ЖЭТФ, 2020, том 158, вып. 3 (9), стр. 440–458

О ПРОСТОЙ КВАНТОВО-СТАТИСТИЧЕСКОЙ ИНТЕРПРЕТАЦИИ КРИТЕРИЯ СЕКРЕТНОСТИ КЛЮЧЕЙ В КВАНТОВОЙ КРИПТОГРАФИИ

С. Н. Молотков*

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

Академия криптографии Российской Федерации
121552, Москва, Россия

Центр квантовых технологий,
Московский государственный университет им. М. В. Ломоносова
119899, Москва, Россия

Поступила в редакцию 25 февраля 2020 г.,
после переработки 25 февраля 2020 г.
Принята к публикации 26 марта 2020 г.

Несмотря на то что квантовая криптография на сегодняшний день является единственным разделом квантовой информатики, который от фундаментальных физических принципов квантовой механики доведен до практических применений в области передачи и защиты информации, многие результаты остаются, на наш взгляд, малопонятными широкой физической аудитории. Цель данной работы — минимальными и простыми математическими средствами дать простую и интуитивно понятную на физическом уровне интерпретацию центрального результата квантовой криптографии — критерия секретности ключей, основанного на следовой метрике — расстоянии между двумя квантовыми состояниями. Предлагаемая интерпретация является самодостаточной и использует стандартную борновскую квантово-статистическую интерпретацию матрицы плотности — квантового ансамбля — статистической смеси квантовых состояний.

DOI: 10.31857/S0044451020090035

1. ВВЕДЕНИЕ

Квантовая криптография является одним из разделов квантовой информатики, которая на сегодняшний день, в отличие от других квантовых технологий, доведена до реальных практических применений.

Симметричная криптография — шифрование с секретными ключами, используется в системах защиты информации, где необходимы высокая степень защиты и надежности, и требует общего секрета — секретного ключа между пространственно-удаленными пользователями. Симметричная криптография позволяет в принципе достичь высшей степени защиты информации: шифрования в режиме одноразового блокнота — шифрования с одноразовыми ключами [1–3]. Такие системы невозможно дешифровать (взломать) даже теоретически [1–3]. Криптографическая стойкость таких систем основывается на теоретико-информационных критериях стойкости, в отличие от систем асимметричной криптографии с открытыми ключами, криптографическая стойкость которых базируется на строго недоказанных критериях алгоритмической сложности. Одноразовые ключи используются только в специфических ситуациях. Обычно ключ, на котором происходит шифрование, используется неоднократно в течение определенного времени. После передачи определенного объема зашифрованной информации ключ вырабатывает свой криптографический ресурс и требуется смена ключей. При современных объемах передачи информации, например, между центрами обработки данных, требуется все более частая смена секретных ключей. При смене

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

ключей всегда присутствует человеческий фактор, что может приводить к компрометации ключей и взлому системы.

Передача секретных ключей сама по себе требует защищенного канала связи. Для защищенного канала связи в свою очередь требуются секретные ключи, т. е. возникает проблема "Chicken and Egg Problem", которая не имеет решения в области классической физики, когда носителями информации являются классические объекты — сигналы.

Квантовая криптография разрывает данный логический круг и решает проблему распределения ключей по открытым и доступным для подслушивания каналам связи. По сути, квантовая криптография является процедурой согласования двух независимых случайных последовательностей на передающей и приемной сторонах посредством посылки и регистрации квантовых объектов — квантовых состояний через открытый квантовый канал связи. Для согласования результатов измерений, коррекции ошибок в первичных ключах на приемной стороне и сжатия очищенных ключей используется вспомогательный классический открытый аутентичный канал связи. Одна и та же линия связи может выполнять роль как квантового, так и классического канала связи, в зависимости от того, какие состояния посылаются через канал связи.

Неформально секретность ключей в квантовой криптографии базируется на фундаментальном свойстве квантовых состояний — вторжение в квантовый канал связи неизбежно приводит к возмущению передаваемых квантовых состояний и ошибкам измерений на приемной стороне. Энтропийные соотношения неопределенностей [4, 5] позволяют связать наблюдаемый уровень ошибок, навязанный степенью возмущения квантовых состояний на приемной стороне, с верхней фундаментальной границей утечки информации к подслушивателю. Наблюдаемый уровень ошибок на приемной стороне оценивается через открытый классический канал связи посредством раскрытия части переданной последовательности. Раскрытая часть последовательности затем отбрасывается и не фигурирует в ключе. Если наблюдаемая ошибка на приемной стороне, соответственно утечка информации к подслушивателю, меньше критической величины, то взаимная информация между Алисой и Бобом больше, чем информация между Евой и Алисой–Бобом. Неформально разность этих информаций является общим секретом Алисы и Боба — секретным ключом, и неизвестна Еве. При достижении наблюдаемой ошибкой критической величины длина секретного ключа в битах стремится к нулю. В этом случае секретный ключ получить нельзя. Таким образом, до тех пор, пока наблюдаемая ошибка меньше критической величины, Алиса и Боб могут не обращать внимание на присутствие Евы и получать секретный ключ. Если наблюдаемая ошибка больше критической, то проблема с Евой решается другими средствами. Иначе говоря, если ключ получен — ошибка меньше критической, то ключ секретен. Никогда не будет следующей ситуации: ключ получен, считается, что он секретен, а на самом деле таковым не является.

Выше была описана на неформальном уровне причина секретности ключей, которая гарантируется фундаментальными законами Природы. На формальном уровне секретность ключей в квантовой криптографии выражается в довольно абстрактных терминах, и доказательства секретности являются «многоходовыми» [6]. Доказуемая секретность ключей в квантовой криптографии дается в терминах следовой метрики — расстоянии между двумя квантовыми состояниями, описывающими реальную ситуацию после квантового распределения ключей и идеальную ситуацию, когда ключи строго равновероятны и полностью некоррелированы с квантовым состоянием Евы. Данный критерий вызывал споры даже среди специалистов [7]. Абстрактность критерия секретности ключей на основе следовой метрики не содержит интуитивно прозрачных соображений, которые были выработаны применительно к использованию ключей в классической криптографии, например, таких как переборная сложность по поиску истинного ключа, число шифр-сообщений до их первого дешифрования, при условии, что шифрование происходит на ключах, полученных в результате квантового распределения.

Явная связь следового критерия секретности ключей в квантовой криптографии с переборными критериями секретности в классической криптографии была установлена в работе [8].

Простая и прозрачная интерпретация критерия секретности ключей в квантовой криптографии, понятная на физическом уровне интуиции, на наш взгляд, до сих пор отсутствует. Отсутствие такой простой и интуитивно понятной на физическом уровне интерпретации, на наш взгляд, вызывает как минимум состояние неудовлетворенности и ощущение «криптографических фокусов», что не отвечает реальной ситуации.

Цель данной работы — дать простую и физически прозрачную интерпретацию критерия секретности ключей в квантовой криптографии, не прибегая

к сложному математическому аппарату квантовой теории информации. Данная интерпретация использует стандартную квантово-статистическую борновскую трактовку матрицы плотности как статистической смеси квантовых состояний — квантового ансамбля. Данная интерпретация является самодостаточной, при такой трактовке даже не требуется предварительных знаний из классической и квантовой теории информации.

2. СТАДИИ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Для самодостаточности текста напомним, как возникает критерий секретности, основанный на следовой метрике.

После квантового распределения ключей: передачи и измерения квантовых состояний, исправления ошибок и усиления секретности (сжатия очищенных ключей), Алиса и Боб имеют общий ключ — битовую строку длины n, $n \in \mathcal{K} = \{0,1\}^n$. Кратко напомним основные стадии протокола.

После передачи квантовых состояний в соответствии со случайной последовательностью 0 и 1 на передающей стороне Алисы и измерений на приемной стороне в случайных базисах в соответствии со случайной строкой на приемной стороне Боба возникают две битовые последовательности 0 и 1 длиной $m > n$. Результаты измерений на приемной стороне интерпретируются Бобом как 0 и 1. Если бы не было вторжения в квантовый канал связи и собственных неидеальностей аппаратуры (темновых шумов, неточной балансировки интерферометра), то битовая строка Алисы, являющаяся эталоном, совпадала бы со строкой Боба. В реальной ситуации на приемной стороне возникают ошибки. Принципиально невозможно различить ошибки от неидеальностей аппаратуры и ошибки от действия подслушивателя, поэтому все наблюдаемые ошибки относят к действиям подслушивателя.

Удобно сопоставить классическим битовым строкам Алисы и Боба квантовые регистры, в которые записаны ключи

$$(k_1, k_2, \ldots, k_m)_{A,B} \to |k\rangle_{A,B} = \\ = |k_1\rangle_{A,B} \otimes |k_2\rangle_{A,B} \ldots \otimes |k_m\rangle_{A,B}, \quad (1)$$

$$(k_i = 0,1), \quad i = 1,2,\ldots,m, \quad {}_{A,B}\langle k|k'\rangle_{A,B} = \delta_{k,k'}.$$

Квантовые состояния регистров с разными ключами ортогональны, т. е. достоверно различимы. Квантовое состояние регистра Алисы остается у нее как эталонная битовая строка, а второе такое же квантовое состояние направляется в канал связи к Бобу. Это состояние доступно для атаки Евы. Наиболее общая атака Евы на каждое передаваемое состояние может быть представлена следующим образом. Ева готовит вспомогательное квантовое состояние $|E\rangle_E$ и приводит его во взаимодействие с передаваемым состоянием — запутывает состояние $|k_i\rangle_B$ с состоянием $|E\rangle_E$. На формальном языке такое запутывание описывается действием унитарного оператора U_{BE} на эти состояния. Вид унитарного оператора задается Евой. Атака Евы на каждое передаваемое квантовое состояние может быть представлено как

$$|k_i\rangle_A \otimes |k_i\rangle_B \to |k_i\rangle_A \otimes U_{BE}(|k_i\rangle_B \otimes |E\rangle_E) \to \\ \to |k_i\rangle_A \otimes |\Psi^{k_i}\rangle_{BE}. \quad (2)$$

Здесь $|\Psi^{k_i}\rangle_{BE}$ — запутанное состояние Боба и Евы, которое возникло при атаке на состояние $|k_i\rangle_B$ и зависит от выбора унитарного оператора Евы. Подсистему «B» Ева направляет к Бобу, а свою подсистему «E» оставляет в квантовой памяти. В результате атаки к Бобу вместо исходного состояния $|k_i\rangle_{BB}\langle k_i|$ поступает искаженное состояние — состояние подсистемы «B» (2), которое дается частичной матрицей плотности, имеем

$$|k_i\rangle_{BB}\langle k_i| \to \rho_B^{k_i}, \quad \rho_B^{k_i} = \mathrm{Tr}_E\{|\Psi_{BE}^{k_i}{}_{BE}\langle\Psi^{k_i}|\}. \quad (3)$$

Атаку, при которой Ева атакует унитарно передаваемые квантовые состояния индивидуально и независимо в каждой посылке, а затем проводит коллективные измерения над квантовыми состояниями всей последовательности, называют коллективной. В принципе, возможна атака, при которой Ева присоединяет одно свое квантовое состояние ко всей передаваемой последовательности, а затем проводит измерение над своей искаженной квантовой системой. Такая атака была названа когерентной. На первый взгляд, такая атака выглядит для Евы как более эффективная. Однако было доказано [6], что данная атака эквивалента коллективной.

Отметим, что преобразование (2) является наиболее общим преобразованием, допустимым законами квантовой механики. Это следует из одного из центральных результатов квантовой теории информации — теоремы представления Крауса [9,10]. В общем случае описание состояния квантовой системы задается матрицей плотности ρ — положительным эрмитовым оператором со следом единица. Описание при помощи вектора состояния квантовой системы (волновой функции) является частным случаем этого описания. В случае чистого состояния

$|\psi\rangle$ матрица плотности $\rho = |\psi\rangle\langle\psi|$ является проектором ($\rho^2 = \rho$). Неформально теорема Крауса гласит: любое допустимое преобразование квантового состояния в другое квантовое состояние — преобразование оператора матрицы плотности ρ в оператор матрицы плотности ρ' — преобразование, сохраняющее положительность, эрмитовость и не увеличивающее след, задается вполне положительным отображением — супероператором $\mathcal{T}$ [9, 10],

$$\rho' = \mathcal{T}(\rho). \tag{4}$$

При этом любой супероператор унитарно представим, т. е. может быть представлен как действие унитарного оператора на исследуемую квантовую систему вместе с дополнительной квантовой системой, запутывание исследуемой системы со вспомогательной, затем взятие частичного следа по вспомогательной системе. Фактически в (2) использовано унитарное представление наиболее общего преобразования состояния квантовой системы в другое состояние квантовой системы.

Унитарный оператор Ева выбирает оптимальным. Оптимальный выбор осуществляется таким образом, чтобы Ева могла получить максимум информации при заданной наблюдаемой ошибке на приемной стороне. Оптимальный унитарный оператор позволяет получить Еве максимум информации о передаваемом ключе и произвести минимальное возмущение передаваемых состояний. Напомним, что эталонное состояние Алисы $|k_i\rangle_A$ остается неизменным.

Следующая стадия — измерение квантовых состояний на приемной стороне. Остаются только те посылки, в которых базисы измерения и приготовления состояний совпадали, т. е. логические значения 0 и 1 и соответствующие им базисные состояния Алисы $|k_A\rangle_A$ ($k_A = 0, 1$) и Боба $|k_B\rangle_B$ ($k_B = 0, 1$) в (1), (2) записаны в одном и том же базисе. Посылки, в которых базис измерений Боба и базис приготовления состояний Алисы не совпадали, отбрасываются. Поэтому ниже рассматриваем только те посылки, где базисы приготовления и измерения состояний совпадали.

Любое измерение в квантовой теории задается разложением единицы. Разложение единицы является формальным описанием процесса измерений, для i-й посылки имеем

$$I = \sum_{k_i \in \{0,1\}} |k_i\rangle_{BB}\langle k_i|. \tag{5}$$

Для всех m посылок разложение единицы имеет вид

$$I_B = I^{\otimes m} = \left(\sum_{k_i \in \{0,1\}} |k_i\rangle_{BB}\langle k_i| \right)^{\otimes m} = \\ = \sum_{k_B \in \{0,1\}^m} |k_B\rangle_{BB}\langle k_B|, \tag{6}$$

$$|k_B\rangle_B = |k_{i_1}\rangle_B \otimes |k_{i_2}\rangle_B \otimes \ldots |k_{i_m}\rangle_B.$$

Измерения Боба в каждой посылке над возмущенными состояниями (3) приводят к следующим вероятностям результатов измерений у Боба:

$$P_{K_B|K_A}(k_B|k_A) = \mathrm{Tr}_{BE}\{(|k_B\rangle_{BB}\langle k_B| \otimes I_E) \times \\ \times |\Psi^{k_A}\rangle_{BEBE}\langle\Psi^{k_A}|\} = \mathrm{Tr}_B\{|k_B\rangle_{BB}\langle k_B|\rho_B^{k_A}\} = \\ = {}_B\langle k_B|\rho_B^{k_A}|k_B\rangle_B, \tag{7}$$

$$\rho_B^{k_A} = \mathrm{Tr}_E\{|\Psi^{k_A}_{BE}{}_{BE}\langle\Psi^{k_A}|\}.$$

Вероятность $P_{K_B|K_A}(k_B|k_A)$ в (7) имеет смысл условной вероятности того, что Алисой было послано состояние $|k_A\rangle_A$, а Боб зарегистрировал состояние $|k_B\rangle_B$.

После измерений Боба общее квантовое состояние всех участников протокола имеет вид

$$\rho_{ABE} = \sum_{k_A \in \{0,1\}^m} \sum_{k_B \in \{0,1\}^m} P_{K_A}(k_A) \times \\ \times P_{K_B|K_A}(k_B|k_A)|k_A\rangle_{AA}\langle k_A| \otimes |k_B\rangle_{BB} \times \\ \times \langle k_B| \otimes \rho_E^{k_B|k_A}, \tag{8}$$

$$P_{K_BK_A}(k_B, k_A) = P_{K_A}(k_A)P_{K_B|K_A}(k_B|k_A), \tag{9}$$

где $P_{K_BK_A}(k_B, k_A)$ — совместная функция распределения первичных ключей Алисы и Боба, $P_{K_A}(k_A)$ — вероятность распределения битовых строк у Алисы, $P_{K_B}(k_B)$ — вероятность распределения битовых строк (первичных ключей) у Боба, $P_{K_B|K_A}(k_B|k_A)$ — условная вероятность Боба получить результат измерений k_B при условии, что у Алисы битовая строка есть k_A.

Матрица плотности состояния, которое «видит» Ева, зависит от результата измерений Боба и имеет вид

$$\rho_E^{k_B|k_A} = \frac{{}_B\langle k_B|\Psi^{k_A}\rangle_{BEBE}\langle\Psi^{k_A}|k_B\rangle_B}{P_{K_B|K_A}(k_B|k_A)},$$

$$\mathrm{Tr}_E\{\rho_E^{k_B|k_A}\} = 1,$$

$$\rho_E^{k_B|k_A} = \rho_E^{k_{i_1}|k_{j_1}} \otimes \rho_E^{k_{i_2}|k_{j_2}} \otimes \ldots \rho_E^{k_{i_m}|k_{j_m}},$$

$$\mathrm{Tr}_E\{\rho_E^{k_{i_r}|k_{j_r}}\} = 1,$$

$$k_A = (k_{j_1}, k_{j_2}, \ldots, k_{j_m}),$$
$$k_B = (k_{i_1}, k_{i_2}, \ldots, k_{i_m}).$$

Поскольку Еве недоступны результаты измерений Боба, Ева видит статистический ансамбль

$$\rho_{AE} = \mathrm{Tr}_B\{\rho_{ABE}\} = \\ = \sum_{k_A \in \{0,1\}^m} P_{K_A}(k_A) |k_A\rangle_{AA}\langle k_A| \otimes \rho_E^{k_A}, \quad (10)$$
$$\rho_E^{k_A} = \mathrm{Tr}_B\{|\Psi^{k_A}\rangle_{BEBE}\langle\Psi^{k_A}|\}.$$

На этом этапе битовая строка Боба представляет собой первичный ключ. Пусть длина первичного ключа равна m.

После измерений на приемной стороне Алиса и Боб оказываются в ситуации бинарного (не обязательно симметричного) классического канала связи (см. рис. 1). Вся информация, доступная Алисе и Бобу, содержится в совместной матрице плотности Алиса–Боб, которая дается частичным следом по состояниям Евы трехчастичной матрицы плотности Алиса–Боб–Ева в (8), имеем

$$\rho_{AB} = \mathrm{Tr}_E\{\rho_{ABE}\} = \\ = \sum_{k_A \in \{0,1\}^m} \sum_{k_B \in \{0,1\}^m} P_{K_A}(k_A) P_{K_B|K_A}(k_B|k_A) \times \\ \times |k_A\rangle_{AA}\langle k_A| \otimes |k_B\rangle_{BB}\langle k_B|. \quad (11)$$

Дискретный классический канал связи без памяти задается переходными (условными) вероятностями (7), (9), которые определяют вероятность наблюдаемой ошибки на приемной стороне. Сами переходные вероятности связаны с искажениями информационных состояний, которые зависят от атаки Евы (см. формулы (2), (3)) на передаваемые состояния.

Далее следует коррекция ошибок. Коррекция ошибок приводит к тому, что очищенный ключ Боба совпадает с ключом Алисы. Матрица плотности Алиса–Боб вместо (11) становится равной

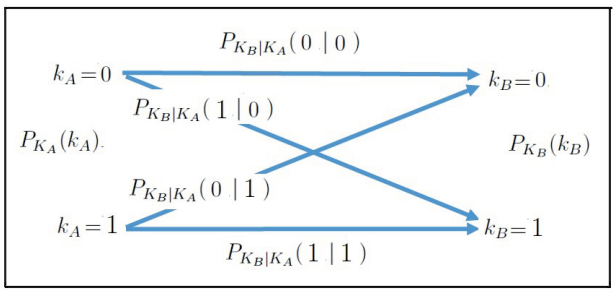

Рис. 1. Бинарный классический канал связи Алиса–Боб, возникающий после измерений Боба

$$\rho_{K_AK_B} = \sum_{k_A \in \{0,1\}^m} \sum_{k_B \in \{0,1\}^m} P_{K_AK_B}(k_A, k_B) \times \\ \times |k_A\rangle_{AA}\langle k_A| \otimes |k_B\rangle_{BB}\langle k_B|, \quad (12)$$

$$P_{K_AK_B}(k_A, k_B) = P_{K_A}(k_A)\delta_{k_Ak_B},$$

теперь $k_B = k_A$. Информация, передаваемая между Алисой и Бобом при коррекции ошибок через открытый классический канал связи, считается доступной Еве. Количество информации в битах, которое передается через классический канал связи при коррекции ошибок в битовой строке длиной m, зависит от используемых кодов коррекции ошибок. Обозначим эту информацию в битах как leak_m. Конкретная величина leak_m в дальнейшем нам не понадобится. После стадии коррекции ошибок Алиса и Боб имеют одинаковые битовые строки — очищенный ключ, о котором Ева имеет частичную информацию, которую она получила при вторжении в квантовый канал связи и коррекции ошибок.

Следующая стадия — усиление секретности — сжатие очищенного ключа при помощи универсальных хеш-функций второго порядка $g \in \mathcal{G}$. Функции осуществляют отображение очищенного ключа — битовой строки длиной m в секретный ключ — битовую строку меньшей длины n, имеем

$$g: \quad k_A \in \{0,1\}^m \to k = g(k_A), \\ k \in \{0,1\}^n, \quad n < m, \quad (13)$$

причем хеш-функция сама является случайной величиной, она выбирается равновероятно из множества функций $\mathcal{G}$. Вероятность выбора конкретной хеш-функции g есть $P_G(g) = 1/|\mathcal{G}|$ ($|\mathcal{G}|$ — размер множества хеш-функций). Данные функции были введены в работе [11], где было также доказано существование таких функций. Более формально, $g(\ldots)$ является хеш-функцией второго порядка, если имеет место соотношение

$$\mathrm{Pr}_G\left\{g(k_A) = g(k_A^{'})\right\} < \frac{1}{|G|} = \frac{1}{2^n}, \quad (14)$$

$$\forall \quad k_A \neq k_A^{'} \in \{0,1\}^m, \quad k = g(k_A),$$
$$k' = g(k_A^{'}), \quad k, k' \in \{0,1\}^n,$$

где усреднение проводится по равновероятному случайному выбору по множеству хеш-функций. Интуитивный смысл использования хеш-функций второго порядка состоит в следующем. Неравенство (14) говорит о том, что в каждое хеш-значение попадает в среднем одинаковое число исходных битовых

строк, соответственно, для Евы — одинаковое число матриц плотности, привязанных к каждому первичному ключу. Такое сжатие обеспечивает равномерное распределение хеш-значений, что приводит к уменьшению частичной информации Евы о первичном ключе на любую наперед заданную величину.

У Алисы и Боба очищенные ключи одинаковы, поэтому отображаются в одну и ту же битовую строку. Ева имеет частичную информацию об исходной битовой строке (грубо говоря, часть строки не знает), поэтому битовая строка, которая известна лишь частично, будет отображаться в разные сжатые строки.

Покажем пример плохого неравномерного сжатия. Пусть все исходные битовые строки отображаются в одно и то же хеш-значение (все точки-прообразы переходят в одну точку). В этом случае информация Евы о сжатой битовой строке не уменьшается, а, наоборот, становится достоверной. Следовый критерий секретности (см. ниже) доказывается только для такого равномерного сжатия.

Степень сжатия определяется частичной матрицей плотности ρ_{AE} (15), через которую (см. ниже) выражается нехватка информации Евы о первичном ключе, имеем

$$\rho_{AE} = \sum_{k_A \in \{0,1\}^m} P_{K_A}(k_A) |k_A\rangle_{AA}\langle k_A| \otimes \rho_E^{k_A}, \quad (15)$$

$$\rho_E^{k_A} = \mathrm{Tr}_B\{|\Psi^{k_A}\rangle_{BEBE}\langle\Psi^{k_A}|\}.$$

Матрица плотности (15) описывает корреляции между эталонной битовой строкой Алисы и квантовыми состояниями Евы до сжатия ключей — усиления секретности. После процедуры усиления секретности матрица плотности (15) переходит в ρ_{KE}, $\rho_{AE} \to \rho_{KE}$. Теперь вместо $\rho_E^{k_A}$ Ева «видит» состояния

$$\rho_{KE} = \rho_{GAGE} = \sum_{k \in \{0,1\}^n} P_K(k) |k\rangle_{KK}\langle k| \otimes \rho_E^k, \quad (16)$$

$$P_K(k)\rho_E^k = \overline{\rho}_E^k, \quad \overline{\rho}_E^k = \sum_{g \in \{G\}} P_G(g) |g\rangle_{GG}\langle g| \otimes \otimes \left(\sum_{k_A = g^{-1}(k)} P_{K_A}(k_A) \rho_E^{k_A} \right), \quad (17)$$

где $P_{K_A}(k_A)$ ($k_A \in \{0,1\}^m$) — функция распределения исходных первичных ключей, $P_K(k)$ ($k \in \in \{0,1\}^n$, $n < m$) — функция распределения финальных секретных ключей (см. ниже), $P_G(g) = = 1/|G|$ — однородное распределение вероятностей при случайном выборе хеш-функций, $|g\rangle_{GG}\langle g|$ — публично доступный классический регистр, в котором хранится выбранная хеш-функция. Сжатие ключей происходит через открытый канал связи, поэтому выбор хеш-функции доступен Еве. Сжимающее отображение исходной битовой строки легитимных пользователей $|k_A\rangle_A \to |k\rangle_K$ ($k_A \in \{0,1\}^m \to \to k \in \{0,1\}^n$, $k = g(k_A)$, $n < m$, n — длина сжатого секретного ключа) индуцирует преобразование квантовых состояний Евы.

Далее $g^{-1}(\ldots)$ — обратная функция $g(\ldots)$. Формула (17) имеет простой смысл: Ева вместо исходного состояния $\rho_E^{k_A}$ видит статистическую смесь состояний, в которую переходят состояния ρ_E^k при сжатии очищенных ключей.

Перейдем теперь к обсуждению критерия секретности ключей.

3. КРИТЕРИЙ СЕКРЕТНОСТИ КЛЮЧЕЙ, ОСНОВАННЫЙ НА СЛЕДОВОЙ МЕТРИКЕ

Критерий секретности гласит [6], что следовое расстояние между матрицами плотности, описывающее реальную ситуацию после квантового распределения ключей и идеальную ситуацию после усиления секретности очищенных ключей, не превосходит

$$||\rho_{KE} - \rho_U \otimes \rho_E||_1 < \varepsilon, \quad (18)$$

где следовое расстояние между двумя матрицами плотности ρ и σ по определению равно

$$||\rho - \sigma||_1 = \mathrm{Tr}\{|\rho - \sigma)|\} = = \mathrm{Tr}\left\{\sqrt{(\rho^+ - \sigma^+)(\rho - \sigma)}\right\}. \quad (19)$$

Здесь ε — параметр секретности, который задается легитимными пользователями,

$$\rho_{KE} = \sum_{k \in \{0,1\}^n} P_K(k) |k\rangle_{KK}\langle k| \otimes \rho_E^k, \quad (20)$$

$$\sum_{k \in \{0,1\}^n} P_K(k) = 1, \quad \mathrm{Tr}\{\rho_E^k\} = 1.$$

$$\rho_E = \mathrm{Tr}\{\rho_{KE}\} = \sum_{k \in \{0,1\}^n} P_K(k)\rho_E^k,$$
$$\rho_U = \frac{1}{2^n} \sum_{k \in \{0,1\}^n} |k\rangle_{KK}\langle k|, \quad (21)$$

ρ_{KE} — совместная матрица плотности Алиса–Боб и Ева, ρ_E — полная матрица плотности Евы, ρ_E^k — частичные матрицы плотности Евы, «привязанные»

к ключам Алисы–Боба k, $P_K(k)$ — функция распределения секретных ключей Алисы–Боба, ρ_U — матрица плотности, отвечающая идеальным ключам Алисы–Боба. Все матрицы плотности в (18)–(21) нормированы на единицу. Центральный результат теории квантовой криптографии состоит в следующем:

$$||\rho_{KE} - \rho_U \otimes \rho_E||_1 < \\ < \varepsilon_1 + 2^{-(H_{min}^{\varepsilon_1}(\rho_{AE}|\rho_E) - \mathrm{leak}_m - n)/2}, \quad (22)$$

где $H_{min}^{\varepsilon_1}(\rho_{AE}|\rho_E)$ — сглаженная условная минимальная энтропия (см. детали, например, в [6]), leak_m — информация в битах, расходуемая на коррекцию ошибок. По определению

$$H_{min}^{\varepsilon_1}(\rho_{AE}|\rho_E) = \\ = \mathrm{supp}_{\overline{\rho}_{AE} \in \mathcal{B}^{\varepsilon_1}(\rho_{AE})} H_{min}(\overline{\rho}_{AE}|\overline{\rho}_E), \quad (23)$$

$$H_{min}(\overline{\rho}_{AE}|\overline{\rho}_E) = -\log(\lambda), \quad (24)$$

где $\log \equiv \log_2$, λ — минимальное число, такое что оператор $\lambda I_A \otimes \rho_E - \rho_{AE} > 0$. Поиск минимума происходит по матрицам плотности, которые лежат в шаре радиусом ε_1. При больших m имеет место соотношение [6]

$$\frac{1}{m} H_{min}^{\varepsilon_1}(\rho_{AE}|\rho_E) \geq \min_{\overline{\rho}_{AE} \in \mathcal{B}^{\varepsilon_1}(\rho_{AE})} H(\overline{\rho}_{AE}|\overline{\rho}_E). \quad (25)$$

Поясним на неформальном уровне возникновение сглаженной энтропии в (22). Появление величины ε_1 в (22)–(25) связано со следующим. При конечных длинах последовательностей m величина ошибки на приемной стороне флуктуирует. В эксперименте наблюдаемой величиной является частота ошибок, которая стремится при большом объеме выборки к истинной вероятности ошибки. Из-за флуктуаций частота ошибок имеет разброс, соответственно матрица плотности также имеет разброс. Далее ρ_{AE} — матрица плотности, которая приводит к наблюдаемой частоте ошибок.

Для наших целей будет достаточно следующей оценки минимальной энтропии, когда матрица плотности ρ_{AE} представляет собой тензорное произведение [6]:

$$\frac{1}{m} H_{min}^{\varepsilon_1}(\rho_{AE}|\rho_E) \geq H(\rho_{AE}|\rho_E) - \\ - \mathrm{const} \cdot \sqrt{\frac{\log(1/\varepsilon_1)}{m}}, \quad (26)$$

где const — постоянная порядка единицы,

$$H(\rho_{AE}|\rho_E) = H(\rho_{AE}) - H(\rho_E), \quad (27)$$

$$H(\rho_{AE}) = -\mathrm{Tr}\{\rho_{AE} \log(\rho_{AE})\}, \\ H(\rho_E) = -\mathrm{Tr}\{\rho_E \log(\rho_E)\}, \quad (28)$$

— энтропия фон Неймана. Если бы длина последовательности была равна $m = \infty$, то частота наблюдаемых ошибок совпадала бы с вероятностью ошибок. В этом случае условная минимальная энтропия совпадала бы с энтропией фон Неймана в (27). Присутствие отрицательного слагаемого в правой части (26) эффективно уменьшает нехватку информации Евы, это эффективный учет того факта, что наблюдаемая частота ошибок (вычисляется через ρ_{AE}) может оказаться несколько меньше истинной вероятности ошибки за счет флуктуаций, поэтому следует уменьшить нехватку информации Евы (слагаемое с log в правой части (26)).

Величина ε_1 выбирается легитимными пользователями и определяет, по существу, величину доверительного интервала для оценки вероятности ошибки по наблюдаемой частоте. Как видно из (26), величина ε_1 при заданной длине зарегистрированной последовательности квантовых состояний m определяет точность оценки величины энтропии — нехватки информации Евы. Чем точнее требуется оценка (ε_1 задано), тем бóльшая длина последовательности m требуется.

Отметим, что в критерии (22) фигурируют квантовые состояния — матрицы плотности составной системы Алиса–Боб и Ева до коррекции ошибок (15). Физический смысл условной минимальной энтропии и энтропии фон Неймана (23)–(25), (27) — нехватка информации Евы в битах о битовой строке длиной m при условии, что Ева имеет в своем распоряжении квантовую систему (15), привязанную к каждой позиции первичного ключа. При коррекции ошибок через открытый канал, доступный в том числе и Еве, выдается leak_m битов информации. Данная информация уменьшает нехватку информации Евы о битовой строке — данная информация вычитается из первичной нехватки информации $H_{min}^{\varepsilon_1}(\rho_{AE}|\rho_E)$ в экспоненте (22).

Как следует из (22), если длина финального секретного ключа $n < m$ выбрана так, что

$$2^{-(H_{min}^{\varepsilon_1}(\rho_{AE}|\rho_E) - \mathrm{leak}_m - n)/2} < \varepsilon_1, \quad (29)$$

фактически при требуемой (заданной) длине финального секретного ключа n сначала выбирается $\varepsilon_1/2 = \varepsilon$, затем выбирается длина последовательности m, чтобы удовлетворялось (29), и тогда финальный ключ длиной n битов будет ε-секретным.

Таким образом, заданное ε достигается путем сжатия очищенного ключа, естественно, если нужно, чтобы финальный ключ был заданной длины n и был ε-секретным, то необходимо обеспечить соответствующую длину m первичного ключа.

Вся информация об атаках Евы заключена в матрице плотности $\rho_E^{k_A}$ (см. формулы (15)), они же, по сути, фигурируют в критерии секретности (22). Вычисление данных матриц плотности для различных атак, включая атаки активного зондирования аппаратуры Алисы и Боба [12], представляет собой задачу квантового криптоанализа систем квантовой криптографии.

Далее нас будет интересовать интерпретация самого критерия секретности ключей (18), (22). В следующих разделах, используя стандартную квантово-статистическую интерпретацию матрицы плотности как квантового ансамбля, дадим простую физическую интерпретацию следового критерия секретности (18).

4. СУЩЕСТВУЮЩИЕ ИНТЕРПРЕТАЦИИ КРИТЕРИЯ СЕКРЕТНОСТИ КЛЮЧЕЙ

Следовое расстояние является интегральной характеристикой, которая характеризует близость двух квантовых состояний. Возможны различные интерпретации следового расстояния. Рассмотрим несколько существующих интерпретаций.

1. Вероятность различения квантовых состояний.

Эта интерпретация сводится к следующему. Имеется два квантовых состояния $\rho_0 = \rho_{KE}$, описывающих реальную ситуацию после квантового распределения ключей — квантовые состояния Евы коррелированы с ключами. Состояние $\rho_1 = \rho_U \otimes \rho_E$ описывает идеальную ситуацию: идеальные ключи строго равновероятны и квантовая система Евы никак не коррелирована с ключами. Задача состоит в различении одного квантового состояния от другого с минимально возможной вероятностью ошибки. Пусть состояния предъявляются для различения равновероятно. Различение квантовых состояний может быть сделано при помощи измерений. Измерение, различающее два квантовых состояния (возможно с некоторой вероятностью ошибки), имеет два исхода. Исходы измерений над квантовой системой случайны. Один исход измерений интерпретируется как состояние ρ_0, второй исход измерений — как ρ_1. Задача об оптимальном различении двух квантовых состояний в квантовой теории информации известна давно и имеет точное решение [13]. Ошибка различения двух состояний есть

$$P_{err} = \frac{1}{2}\left(1 - ||\rho_{KE} - \rho_U \otimes \rho_E||_1\right) < \frac{1}{2}\left(1 - \varepsilon\right) \quad (30)$$

и выражается через следовое расстояние. В идеальном случае $\varepsilon = 0$, так как состояния слипаются, ошибка различения равна вероятности простого угадывания, это и есть наихудший случай. На основании вероятности (30) различения двух квантовых состояний дается интерпретация. Если практически нельзя отличить квантовое состояние, описывающее реальную ситуацию, от квантового состояния идеальной ситуации, то произносятся слова, что ключи, полученные в реальном сеансе квантового распределения ключей, неотличимы (с вероятностью ε (18)) от ключей, полученных в идеальной ситуации. Хотя вероятности различения самих ключей в (30) явно нет. Есть только вероятность различения двух ситуаций как целого.

Данная интерпретация была, по-видимому, первой и вызывала большие споры [7]. Такая интерпретация является крайне абстрактной — подразумевает измерение двух квантовых состояний, отвечающих двум ситуациям. Совершенно непонятно, как устроить измерения двух таких состояний.

2. Вероятность угадывания ключей.

Из-за неудовлетворительности предыдущей интерпретации была предложена следующая. Измеряя свои квантовые состояния после реального сеанса квантового распределения ключей, подслушиватель получает свою битовую строку, которая является неидеальной копией секретного ключа Алисы и Боба. Оказалось, что средняя вероятность по всем ключам того, что копия ключа Евы k_E будет совпадать с секретным ключом Алисы и Боба k, не превосходит следующие величины [13, 14]:

$$P(k = k_E) < \frac{1}{2^n} + ||\rho_{KE} - \rho_U \otimes \rho_E||_1 < \frac{1}{2^n} + \varepsilon, \quad (31)$$

т. е. превышает вероятность простого угадывания ключа — первое слагаемое в правой части (31) ($1/2^n$, n — длина ключа в битах) — лишь на величину ε.

3. Трудоемкость определения истинного ключа.

Предыдущая интерпретация также не является полной. В криптографии важными являются критерии секретности, использующие трудоемкость перебора по поиску истинного ключа. Ранее [8] была установлена связь критерия секретности (18) и критериев, использующих понятие трудоемкости — число шагов перебора по определению ключа до нахождения истинного ключа. Ключи используются в

системах шифрования. Возникает вопрос, как изменится число шагов перебора ключей по поиску истинного, если вместо идеальных ключей (строго равновероятных и полностью неизвестных подслушивателю) будут использоваться ε-секретные ключи (18). Полный перебор по всему ключевому пространству — трудоемкость (в англоязычной версии Guess Work [15]), при идеальных ключах составляет

$$G(K) = \frac{N_n}{2}, \quad N_n = 2^n, \tag{32}$$

для ε-секретных ключей число шагов перебора становится равным

$$G_\varepsilon(K) \geq \frac{N_n(1-2\varepsilon)}{2}. \tag{33}$$

Возможен также частичный перебор по части ключевого пространства (см. подробности в [8]), который также выражается через величину следового расстояния. Оказалось [8], что величина $1/\varepsilon$ определяет число шифр-сообщений до первого прочтения сообщения — вскрытия шифра. Результаты [8] дают четкие границы для использования ε-секретных ключей в системах шифрования.

Последняя интерпретация является уже достаточной и вполне содержательной для использования ключей, полученных в системах квантовой криптографии, в криптографических приложениях, однако данная интерпретация далека от простой и интуитивно понятной на физическом уровне интерпретации.

5. КВАНТОВО-СТАТИСТИЧЕСКАЯ ИНТЕРПРЕТАЦИЯ КРИТЕРИЯ СЕКРЕТНОСТИ КЛЮЧЕЙ

Ниже будет дана простая и понятная на уровне физической интуиции интерпретация критерия секретности ключей в квантовой криптографии, которая базируется на стандартной борновской интерпретации матрицы плотности как статистического ансамбля квантовых состояний. При этом интерпретация не требует предварительных знаний как из классической, так и квантовой теории информации. В этой части она основана на простых комбинаторных соображениях и интерпретации вероятности как предела частоты появления случайных событий при большом числе испытаний.

5.1. Интерпретация матрицы плотности легитимных пользователей

Составная квантовая система Алиса–Боб и Ева описывается матрицей плотности ρ_{KE}. Дадим стандартную квантовомеханическую интерпретацию данной матрицы плотности. Алиса в своем распоряжении имеет матрицу плотности, которая дается частичным следом матрицы плотности составной системы, имеем

$$\rho_K = \mathrm{Tr}_E\{\rho_{KE}\} = \sum_{k\in K} P_K(k)|k\rangle_{KK}\langle k|. \tag{34}$$

Стандартная борновская интерпретация матрицы плотности (34) в нашем случае сводится к следующему. Каждый ключ k в (34) возникает с вероятностью $P_K(k)$. С каждым ключом в (34) ассоциирована, т. е. «привязана» к ключу, матрица плотности ρ_E^k Евы.

Вероятность $P_K(k)$ появления конкретного значения ключа k также должна быть интерпретирована. Вероятность интерпретируется через предел частоты событий при большом числе испытаний. Пусть проводится N независимых квантовых распределений ключей — испытаний в одних и тех же условиях. После каждого квантового распределения ключей (каждого испытания) возникает конкретный ключ k и состояние Евы ρ_E^k. После серии экспериментов в одних и тех же условиях возникает последовательность исходов — последовательность состояний у Алисы–Боба и Евы.

В результате N испытаний у Алисы–Боба может возникнуть одна из последовательностей состояний — ключей. Все последовательности, возникающие в результате распределения ключей, могут быть представлены в виде

$$\left.\begin{array}{l} |k_{1_1}\rangle_{KK}\langle k_{1_1}| \otimes |k_{1_2}\rangle_{KK}\langle k_{1_2}| \otimes \ldots \otimes |k_{1_N}\rangle_{KK}\langle k_{1_N}|, \\ \ldots \\ |k_{j_1}\rangle_{KK}\langle k_{j_1}| \otimes |k_{j_1}\rangle_{KK}\langle k_{j_1}| \otimes \ldots \otimes |k_{j_N}\rangle_{KK}\langle k_{j_N}|, \\ \ldots \\ |k_{N_1}\rangle_{KK}\langle k_{N_1}| \otimes |k_{N_1}\rangle_{KK}\langle k_{N_1}| \otimes \ldots \otimes |k_{N_N}\rangle_{KK}\langle k_{N_N}|, \end{array}\right\} 2^{nN} \text{ вариантов серий длиной } N. \tag{35}$$

Здесь k_{j_i} — ключ в j-й серии испытаний на i-м месте, $i = 1, 2, \ldots, N$.

Для дальнейшего будет использован следующий факт. Все последовательности в (35) содержатся в тензорном произведении матрицы плотности:

$$\begin{aligned}(\rho_K)^{\otimes N} &= (\mathrm{Tr}_E\{\rho_{KE}\})^{\otimes N} = \\ &= \left(\sum_{k\in K} P_K(k)|k\rangle_{K\,K}\langle k|\right)^{\otimes N} = \\ &= P_K(k_1)|k_1\rangle_{K\,K}\langle k_1| \otimes P_K(k_2) \times \\ \times\, |k_2\rangle_{K\,K}\langle k_2| \otimes \ldots \otimes P_K(k_N)|k_N\rangle_{K\,K}\langle k_N| + \ldots \quad (36)\end{aligned}$$

Отдельные последовательности в (35) отвечают различным слагаемым в (36) при возведении в тензорную степень. Порядок сомножителей в каждом слагаемом в разложении (36) важен, он отвечает за номер испытания, в котором появляется данный ключ.

При каждом испытании ключ может принимать одно из 2^n значений (напомним, что n — длина битовой строки ключа), поэтому всего возможно 2^{nN} разных вариантов последовательностей в (35).

Различные последовательности в (35) встречаются с разными вероятностями. При большой длине серии N число ключей k_1 в каждой серии примерно равно $n_1 = NP_K(k_1)$, число ключей k_2 равно $n_2 = NP_K(k_2)$, ..., число ключей k_{2^n} равно $n_{2^n} = NP_K(k_{2^n})$, что является выражением того факта, что среднее по числу испытаний стремится к математическому ожиданию. Данные последовательности являются наиболее вероятными, т. е. типичными (см. ниже). Напомним, что имеет место условие нормировки

$$\sum_{k=1}^{2^n} P_K(k) = 1. \quad (37)$$

Полное число таких типичных последовательностей оценивается как

$$\begin{aligned}N(n_1, n_2, \ldots, n_{2^n}) &= C_N^{n_1 n_2 \ldots n_{2^n}} = \\ &= \frac{N!}{n_1! n_2! \ldots n_{2^n}!}, \quad N = n_1 + n_2 + \ldots + n_{2^n}, \quad (38)\end{aligned}$$

что равно числу размещений n_1, $n_2, \ldots, n_{2^n}$ ключей типа $1, 2, \ldots, 2^n$ по N позициям. Все последовательности такого типа имеют одинаковую вероятность и различаются только перестановками ключей по N позициям.

Учитывая, что вероятность появления каждой типичной последовательности есть

$$\begin{aligned}P(n_1, n_2, \ldots, n_{2^n}) &= \\ &= (P_K(k_1))^{n_1}(P_K(k_2))^{n_2} \ldots (P_K(k_{2^n}))^{n_{2^n}}, \quad (39)\end{aligned}$$

используя формулу Стирлинга

$$N! \approx \sqrt{2\pi N}\left(\frac{N}{e}\right)^N, \quad (40)$$

в главном приближении можно записать

$$\frac{N!}{n_1! n_2! \ldots n_N!} \to \frac{N^N}{(NP_K(k_1))^{NP_K(k_1)}(NP_K(k_2))^{NP_K(k_2)} \ldots (NP_K(x_{k_{2^n}}))^{NP_K(k_{2^n})}}, \quad (41)$$

с учетом (38)–(41) в асимптотическом пределе больших N получаем оценку для числа типичных последовательностей

$$\begin{aligned}N(n_1, n_2, \ldots, n_{2^n}) &= 2^{NH(X)}, \\ H(K) &= -\sum_{k\in\{0,1\}^n} P_K(k)\log(P_K(k)).\end{aligned} \quad (42)$$

Здесь $H(K)$ — энтропия Шеннона.

Из физически и интуитивно простых комбинаторных соображений получено следующее утверждение: с вероятностью единица при длинной серии испытаний — квантовых распределений ключей у Алисы–Боба возникнет одна из типичных последовательностей ключей. При длинной серии испытаний типичные последовательности равновероятны и различаются только размещением ключей в разных позициях — испытаниях, в каждой типичной последовательности. Энтропия Шеннона является мерой информации в битах, заключенной во множестве типичных последовательностей.

Отметим важное для дальнейшего утверждение. Поскольку матрица плотности (34) записана в диагональном виде, подсчет числа типичных последовательностей, соответственно, размерность пространства, в которое вкладываются состояния в (35), возможен путем простых комбинаторных соображений (38)–(41).

Фактически, это один из центральных результатов классической теории информации — теорема о асимптотически равновероятном распределении типичных последовательностей [16]. Определим $\mathcal{T}_\delta^{(N)}$ как множество δ типичных последовательностей по отношению к распределению вероятностей $P_K(k)$, вероятности которых удовлетворяют условию

$$(k_1, k_2, \ldots, k_{2^n}) \in \mathcal{K}^n, \quad 2^{-N(H(K)+\delta)} \leq \leq P(n_1 n_2 \ldots n_{2^n}) \leq 2^{-N(H(K)-\delta)}. \quad (43)$$

Тогда в более аккуратной формулировке теорема о асимптотически равнораспределенности формулируется следующим образом:

1) если $(k_1, k_2, \ldots, k_{2^n}) \in \mathcal{T}_\delta^{(N)}$, то вероятность такой последовательности удовлетворяет соотношению

$$H(K) - \delta \leq -\frac{1}{N}\log(P(n_1 n_2 \ldots n_{2^n})) \leq H(K) + \delta;$$

2) вероятность последовательности при N испытаниях попасть в типичное множество последовательностей не менее $\Pr\{\mathcal{T}_\delta^{(N)}\} \geq 1 - \delta$;

3) количество типичных последовательностей $|\mathcal{T}_\delta^{(N)}|$ лежит в диапазоне $(1-\delta)2^{N(H(K)-\delta)} \leq |\mathcal{T}_\delta^{(N)}| \leq 2^{N(H(K)+\delta)}$.

Неформально говоря, вероятность попасть в типичное множество последовательностей при больших N равна единице, все типичные последовательности равновероятны и их число равно $2^{NH(K)}$, соответственно, вероятность каждой последовательности есть $2^{-NH(K)}$.

Таким образом, в результате серии реальных квантовых распределений ключей Алиса–Боб будут иметь в своем распоряжении одну из типичных последовательностей ε-секретных ключей, где с каждым ключом ассоциирована квантовая системы Евы (см. (20), (21)).

5.2. Связь энтропии Шеннона ключей со следовым расстоянием

Выше была дана интерпретация матрицы плотности Алисы–Боба в реальной ситуации квантового распределения ключей. В идеальной ситуации матрица плотности Алисы–Боба соответствует идеальному распределению ключей ρ_U — все ключи равновероятны, поэтому все битовые последовательности в идеальной ситуации являются типичными. Вероятность любого ключа $P_K(k) = 1/2^n$, энтропия Шеннона в этом случае $H(K) = n$ и ключи некоррелированы с квантовой системой Евы ρ_E.

Фактически имеет место ситуация с классическим источником состояний — ключей. Ключи в каждом акте реального квантового распределения ключей выбираются из алфавита $k \in \mathcal{K} = \{0,1\}^n$ с вероятностями $P_K(k)$, заданными над алфавитом. Квантовые состояния $|k\rangle$, отвечающие разным битовым строкам ключей, ортогональны, поэтому достоверно различимы у Алисы–Боба. Достоверная различимость ключей у Алисы–Боба означает их классический характер. Полное пространство идеальных ключей имеет размерность 2^{nN}.

В реальной ситуации размерность типичного пространства ключей есть $2^{H(K)N}$, что несколько меньше, чем размерность пространства идеальных ключей. После каждого квантового распределения ключей Алиса–Боб будут иметь с вероятностью единица один из ключей, который лежит в пространстве типичных последовательностей (43).

Размерность ключевого пространства определяется энтропией Шеннона (42), для вычисления которой требуется знать распределение вероятностей ключей $P_K(k)$ в (42). Однако явно само распределение вероятностей ключей после квантового распределения ключей неизвестно, известно лишь, что распределение вероятностей близко в смысле следового расстояния к равномерному распределению $P_U(k) = = 1/2^n$.

Для дальнейшего потребуется воспользоваться одним полезным свойством следовой метрики, а именно, следовое расстояние не возрастает при действии квантового преобразования — супероператоров над матрицами плотности [13]. Взятие частичного следа является частным примером супероператора. Интуитивно данное свойство очень понятно, поскольку при взятии частичного следа одна из квантовых подсистем составной квантовой системы становится недоступной, что, очевидно, должно уменьшать различимость состояний. Из свойств следового расстояния [13] следует, что

$$||P_K - P_U||_1 = \frac{1}{2}\sum_{k\in\mathcal{K}} |P_K(k) - P_U(k)| = = ||\rho_K - \rho_U||_1 \leq ||\rho_{KE} - \rho_U \otimes \rho_E||_1 < \varepsilon. \quad (44)$$

Для того чтобы выяснить размерность типичного пространства ключей, требуется связать энтропию Шеннона со следовым расстоянием. Энтропия Шеннона оказывается не меньше, чем [15]

$$H(K) \geq \log|K| + 2||P_K - P_U||_1 \times \times \log\left(\frac{2||P_K - P_U||_1}{|K|}\right) = n(1-2\varepsilon) + 2\varepsilon\log(2\varepsilon), \quad (45)$$

где $|K| = 2^n$ — размерность ключевого пространства идеальных ключей. С логарифмической точностью размерность пространства ключей после реального квантового распределения ключей $H(K) \geq n(1-2\varepsilon)$, т. е. после распределения ключей Алиса–Боб с вероятностью единица имеют один из ключей из множества, изображенного на рис. 2.

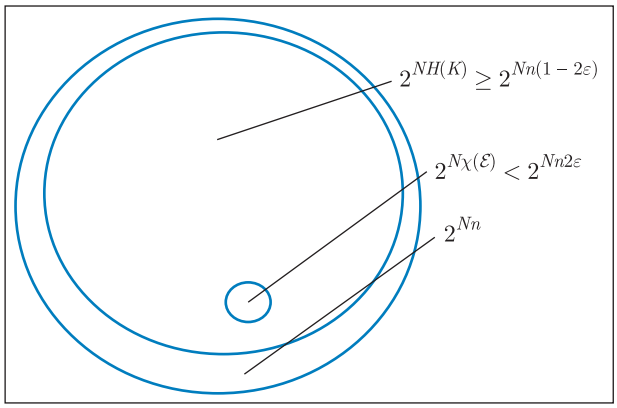

Рис. 2. Схематическое изображение областей пространства типичных последовательностей для случая идеальных ключей (размер множества 2^{Nn}), множества ε-секретных ключей (размер множества $2^{NH(K)}$) и множества последовательностей, которые может различить подслушиватель (размер множества $2^{N\chi(\mathcal{E})}$)

Следующий вопрос, на который мы хотим ответить, какова размерность типичного множества копий ключей у Евы. Неформально говоря, какую долю ключевого пространства Алисы–Боба с размерностью $2^{n(1-2\varepsilon)}$ Ева сможет различить после измерений над своей квантовой системой, коррелированной с каждым ключом.

5.3. Интерпретация матрицы плотности и измерений подслушивателя

Принципиально другая ситуация возникает у Евы, которая имеет в своем распоряжении квантовые состояния ρ_E^k, привязанные к каждому ключу k. Для того чтобы узнать ключ Алисы–Боба, Ева должна проводить измерения над своими квантовыми состояниями.

Перейдем теперь к интерпретации матрицы плотности Евы и ее измерений над квантовыми состояниями. В результате N испытаний у Евы вместо множества вариантов возникает одна из последовательностей квантовых состояний. В каждой последовательности в каждом акте испытаний Ева имеет в своем распоряжении квантовое состояние, которое «привязано» к ключу (коррелировано с ключом) Алисы–Боба. Все возникающие последовательности квантовых состояний у Евы могут быть представлены в виде

$$\left.\begin{array}{l} \rho_E^{k_{1_1}} \otimes \rho_E^{k_{1_2}} \otimes \ldots \otimes \rho_E^{k_{1_N}}, \\ \ldots \\ \rho_E^{k_{j_1}} \otimes \rho_E^{k_{j_2}} \otimes \ldots \otimes \rho_E^{k_{j_N}}, \\ \ldots \\ \rho_E^{k_{N_1}} \otimes \rho_E^{k_{N_2}} \otimes \ldots \otimes \rho_E^{k_{N_N}}, \end{array}\right\} \begin{array}{l} 2^{nN} \text{ вариантов} \\ \text{серий длиной } N. \end{array} \tag{46}$$

Неформально формула (46) означает, что после каждого акта квантового распределения ключей Ева имеет в своем распоряжении квантовое состояние $\rho_E^{k_{j_m}}$ с вероятностью $P_K(k_{j_m})$, привязанное к ключу Алисы–Боба, возникающему с той же вероятностью (см. (47)).

Всевозможные последовательности в (46) представляют собой матрицу плотности вида

$$\rho_E^{\otimes N} = \left(\sum_{k\in\mathcal{K}} P_K(k)\rho_E^k\right)^{\otimes N}. \tag{47}$$

Вероятность каждой последовательности определяется числом появлений одного и того же типа матриц плотности Евы аналогично соответствующему числу появлений ключей одного типа. Вероятность каждой последовательности дается формулой (47).

Цель Евы — проводя измерения над своими квантовыми состояниями, узнать ключ, к которому привязаны ее матрицы плотности. Возможны два типа измерений:

1) индивидуальные;

2) коллективные.

После каждого акта распределения ключей в квантовой памяти возможно одно из 2^n состояний ρ_E^k, привязанных к ключу k Алисы–Боба. Квантовые состояния ρ_E^k, отвечающие различным ключам k, являются неортогональными — матрицы плотности этих состояний не коммутируют, поэтому данные состояния достоверно неразличимы, т. е. различимы с некоторой вероятностью ошибки. Степень различимости связана с величиной параметра секретности ε в (18). Чем больше параметр ε, тем ситуация после распределения ключей дальше от идеальной и тем лучше различимы состояния Евы, и наоборот. При $\varepsilon \to 0$ квантовые состояния Евы некоррелированы с ключами, т. е. матрицы плотности Евы, отвечающие отдельным ключам, неразличимы в том смысле, что любому ключу отвечает одна и та же матрица плотности, иначе говоря, матрица плотности $\rho_E^k = \rho_E/2^n$ не зависит от k.

Важно подчеркнуть, что индивидуальные измерения Ева проводит независимо после каждого распределения ключей над конкретной ρ_E^k, полученной

в этом акте. Измерения даются разложением единицы в пространстве состояний Евы:

$$I_E = \sum_{k_E \in K_E} \mathcal{M}_{k_E}, \quad \mathcal{K}_E = \{0,1\}^n, \tag{48}$$

где k_E — значение копии истинного ключа у Евы, $\mathcal{M}_{k_E}$ — операторно-значная мера. Условная вероятность того, что истинный ключ Алисы–Боба есть k, а Ева в результате измерений получит значение ключа k_E, равна

$$P_{K_E|K}(k_E|k) = \mathrm{Tr}_E\{\rho_E^k \mathcal{M}_{k_E}\}. \tag{49}$$

Вероятность правильной идентификации ключа у Евы после конкретного квантового распределения ключей равна $P_{K_E|K}(k|k)$. Квантовое состояние у Евы после каждого квантового распределения ключей, согласно (47), возникает с вероятностью $P_K(k)$ (см. (47)), поэтому средняя вероятность правильного различения ключей при индивидуальных измерениях квантовых состояний у Евы есть

$$\overline{\mathrm{Pr}}_{OK} = \sum_{k \in K} P_K(k) P_{K_E|K}(k|k). \tag{50}$$

Соответственно, совместное распределение вероятностей

$$P_{K_E K}(k_E, k) = P_K(k)\ \mathrm{Pr}_{K_E|K}(k_E|k) = \\ = P_{K_E}(k_E) \mathrm{Pr}_{K|K_E}(k|k_E). \tag{51}$$

Оказывается, что индивидуальные измерения являются не самыми оптимальными, коллективные измерения позволяют получать больше информации.

Неформально, количество битов информации, которых Еве не хватает после измерений для того, чтобы знать ключ Алисы–Боба, есть

$$H(K|K_E) = \sum_{k_E \in K_E} P_{K_E}(k_E) H(K|K_E = k_E) = \\ = -\sum_{k_E \in K_E} P_{K_E}(k_E) \sum_{k \in K} P_{K|K_E}(k|k_E) \times \\ \times \log(P_{K|K_E}(k|k_E)). \tag{52}$$

Далее кроме (52) удобно использовать выражение

$$H(K_E|K) = \sum_{k \in K} P_K(k) H(K_E|K = k) = \\ = -\sum_{k \in K} P_K(k) \sum_{k_E \in K_E} P_{K_E|K}(k_E|k) \times \\ \times \log(P_{K_E|K}(k_E|k)). \tag{53}$$

Количество информации в битах, которое может получить Ева в результате индивидуальных измерений в пересчете на один акт квантового распределения ключей, дается взаимной информацией:

$$I(K_E : K) = H(K) - H(K|K_E) = \\ = H(K_E) - H(K_E|K). \tag{54}$$

Формула (54) имеет простую интерпретацию. Полная размерность пространства ключей Алисы–Боба равна $2^{NH(K)}$. Ева может различить долю ключей из этого множества не более

$$2^{I(K_E:K)} = \frac{2^{NH(K)}}{2^{NH(K|K_E)}} = 2^{N(H(K)-H(K|K_E))}. \tag{55}$$

Результат (55) можно получить и несколько другими рассуждениями, которые используются для качественного вывода пропускной способности классического дискретного канала связи без памяти [16].

Подслушиватель после измерений «видит» наблюдение k_E — копию истинного ключа k. Количество типичных последовательностей копий ключей k_E у Евы — размерность пространства, есть

$$|K_E| = 2^{NH(K_E)}, \\ H(K_E) = -\sum_{k_E \in K_E} P_{K_E}(k_E) \log(P_{K_E}(k_E)). \tag{56}$$

Символически множество условно типичных последовательностей наблюдений Евы приведено на рис. 3. При каждом фиксированном значении истинного ключа k в N испытаниях возникает $2^{NH(K_E|K=k)}$ условно типичных последовательностей у Евы. Неформально говоря, при измерениях Евы над квантовым состоянием каждый ключ размазывается в множество размерности $2^{NH(K_E|K=k)}$.

С учетом того, что каждый ключ k возникает с вероятностью $P_K(k)$, среднее число условно типичных последовательностей становится равным $2^{NH(K_E|K)}$.

Различить истинные ключи k по результатам измерений Ева может, только если количество истинных ключей такое, что их образы в пространстве K_E не перекрываются (см. рис. 3). Каждому ключу k в среднем отвечает область размером $2^{NH(K_E|K)}$. Поэтому Ева может различить такую долю истинных ключей, для которой области в K_E не перекрываются (см. рис. 3 для качественного пояснения), имеем

$$\frac{2^{NH(K_E)}}{2^{NH(K_E|K)}} = 2^{NI(K_E:K)}. \tag{57}$$

Иными словами, равенство (57) означает следующее. У Алисы–Боба с вероятностью единица существует $2^{NH(K)}$ типичных последовательностей. Каждая последовательность Алисы–Боба переходит с

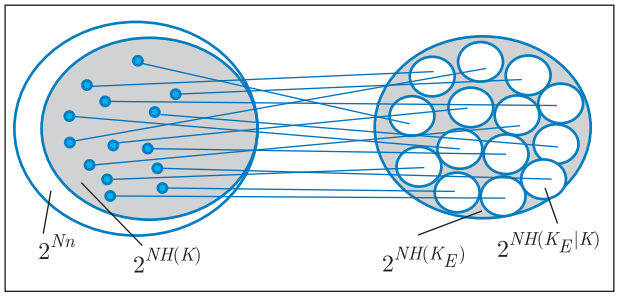

Рис. 3. Схематическое изображение множества ε-секретных ключей (жирные кружки в множестве типичных последовательностей ключей Алисы–Боба, левая половина), которые переходят в целые области размером $2^{NH(K_E|K)}$ (размер области условно-типичных последовательностей при измерениях Евы). Число ключей Алисы–Боба, которые может различить подслушиватель, определяется числом областей условно типичных последовательностей, которыми можно покрыть все пространство типичных последовательностей (размер области $2^{NH(K_E)}$) Евы без наложения

вероятностью единица в $2^{NH(K|K_E)}$ типичных последовательностей у Евы (см. рис. 3). Ева по своему измерению может отличить лишь ту долю типичных последовательностей Алисы–Боба, которые приводят к неперекрывающимся множествам у Евы (рис. 3). Эта доля как раз и равна

$$\frac{2^{NH(K)}}{2^{NH(K|K_E)}} = 2^{NI(K_E:K)}.$$

Если бы квантовые состояния Евы, привязанные к ключам Алисы–Боба после квантового распределения ключей, были бы известны явно, то в принципе (умозрительно) можно было бы построить индивидуальные измерения — операторно-значные меры в (48), (49), которые минимизируют ошибку различения ключей, т. е. минимизируют условную энтропию $H(K|K_E)$ в (52), имеющую смысл нехватки информации Евы о ключе, при условии наблюдения k_E. Длина ключа в битах для алгоритмов шифрования $n = 256$, поэтому измерение (48) имеет $2^{256} \approx$ $\approx 10^{77}$ исходов. То есть размерность ключевого пространства даже после одного акта квантового распределения ключей является запредельной, поэтому явно построить такие оптимальные измерения практически невозможно, даже если были бы явно известны сами матрицы плотности Евы в (47).

Однако матрицы плотности Евы явно неизвестны, известно только, что матрицы плотности в (47) ε-близки в смысле следового расстояния к матрицам плотности для идеальной ситуации. По этой причине не удается получить явную оценку сверху для взаимной информации $I(K_E : K)$ в (54) при индивидуальных измерениях через величину следового расстояния ε.

5.4. Коллективные измерения подслушивателя

Рассмотрим коллективные измерения Евы. Важно отметить, что коллективные измерения проводятся не над одним квантовым состоянием ρ_E^k после каждого акта распределения ключей, а над всей последовательностью из n квантовых состояний в каждой серии из N квантовых распределений ключей $\rho_E^{k_{1_1}} \otimes \rho_E^{k_{1_2}} \otimes \ldots \otimes \rho_E^{k_{1_N}}$ (см. (46)). Такие измерения называются коллективными. При таких измерениях Ева получает больше информации о передаваемых ключах.

Оказывается, что для коллективных измерений можно получить явную оценку фундаментальной верхней границы информации Евы, которая является фундаментальным пределом классической информации в битах, которую можно извлечь из квантового ансамбля. Данную границу можно выразить через величину следового расстояния (18) без явного знания матрицы плотности (47).

Как было видно выше на примере состояний Алисы–Боба (34), число типичных последовательностей определяется размерностью пространства, в которое вкладывается (35). Для этого, аналогично разделу выше, представим матрицу плотности (47) в диагональном виде:

$$\begin{gathered}\rho_E = \sum_{\lambda_i} P_\Lambda(\lambda_i)|\lambda_i\rangle_E{}_E\langle\lambda_i|, \\ {}_E\langle\lambda_i|\lambda_{i'}\rangle_E = \delta_{\lambda_i,\lambda_{i'}}, \quad \sum_{\lambda_i}\lambda_i = 1,\end{gathered} \tag{58}$$

где $P_\Lambda(\lambda) \geq 0$ — собственные числа матрицы плотности, $|\lambda_i\rangle_E$ — собственные векторы. Векторы, отвечающие различным собственным числам матрицы плотности (эрмитового положительного оператора), ортогональны. Поскольку след матрицы плотности равен единице, собственные числа в (47) имеют интерпретацию вероятностей.

После диагонализации матрицы плотности Евы приходим к предыдущей задаче, где вместо произведений ортогональных состояний $|K\rangle_K$ с вероятностями $P_K(k)$ фигурируют произведения ортогональных состояний $|\lambda\rangle_E$ с вероятностями $P_\Lambda(\lambda)$. Вероятность появления каждой типичной последовательности есть

$$P(n_{\lambda_1}, n_{\lambda_2}, \ldots, n_{\lambda_M}) = \\ = (P_\Lambda(\lambda_1))^{n_{\lambda_1}} (P_\Lambda(\lambda_2))^{n_{\lambda_2}} \ldots (P_\Lambda(\lambda_M))^{n_M}, \quad (59)$$

где n_{λ_i} — число вхождений состояния $|\lambda_i\rangle_E$ в последовательность длины N, M — число собственных векторов матрицы плотности. С учетом (58), (59) аналогично (37)–(42) получаем оценку для числа типичных последовательностей:

$$N_{Typ} = 2^{NH(\Lambda)}, \\ H(\Lambda) = -\sum_{\lambda\in\{\Lambda\}} P_\Lambda(\lambda)\log(P_\Lambda(\lambda)), \quad (60)$$

здесь $H(\Lambda)$ — энтропия фон Неймана,

$$H(\rho_E) = -\mathrm{Tr}\{\rho_E \log(\rho_E)\} = H(\Lambda) = \\ = -\sum_{\lambda\in\{\Lambda\}} P_\Lambda(\lambda)\log(P_\Lambda(\lambda)). \quad (61)$$

Таким образом, полная размерность пространства состояний у Евы есть $2^{NH(\Lambda)}$. Однако не все ортогональные состояния, на которые натянуто данное пространство, достоверно различимы в том смысле, что ключу отвечают не отдельные ортогональные векторы, а набор ортогональных векторов, которые возникают из данного ключа. Размер областей определяется при заданном k размером типичного пространства матрицы плотности ρ_E^k, привязанной к данному ключу, аналогично условно типичным последовательностям предыдущего раздела.

К каждому ключу привязана матрица плотности ρ_E^k, вероятность ключа k есть $P_K(k)$. Матрица плотности может быть представлена в диагональном виде:

$$\rho_E^k = \sum_{\mu_i^{(k)}} P_{\mu^{(k)}}(\mu_i^{(k)})|\mu_i^{(k)}\rangle_{E\,E}\langle\mu_i^{(k)}|, \\ {}_E\langle\mu_i^{(k)}|\mu_{i'}^{(k)}\rangle_E = \delta_{\mu_i^{(k)},\mu_{i'}^{(k)}}, \quad \sum_{\mu_i^{(k)}} P_{\mu^{(k)}}(\mu_i^{(k)}) = 1, \quad (62)$$

$$H(\rho_E^k) = -\sum_{\mu_i^{(k)}} P_{\mu^{(k)}}(\mu_i^{(k)})\log(P_{\mu^{(k)}}(\mu_i^{(k)})).$$

Матрица плотности каждого ключа, имеющего вероятность $P_K(k)$, имеет собственное пространство состояний, которое имеет размерность $2^{NP_K(k)H(\rho_E^k)}$. Данный результат получается следующими рассуждениями. В последовательности N испытаний матрица плотности для ключа k встречается с вероятностью $P_K(k)$. В полном пространстве с размерностью $2^{NH(\rho_E)}$ к каждому ключу привязана область размером $2^{NP_K(k)H(\rho_E^k)}$ (см. аналогичные рассуждения предыдущего раздела). Полное число областей, которые можно разместить в полном пространстве, равно $2^{N\sum_k P_K(k)H(\rho_E^k)}$. Поэтому из полного числа ключей будет различима доля

$$\frac{2^{NH(\rho_E)}}{2^{N\left(\sum_k P_K(k)H(\rho_E^k)\right)}} = 2^{N\chi(\mathcal{E})}, \quad (63)$$

где информация Холево [17–19]

$$\chi(\mathcal{E}) = H(\rho_E) - \sum_k P_K(k)H(\rho_E^k). \quad (64)$$

Применительно к нашему случаю информация Холево может быть интерпретирована следующим образом. Имеется классический источник ключей, который генерирует ключи в соответствии с распределением вероятностей $P_K(k)$. Вместо самих ключей в канал связи к Еве поступают квантовые состояния ρ_E^K. Фактически к Еве поступает квантовый ансамбль состояний $\mathcal{E} = \{P_K(k), \rho_E^k\}$.

Каждый ключ в среднем несет в себе информацию $n(1-2\varepsilon)$ битов. В результате измерений над квантовыми состояниями в среднем Ева может получить не более $\chi(\mathcal{E})$ битов информации о ключе. Как увидим ниже, данная информация не более $\chi(\mathcal{E}) < 2n\varepsilon$ битов, т. е. Ева при $\varepsilon \to 0$ знает не более $2n\varepsilon$ битов ключа.

5.5. Связь информации подслушивателя с пропускной способностью квантово-классического канала связи

Фактически Алиса–Боб и Ева находятся в ситуации квантово-классического канала связи. Интерпретация матрицы плотности (47) следующая. Имеется классический алфавит ключей с заданным над ним распределением вероятностей

$$k \in \mathcal{K} = \{0,1\}^n, \quad P_K(k), \quad (65)$$

Алиса–Боб генерируют ключи. К каждому ключу привязано состояние Евы. По сути, ситуация сводится к тому, что источник ключей используется многократно, N раз, т. е. посылает в канал связи к Еве не сами ключи (ортогональные — классические состояния, отвечающие ключам), а квантовые состояния ρ_E^k. Цель Евы, — проводя оптимальные измерения, узнать, какому ключу соответствует квантовое состояние.

Один из фундаментальных результатов квантовой теории информации — теорема Холево [17–19], прямая теорема кодирования, которая применительно к нашей ситуации квантового распределения ключей, гласит следующее. Пусть задан квантовый

ансамбль $\mathcal{E} = \{P_K(k), \rho_E^k\}$ — источник квантовых состояний, который используется многократно, N раз, существует набор кодовых слов — подмножество $k \in \mathcal{R} \in \mathcal{K}$ размером

$$N|R| \le N\chi(\mathcal{E}) = \\ = N\left(H(\rho_E) - \sum_{k\in\mathcal{K}} P_K(k)H(\rho_E^k)\right), \quad (66)$$

такой что для любого наперед заданного $\delta \to 0$, начиная с $N > N_\delta$, ошибка различения квантовых состояний, соответственно, ключей k из кодового набора, будет стремиться к нулю,

$$2^{\text{const}\cdot N(|R|-\chi(\mathcal{E}))} < \delta. \quad (67)$$

Обратная теорема кодирования [19, 20] гласит, что если набор кодовых слов — подмножество $k \in \mathcal{R} \in \in \mathcal{K}$, имеет размер

$$N|R| \ge N\chi(\mathcal{E}) = N(H(\rho_E) - \sum_{k\in\mathcal{K}} P_K(k)H(\rho_E^k)), \quad (68)$$

то вероятность ошибочного различения квантовых состояний как функция (68), соответственно, ключей k из кодового набора, будет стремиться к единице:

$$P_{Err}(N(|R| - \chi(\mathcal{E}))) \to 1. \quad (69)$$

Неформально, сказанное выше означает, что если источник посылает в канал связи число состояний ρ_E^K, которое превышает допустимую величину, определяемую фундаментальной границей Холево, то приемник не сможет различить квантовые состояния, соответственно информация приемника будет стремиться к нулю. Фактически величина Холево определяет число квантовых состояний, которые может различить приемник в асимптотическом пределе длинных последовательностей.

Применительно к квантовой криптографии, сказанное неформально означает следующее. Если источник посылает к Еве состояния всех ключей — размер кодового пространства равен размеру пространства всех ключей $|R| = |K| = 2^n$, и если величина Холево меньше, чем размер ключевого пространства, $2^{N\chi(\mathcal{E})} < |K|^N = 2^{Nn}$, то подслушиватель не сможет различить ключи. Однако для вычисления величины Холево в (64) требуется явно знать матрицы плотности квантовых состояний — квантовый ансамбль.

В квантовой криптографии квантовый ансамбль — матрицы плотности и распределения вероятностей самих ключей, явно неизвестны. Известна только некоторая интегральная характеристика квантового ансамбля — следовое расстояние до идеальной ситуации. Дальнейшей нашей задачей будет нахождение оценки для верхней границы информации Холево, которая должна выражаться через следовое расстояние, фигурирующее в критерии секретности (18).

Информация Холево связана с пропускной способностью квантово-классического канала связи [17–19]. Подслушиватель и Алиса находятся в следующей ситуации. Классическая информация — ключ, генерируемый источником, поступает к Еве в виде квантовых состояний — матриц плотности без искажений. В этом смысле квантово-классический канал Алиса–Ева является идеальным. Говоря более неформально, классическая информация, генерируемая классическим источником (Алисой), в пересчете на один акт квантового распределения ключей есть $H(K) \ge n(1 - 2\varepsilon)$ битов (см. формулы (44), (45)). Из этой информации подслушиватель, имея доступ только к квантовым состояниям, может знать не более $\chi(\mathcal{E})$ битов. Иначе говоря, через такой квантово-классический канал безошибочно в асимптотическом пределе можно передать не более $\chi(\mathcal{E})$ битов информации. Фактически величина Холево совпадает с классической пропускной способностью такого квантово-классического канала связи. Величина Холево, соответственно, пропускная способность такого канала связи, достижима на коллективных измерениях [17–19]. Количество информации, которое подслушиватель может получить при индивидуальных измерениях, ограничена так называемой пропускной способностью за один шаг (one shot capacity) [18, 19], которая меньше, чем классическая пропускная способность квантово-классического канала связи [18, 19].

Для того чтобы знать величину Холево — верхнюю границу информации, которую может получить подслушиватель, необходимо явно знать квантовый ансамбль – полную и частичные матрицы плотности (47), (64), а также вероятности, с которыми матрицы плотности генерируются. Максимум, что позволяют получить достаточно сложные доказательства секретности ключей в квантовой криптографии, это тот факт, что следовое расстояние между реальной и идеальной ситуациями не превышает величины ε. Удивительным свойством следового расстояния является то, что можно получить верхнюю границу величины Холево через величину следового расстояния.

5.6. Связь следового расстояния с фундаментальной границей Холево

В этом разделе получим связь информации Холево со следовым расстоянием. Будет показано, что верхняя граница информации Холево не превышает величины следового расстояния. Это будет означать, что чем меньше ε — расстояние до идеальной ситуации, тем меньше информации о ключах может получить Ева. При идеальной ситуации ($\varepsilon = 0$) ключи строго равновероятны, а квантовые состояния Евы некоррелированы с ключами, информация Евы о ключах строго равна нулю. В этом случае вероятность знать любой ключ для Евы равна вероятности простого угадывания, и это наихудший вариант.

Покажем, что следовое расстояние мажорирует информацию Холево, $\chi(\mathcal{E}) < 2\varepsilon n$. Из этого факта будет следовать, что из полного числа типичных последовательностей ключей $2^{Nn(1-2\varepsilon)}$ подслушиватель сможет различить не более $2^{Nn2\varepsilon}$ битовых последовательностей, т. е. лишь их экспоненциально малую долю $2^{-Nn(1-4\varepsilon)}$ по длине полной битовой последовательности для всех N сеансов квантового распределения ключей.

Нам потребуется несколько вспомогательных величин, связанных с асимметричной относительной квантовой энтропией (см. детали в [21, 22]). Введем отображение для положительных операторов $\Lambda_\rho(\sigma)$:

$$\Lambda_\rho(\sigma) = \frac{d}{dt}\log(\rho+\sigma t)|_{t=0} = \\ = \int\limits_0^\infty ds(\rho+sI)^{-1}\sigma(\rho+sI)^{-1}, \quad \Lambda_\rho(\rho) = I, \quad (70)$$

производная понимается в смысле Фреше. Используя (70), определим полуторалинейную форму, которая может рассматриваться как метрика

$$M_\rho(\sigma,\tau) = \mathrm{Tr}\{\sigma\Lambda_\rho(\tau)\}, \quad M_\rho(\sigma,\sigma) \geq 0. \quad (71)$$

Дифференциал от асимметричной относительной энтропии выразим через (71):

$$D_\alpha(\rho||\sigma) = \alpha\mathrm{Tr}\{\rho\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\rho-\sigma)\} = \\ = -\alpha\frac{d}{d\alpha}H(\rho||\alpha\rho+(1-\alpha)\sigma), \quad (72)$$

здесь относительная энтропия $H(\rho||\sigma)$ и асимметричная энтропия $S_\alpha(\rho||\sigma)$ соответственно

$$H(\rho||\sigma) = \mathrm{Tr}\{\rho(\log(\rho)-\log(\sigma))\}, \quad (73)$$

$$H_\alpha(\rho||\sigma) = -\frac{1}{\log(\alpha)}H(\rho||\alpha\rho+(1-\alpha)\sigma).$$

В отличие от относительной энтропии, асимметричная энтропия является непрерывной и связана с дифференциалом (72):

$$H_\alpha(\rho||\sigma) = -\frac{1}{\log(\alpha)}\times \\ \times \int\limits_0^{-\log(\alpha)} D_\alpha(\rho||\sigma)d(-\log(\alpha')). \quad (74)$$

С учетом (70), (74), дифференциальная энтропия ограничивается сверху следовым расстоянием:

$$D_\alpha(\rho||\sigma) = \alpha\mathrm{Tr}\{\rho\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\rho-\sigma)\} = \\ = \alpha\mathrm{Tr}\{(\rho-\sigma)\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\rho)\} \leq \\ \leq \alpha\mathrm{Tr}\{(\rho-\sigma)_+\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\rho)\} \leq \\ \leq \alpha\mathrm{Tr}\{(\rho-\sigma)_+\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\alpha\rho+(1-\alpha)\sigma)\} = \\ = \mathrm{Tr}\{(\rho-\sigma)_+\} = \delta(\rho,\sigma), \quad (75)$$

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 [17–19] имеет вид

$$\chi(\mathcal{E}) = H(\rho_E) - \sum_{k\in K}P_K(k)H(\rho_E^k), \quad (76)$$

$$\rho_E = \sum_{k\in K}P_K(k)\rho_E^k.$$

Окончательно для величины Холево (76) находим

$$\chi(\mathcal{E}) = \sum_{k\in K}P_K(k)H(\rho_E^k||\rho_E) = \\ = -\sum_{k\in K}P_K(k)\log(P_K(k))H_{P_K(k)}(\rho_E^k||\rho_E^k) \leq \\ \leq -\sum_{k\in K}P_K(k)\log(P_K(k))\delta(\rho_E^k,\rho_E^k) \leq \\ \leq -\sum_{k\in K}P_K(k)\log(P_K(k))\times \\ \times \sum_{k\neq k'\in K}\frac{P_K(k')}{1-P_K(k)}\delta(\rho_E^k,\rho_E^{k'}). \quad (77)$$

Последнее слагаемое в цепочке неравенств (77) мажорируется следовым расстоянием (18):

$$\frac{1}{2}\sum_{k\neq k'\in K}\frac{P_K(k')}{1-P_K(k)}|\rho_E^k-\rho_E^{k'}|\leq$$
$$\leq\frac{1}{2}\sum_{k\neq k'\in K}\frac{1}{1-P_K(k)}\times$$
$$\times\Big(|P_K(k')\rho_E^{k'}-P_K(k)\rho_E^k|+|\rho_E^k(P_K(k')-P_K(k))|\Big)\leq$$
$$\leq\frac{1}{2}\sum_{k\in K}\frac{2}{1-P_K(k)}\times$$
$$\times\left(|\frac{\rho_E}{2^n}-P_K(k)\rho_E^k|+|\rho_E^k||P_K(k)-\frac{1}{2^n}|\right). \quad (78)$$

Вычисляя след от (78) и учитывая, что максимальная вероятность не превышает $\max_{k\in K}P_K(k) < < 1/2^n+\varepsilon$, получаем

$$\sum_{k\in K}\mathrm{Tr}\left\{\left|\frac{\rho_E}{2^n}-P_K(k)\rho_E^k\right|\right\}+\left\|P_K-\frac{1}{2^n}\right\|_1<2\varepsilon. \quad (79)$$

В итоге фундаментальная информация Холево ограничена сверху энтропией Шеннона:

$$\chi(\mathcal{E})<2\varepsilon n. \quad (80)$$

Таким образом, имея интегральную характеристику следовое расстояние и не зная явно квантового ансамбля Евы, можно получить оценку для верхней границы информации Холево — неформально, числа битов, которое Ева может получить из своего квантового ансамбля, коррелированного с ключами Алисы–Боба.

6. ЗАКЛЮЧЕНИЕ

Кратко сформулируем полученные результаты. Конечным «продуктом» работы систем квантовой криптографии является общий секрет у двух пространственно-удаленных легитимных пользователей. Общий секрет — секретный ключ, т. е. случайная битовая строка 0 и 1, которая может использоваться для различных криптографических протоколов защиты информации. Общий секретный ключ является наиболее сильным криптографическим примитивом. Данный секрет возникает из более слабых криптографических примитивов: аутентичного, не секретного и доступного для прослушивания классического канала связи, а также квантового канала связи, который также доступен для прослушивания и возможной произвольной модификации нарушителем. Аутентичность является более слабым криптографическим примитивом, чем общий секретный ключ. Квантовая криптография из более слабого криптографического примитива — аутентичности, и передачи квантовых состояний позволяет получить самый сильный криптографический примитив — общий секретный ключ. В этом смысле квантовая криптография решает упомянутую во Введении “Chicken and Egg Problem”.

Ключ — это информация, известная только Алисе и Бобу. Если бы ключ был истинно случайным, то общая секретная информация Алисы–Боба была бы n битов (n — длина ключа). В реальности общая секретная информация в битах Алисы и Боба, как было показано выше, составляет $n(1-2\varepsilon)$ битов. Типичные значения ε составляют 10^{-9}. Параметр секретности ε может быть выбран сколь угодно малым, что достигается сжатием очищенного ключа. Естественно, уменьшение ε требует очищенного ключа большей длины, причем увеличение длины очищенного ключа, который требуется для достижения заданного ε, растет лишь как $\log(1/\varepsilon)$.

Критерий секретности, основанный на следовом расстоянии, позволяет получить простыми соображениями верхнюю границу информации о ключе, которую имеет подслушиватель. Данная информация составляет не более $2n\varepsilon$ битов. Грубо говоря, подслушиватель из каждой позиции секретного ключа знает информацию не более

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

битов.

Если бы ключи были идеальными — равновероятно распределенными, то общее число секретных битов в ключе было бы n. Но ключи не вполне идеальны — отстоят в смысле следового расстояния от равномерного распределения не более, чем на ε, поэтому число истинно случайных битов не менее $n(1-2\varepsilon)$. Если бы подслушиватель не имел в своем распоряжении квантовых состояний, коррелированных с ключом, то информация подслушивателя о ключе была бы 0 битов. Все $n(1-2\varepsilon)$ битов Алисы–Боба были бы секретными. Из квантовых состояний Ева может получить не более $2n\varepsilon$ битов информации. В итоге общий секрет Алисы–Боба оказывается не менее $n(1-4\varepsilon)$ битов.

На языке размерности полного пространства ключей подслушиватель в среднем в каждом испытании знает, т. е. потенциально может различить, лишь экспоненциально малую долю полного ключевого пространства

$$2^{-n(1-4\varepsilon)}.$$

Данный результат можно перефразировать следующим образом. Для идеальных равновероятных клю-

чей, никак не коррелированных с квантовыми состояниями Евы, максимум, что может делать Ева, это угадывать ключ. Вероятность угадать ключ есть 2^{-n}. Если ключи не строго равновероятно распределены — неформально говоря, содержат меньше случайности, чем идеальные, то вероятность угадать ключ, в меру ε, становится несколько больше $2^{-n(1-2\varepsilon)}$. Если дополнительно в распоряжении Евы имеются квантовые состояния, коррелированные с ключами, то вероятность «угадать» ключ, опять в меру ε, становится не больше $2^{-n(1-4\varepsilon)}$.

Отметим, что обратная величина параметра секретности $(1/\varepsilon)$ определяет число шифр-сообщений до первого дешифрования — до первого прочтения сообщения — взлома системы (см. детали в [8]). Этот результат получается более изощренными математическими средствами, чем представленный выше качественный анализ.

Таким образом, минимальными математическими средствами дана интуитивно прозрачная физическая интерпретация критерия секретности ключей в квантовой криптографии. Данная интерпретация позволяет придать простой теоретико-информационный смысл параметру секретности ε.

Благодарности. Автор выражает благодарность коллегам по Академии криптографии Российской Федерации за обсуждения и поддержку. Автор благодарит также И. М. Арбекова, С. П. Кулика за интересные обсуждения и замечания.

ЛИТЕРАТУРА

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

2. В. А. Котельников, *Отчет*, 19 июня (1949).

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

4. J. M. Renes and Jean-C. Boileau, Phys. Rev. Lett. **103**, 020402 (2009).

5. M. Tomamichel, Ch. Ci Wen Lim, N. Gisin, and R. Renner, arXiv:1103.4130 v2; Nature Comm. **3**, 1 (2012).

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

7. 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].

8. И. М. Арбеков, С. Н. Молотков, ЖЭТФ **152**, 62 (2017) [I. M. Arbekov and S. N. Molotkov, JETP **125**, 50 (2017)].

9. K. Kraus, *States, Effects and Operations*: *Fundamental Notions of Quantum Theory*, Springer Verlag (1983).

10. W. F. Stinespring, Proc. Amer. Math. Soc. **6**, 211 (1955).

11. L. Carter and M. N. Wegman, J. Comp. System Sci. **18**, 143 (1979).

12. С. Н. Молотков, ЖЭТФ **157**, 963 (2020).

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

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

15. J. L. Massey, IEEE Int. Symp. Inform. Theory, 204 (1994).

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

17. А. С. Холево, Пробл. передачи информ. **9**, 3 (1973).

18. A. S. Holevo, Russ. Math. Surveys **53**, 1295 (1998).

19. А. С. Холево, *Квантовые системы, каналы, информация*, МЦНМО (2010).

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

21. K. M. R. Audenaert, J. Math. Phys. **54**, 073506 (2013).

22. K. M. R. Audenaert, J. Math. Phys. **55**, 112202 (2014).