leq -\sum_{x\in X}P_X(x)\log_2(P_X(x))\times \\ \times\sum_{x\neq x'\in X}\frac{P_X(x')}{1-P_X(x)}\delta(\rho_E^x,\rho_E^{x'}). \quad (39)$$

Последнее слагаемое в цепочке неравенств (39) мажорируется следовым расстоянием,

$$\frac{1}{2}\sum_{x\neq x'\in X}\frac{P_X(x')}{1-P_X(x)}|\rho_E^x-\rho_E^{x'}|\leq$$
$$\leq\frac{1}{2}\sum_{x\neq x'\in X}\frac{1}{1-P_X(x)}\times$$
$$\times\left(|P_X(x')\rho_E^{x'}-P_X(x)\rho_E^x|+|\rho_E^x(P_X(x')-P_X(x))|\right)\leq$$
$$\leq\frac{1}{2}\sum_{x\in X}\frac{2}{1-P_X(x)}\times$$
$$\times\left(\left|\frac{\overline{\rho}_E}{N}-P_X(x)\rho_E^x\right|+\left|\rho_E^x||P_X(x)-\frac{1}{N}\right|\right). \quad (40)$$

Вычисляя след от (40) и учитывая, что максимальная вероятность не превышает $\max_{x\in X}P_X(x)<$ $<1/N+\varepsilon$, получаем

$$\frac{1}{1-(1/N+\varepsilon)}\times$$
$$\times\left(\sum_{x\in X}\mathrm{Tr}\left\{\left|\frac{\overline{\rho}_E}{N}-P_X(x)\rho_E^x\right|\right\}+\left\|P_X-\frac{1}{N}\right\|_1\right)<$$
$$<\frac{2\varepsilon}{1-2\varepsilon}. \quad (41)$$

В итоге величина Холево ограничена сверху энтропией Шеннона:

$$\chi(\mathcal{E})<H(X)\frac{2\varepsilon}{1-2\varepsilon}\approx 2\varepsilon H(X)<2\varepsilon n,$$
$$H(X)=-\sum_{x\in X}P_X(x)\log_2(P_X(x)). \quad (42)$$

С учетом того, что параметр $0<|s^*|<1$ в (30), (31), для средней вероятности правильного угадывания находим

$$\mathrm{Pr}_{Guess}(M)<e^{-Mn(1-2\varepsilon)}. \quad (43)$$

## 8. ЗАКЛЮЧЕНИЕ

Интерпретируем формулу (43). В идеальном случае, когда ключи строго равномерно распределены и подслушиватель может их только угадывать, вероятность угадывания равна обратной величине размерности ключевого пространства:

$$\mathrm{Pr}_{Guess}(M)=\frac{1}{2^{Mn}}. \quad (44)$$

В реальной ситуации средняя вероятность успеха различения ключей в $M$ сеансах с учетом коллективных измерений имеет аналогичный (43) вид, и можно думать, что вероятности успеха для отдельных сеансов КРК умножаются.

Рассмотрим ситуацию, когда в одном сеансе КРК получен один $\varepsilon$-секретный бит, $M=n=1$. Вероятность угадывания одного бита подслушивателем в результате измерений над квантовой системой, коррелированной с данным битом, не более $\mathrm{Pr}_{Guess}<$ $<e^{-(1-2\varepsilon)}$ и не увеличивается с ростом $M$. При проведении $M$ независимых сеансов КРК вероятность успеха выглядит как произведение вероятностей для отдельных сеансов, но при этом подслушиватель использует коллективные запутанные измерения сразу над всеми квантовыми системами из разных сеансов.

Важно подчеркнуть, что хотя внешне вероятность (43) выглядит как произведение вероятностей,

$$\mathrm{Pr}_{Guess}(M)<e^{-Mn(1-2\varepsilon)}=$$
$$=\underbrace{e^{-n(1-2\varepsilon)}e^{-n(1-2\varepsilon)}\ldots e^{-n(1-2\varepsilon)}}_{M}, \quad (45)$$

данный результат не может быть получен перемножением вероятностей, вычисленных для отдельных сеансов КРК, поскольку подслушиватель использует коллективные измерения.

Обычно число сеансов КРК $M\gg n$. Для отношения вероятности успеха при подсчете по формуле (27) к вероятности успеха с учетом коллективных измерений (45) имеем

$$\frac{(1/2^n+\varepsilon)^M}{e^{-Mn(1-2\varepsilon)}}>1. \quad (46)$$

Из (46) следует, что оценка типа (27) по сравнению с правильным ответом (45) является существенно завышенной. Максимизация вероятности угадывания по критерию 1) оказывается больше истинного значения (которое нужно знать и уметь вычислять, чтобы было с чем сравнивать), и является лишь результатом везения. Поэтому без ущерба для криптостойкости ключи из разных сеансов можно конкатенировать в единый ключ.

Оценка по критерию 1) могла бы получиться и заниженной по сравнению с вероятностью при прямой максимизации по критерию 2). В этом случае использование оценки по критерию 1) было бы катастрофическим для секретности ключей.

Таким образом, если ключ, полученный в одном сеансе КРК является $\varepsilon$-секретным, то он является таковым и для произвольного числа сеансов КРК.

Однако этот вывод логически не следует из максимизации по критерию 1), а возникает как результат прямой максимизации средней вероятности угадывания по ключам, а не максимизации следового расстояния для классических распределений вероятностей.

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

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

## ЛИТЕРАТУРА

**1**. A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973); А. С. Холево, УМН **53**, 193 (1998); *Введение в квантовую теорию информации*, сер. *Современная математическая физика*, вып. 5, МЦНМО, Москва (2002); А. С. Холево, *Квантовые системы, каналы, информация*, МЦНМО, Москва (2010).

**2**. E. Schrödinger, Naturwissenschaften **23**(48), 807 (1935).

**3**. A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

**4**. J. S. Bell, Physics (Amer. Phys. Soc.) **1**, 195 (1964).

**5**. A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **49**, 91 (1982).

**6**. A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

**7**. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

**8**. C. H. Bennett and S. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

**9**. M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).

**10**. B. Schumacher, Phys. Rev. A **51**, 2738 (1995).

**11**. M. Tomamichel, Ch. Ci Wen Lim, N. Gisin, and R. Renner, Nature Commun. **3**, 1 (2012); arXiv: quant-ph:1103.4130 v2.

**12**. M. Tomamichel and A. Leverrier, arXiv:quant-ph: 1506.08458 V2.

**13**. W. Heisenberg, Z. Physik **43**, 172 (1927).

**14**. H. P. Robertson, Phys. Rev. **34**, 163 (1929).

**15**. R. Renner, PhD Thesis, ETH Zürich, Dec. (2005); arXiv:quant-ph:0512258.

**16**. J. Müller-Quade and R. Renner, arXiv:quant-ph: 1006.2215.

**17**. C. Portmann and R. Renner, arXiv:quant-ph:1409. 3525.

**18**. M. M. Wilde, arXiv:quant-ph:1106.1445.

**19**. H. P. Yuen, Phys. Rev. A **82**, 062304 (2010).

**20**. И. М. Арбеков, С. Н. Молотков, ЖЭТФ **152**, 62 (2017).

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

**22**. T. Ogawa and H. Nagaoka, IEEE Trans. Inform. Theory **45**, 2486 (1999).

**23**. R. G. Gallager, *A Simple Derivation of the Coding Theorem and Some Applications*, IEEE Trans. Inf. Theory **IT-11**, 3 (1965).

**24**. S. Arimoto, *On the Converse to the Coding Theorem for Discrete Memoryless Channels*, IEEE Trans. Inf. Theory **IT-19**, 357 (1973).

**25**. W. Roga, M. Fannes, and K. Zyczkowski, Phys. Rev. Lett. **105**, 040505 (2010).

**26**. K. M. R. Audenaert, J. Math. Phys. **54**, 073506 (2013); *ibid* **55**, 112202 (2014).