Октябрь 2025 г. *Том 195, № 10*

УСПЕХИ ФИЗИЧЕСКИХ НАУК

МЕЖДУНАРОДНЫЙ ГОД КВАНТОВЫХ НАУК И ТЕХНОЛОГИЙ

ОБЗОРЫ АКТУАЛЬНЫХ ПРОБЛЕМ

Одноразовый блокнот Вернама, Котельникова, Шеннона и квантовая криптография

И.М. Арбеков, С.Н. Молотков

Квантовая криптография — квантовое распределение ключей (КРК) — одно из первых направлений квантовой теории информации, которое достигло зрелого научного уровня и было доведено до коммерческих систем в области защищённой квантовой связи. Проблема распределения ключей является центральной проблемой симметричной криптографии. Квантовая криптография решает эту проблему, причём решение базируется на фундаментальных законах Природы — законах квантовой механики. Квантовое распределение ключей, по сути, представляет собой согласование двух независимых случайных последовательностей на передающей и приёмной сторонах посредством посылки квантовых состояний. Кроме квантового канала необходим ещё аутентичный классический канал связи. Оба канала связи являются открытыми и доступными для вторжения нарушителя. Для обеспечения аутентичности классического канала при первом запуске системы необходим стартовый ключ, используемый для обеспечения теоретико-информационной аутентификации. По сути, системы квантовой криптографии являются системами расширения этого стартового ключа. В последующих сеансах возникает квантовый ключ, часть которого используется для аутентификации, а другая часть — для других криптографических целей, например шифрования. Принципиальный для квантовой криптографии вопрос — сколько сеансов квантового распределения ключей с момента первого запуска системы можно проводить до нового перезапуска системы, когда криптографические свойства квантовых ключей достигнут критического уровня, после которого их уже нельзя будет использовать для криптографических целей и потребуется новый перезапуск системы. Несмотря на существующий ряд обзоров по тематике квантовой криптографии, данный вопрос детально не обсуждался. Показано, что для реальных, достижимых на сегодняшний день параметров систем квантовой криптографии, возможна практически сколь угодно долгая работа системы КРК до следующего перезапуска. Это означает, что системы КРК могут обеспечить реализацию "одноразового блокнота" — множества одноразовых ключей, используя только один стартовый ключ. Представлен также краткий исторический экскурс, в котором излагаются отдельные факты, мало известные широкой аудитории. Обзор ориентирован на широкую аудиторию, доступен студентам старших курсов и аспирантам, прослушавшим университетские лекционные курсы по квантовой информатике, и, как надеются авторы, его содержание позволит глубже понять "криптографическую начинку" современных систем квантового распределения ключей.

Ключевые слова: квантовая криптография, одноразовый блокнот, безопасная связь, аутентификация

PACS numbers: 03.67.Dd, 03.67.Hk, **89.70.–a** DOI: https://doi.org/10.3367/UFNr.2025.07.039972

И.М. Арбеков [(1,*)], **С.Н. Молотков** [(1,2,3,4,†)]
[(1)] Академия криптографии Российской Федерации, 119331 Москва, а/я 100, Российская Федерация
[(2)] Институт физики твёрдого тела имени Ю.А. Осипьяна РАН, ул. Академика Осипьяна 2, 142432 Черноголовка, Московская обл., Российская Федерация
[(3)] Московский государственный университет им. М.В. Ломоносова, факультет вычислительной математики и кибернетики, Ленинские горы 1, стр. 52, 119991 Москва, Российская Федерация
[(4)] Центр квантовых технологий, Московский государственный университет им. М.В. Ломоносова, Ленинские горы 1, стр. 35, 119991 Москва, Российская Федерация
E-mail: [(*)] arbekov53@mail.ru, [(†)] molotkov@issp.ac.ru

Статья поступила 13 января 2025 г., после доработки 28 июля 2025 г.

Содержание

1. Введение, краткая история вопроса

Лет 30 назад термин криптография практически отсутствовал в открытой печати. Криптография, понимаемая как защита информации, была областью деятельности отдельных специализированных организаций. В настоящее время криптография является атрибутом повседневной жизни и касается каждого человека, даже если он по своей профессиональной деятельности далёк от данной области. Компьютерные пароли, PIN-коды смарт-карт и других электронных устройств, банковские транзакции, криптовалюта, цифровая подпись, блокчейн, распределённые базы данных, дистанционное голосование, интернет-технологии и многое другое — за всем этим стоит серьёзная наука, связанная с защитой информации. Практически в любом высшем образовательном учреждении существуют программы по подготовке специалистов в области информационной безопасности.

Квантовая криптография [1], синоним квантового распределения ключей (КРК), является активно развивающейся областью квантовой информатики. В данной области существуют не только отдельные экспериментальные прототипы систем КРК, но и в разных странах созданы целые сети с квантовым распределением ключей [2–4]. Продемонстрировано распределение ключей через спутники [2]. В России университетская квантовая сеть — сеть квантовой телефонии [4] — была запущена в 2021 г., это совместная разработка российской IT-компании ИнфоТеКС и Центра квантовых технологий Московского государственного университета им. М.В. Ломоносова (МГУ).

К настоящему времени существует несколько обзоров [5–9], посвящённых различным аспектам систем КРК. Квантовая криптография в момент своего появления позиционировалась как метод, обеспечивающий *безусловную секретность* (unconditional security). Под безусловной секретностью понимается секретность ключей, которая основывается на фундаментальных законах Природы — квантовой физики, а не на предположениях об ограниченных вычислительных и технических возможностях нарушителя. Данное понятие неоднократно использовалось как в публикациях популярного характера, так и в сугубо научных статьях. Однако подробности того, что стоит за данным термином до сих пор в концентрированном виде в рамках одного обзора не были изложены. Поскольку системы КРК являются элементом реальности сегодняшнего времени, то ознакомление широкой аудитории с тем, что на самом деле стоит за данными понятиями *секретности*, на наш взгляд, требует отдельного подробного рассмотрения в одном месте.

Развитие идей в любой научной области можно понять только в контексте логики исторических событий, поэтому для полноты изложения имеет смысл проследить за событиями, которые привели к возникновению квантовой криптографии, и, в более широком смысле, квантовых коммуникаций.

История криптографии является столь же древней, как и история человечества. Упоминания о криптографии встречаются уже у древних египтян, которые для передачи секретного сообщения использовали наколки на голове раба, скрытые под волосами [1]. С давних времён известны, например, такие шифры, как шифр Цезаря, шифр Древней Спарты *сциталла*. Различные исторические примеры шифров, а также способов их взлома приведены в ряде известных монографий [10, 11]. История шифровального дела в России от древних славян до середины XX столетия описана в книге [12]. Методы криптографического анализа, хотя они и не назывались таковыми, помогли прочитать древние тексты, написанные на трёх архаичных языках на знаменитом Розеттском камне, который был обнаружен в 1799 г. в хорошо сохранившемся состоянии во время вторжения Наполеона в Египет [13].

В этих исторических примерах есть общий элемент — изначальный общий *секрет*, который знают отправитель и получатель зашифрованного сообщения и который обеспечивает защиту передаваемого сообщения. В шифре Цезаря таким общим секретом — секретным ключом — является сдвиг в алфавите, используемый для замены букв, в шифре сциталлы общим секретом будут размеры жезла (сциталлы), на который наматывается лента для нанесения вдоль жезла передаваемого сообщения.

Криптографию, которая использует общий секрет (ключ), известный только отправителю и получателю, принято называть симметричной криптографией. Для симметричной криптографии требуется, чтобы легитимные участники обмена информацией, обычно называемые Алисой и Бобом, исходно имели общий секрет — секретный ключ. В современных условиях секретный ключ — это случайная битовая строка 0 и 1, известная только Алисе и Бобу. Генерация случайных чисел играет принципиальную роль для любой системы криптографии. Для систем квантовой криптографии используются физические квантовые генераторы случайных чисел. Случайная битовая строка 0 и 1 — секретный ключ — позволяет Алисе зашифровать своё сообщение, а Бобу, при наличии идентичного с Алисой секретного ключа, расшифровать передаваемое сообщение. Кстати, о терминологии. Часто, особенно в разных блогах в интернете, говорят "дешифровать" вместо "расшифровать". Дешифрование — взлом шифра, это нелигитимная проце-

[1] Хотя, по современной терминологии, такое сокрытие информации относится к стеганографии — сокрытию секретной информации среди открытой информации, например, в отдельных пикселях картинки.

дура, которую осуществляет злоумышленник, не знающий секретного ключа.

В этом месте возникает принципиальный вопрос о стойкости шифра. Пусть ключ секретен, тогда может ли злоумышленник, не имея секретного ключа, взломать шифр — прочитать сообщение. Иначе говоря, существуют ли способы шифрования с секретным ключом, которые в принципе нельзя взломать? Это принципиальный вопрос для криптографии, ответ на который совсем не очевиден.

Даже великие учёные заблуждались при попытке ответить на данный вопрос. Например, шифр простой замены состоит в том, что каждая буква открытого текста заменяется некоторым символом. Такой шифр является слабым, поскольку частота появления букв в тексте разная, соответственно частота появления символов замены сохраняется. Великий математик Карл Фридрих Гаусс считал, что если каждую букву открытого текста заменять на случайно выбираемый символ из группы символов алфавита шифра, причём количество заменяющих символов для одной буквы сделать пропорциональным частоте встречаемости этой буквы, то такой шифр взломать нельзя. Однако это не спасает ситуацию, шифр остаётся слабым. Заблуждения гениев очень поучительны. Гаусс не сделал ещё одного, последнего, шага — может быть, надо заменять в каждом сообщении все буквы открытого текста каждый раз новыми случайными символами? Потребовалось более 100 лет, чтобы довести эту идею в XX веке до логического завершения и сделать финальный шаг — предъявить систему шифрования, которую нельзя дешифровать (взломать) даже теоретически.

В научном сообществе принято считать, что исторически первым данную идею высказал Гильберт Вернам (G.S. Vernam), который был сотрудником Bell Telephone Laboratories (США). Совместный патент Вернама и майора Моборна (Joseph O. Mauborgne), сотрудника U.S. Army Signal Corps., датирован 1918 г. Работа Вернама опубликована в 1926 г. [14]. Вернам разработал телетайп, в котором буквы открытого текста преобразовывались в соответствии с кодом Бодо (Baudot) — каждой букве сопоставлялась комбинация из пяти значений 0 и 1 (битов). Битовый открытый текст зашифровывался на ключе — случайной битовой последовательности — операцией XOR (сложение по модулю 2). В исходной версии ключ был записан на замкнутую ленту, поэтому через определённое число символов текста ключ повторялся. Данная работа выполнялась в интересах U.S. Army Signal Corps. Представитель заказчика Моборн заметил, что такая система шифрования, из-за повторения ключей шифрования, не будет абсолютно стойкой, и предложил заменить ключи бесконечной бегущей лентой со случайными битами. В работе [14] утверждалось, правда без каких-либо математических обоснований, что системы шифрования с бегущим случайным ключом (running key) будут абсолютно недешифруемыми:

"*If, now, instead of using English words or sentences, we employ a key composed of letters selected absolutely at random, a cipher system is produced which is absolutely unbreakable*".

Новые научные идеи в любой области не возникают одномоментно. Вопрос о том, кто первый озвучил идею *одноразового блокнота* — идею шифрованием одноразовой битовой последовательностью — не оставляет в покое исследователей вплоть до последнего времени. По-видимому, последнее историческое исследование приведено в работе [15]. Автор данной работы "докопался" до архивных материалов, на основании которых утверждается, что идея шифрования одноразовым блокнотом была высказана Фрэнком Миллером (Frank Miller) — банкиром из Калифорнии почти за 35 лет до патента Г. Вернама и Дж. Моборна в публикации *Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams*:

"*A banker in the West should prepare a list of irregular numbers, to be called 'shift-numbers', such as 483, 281, 175, 892, etc.*"

"*The differences between such numbers must not be regular.*"

"*When a shift-number has been applied, or used, it must be erased from the list and not used again.*"

"*A copy of the list is to be sent to the New York Banker, who prepares a different list and sends copy thereof to the Western Banker.*"

Миллер осознавал, что необходимо одноразовое использование ключей:

"*Any system which allows a cipher word to be used twice with the same signification is open to detection. A little talk with a telegraph operator will convince one of this fact.*"

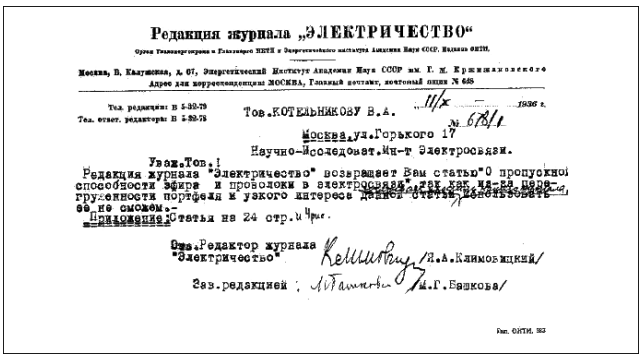
В упомянутой работе также обсуждается вопрос, со ссылкой на архивные документы, о том, мог ли Моборн знать об идее Миллера.

Следующий шаг с простым доказательством абсолютной стойкости способа шифрования с секретными одноразовыми ключами (который в общем случае можно понимать как суммирование со случайными числами по любому модулю) был независимо сделан нашим выдающимся соотечественником академиком АН СССР Владимиром Александровичем Котельниковым. Закрытый отчёт, датированный 19 июня 1941 г., состоял из нескольких страниц машинописного текста [16]. Гриф секретности с данного отчёта был снят более 30 лет назад, однако отчёт до сих пор не известен широкой научной общественности (см. детали в [17]). Важно, что советские криптографы независимо от своих западных коллег имели представление о секретности такого способа шифрования.

Не нужно путать отчёт [16] с другой широко известной работой В.А. Котельникова 1932 г. под названием "О пропускной способности "эфира" и проволоки в электросвязи", в которой была доказана знаменитая *теорема об отсчётах* и которая положила начало цифровой эпохе [18]. Идеи работы сильно опережали своё время. Содержание этой теоремы излагается в любом учебнике, но в виде журнальной статьи работы не существует, поскольку она была отклонена редакцией журнала как не представляющая научного интереса. Поскольку информация в истории никуда не пропадает, интересно привести ответ редакции на представленную работу (рис. 1).

Несмотря на это, приоритет В.А. Котельникова в доказательстве теоремы отсчётов спустя много лет был признан мировым научным сообществом [19].

Следующий шаг с полным математическим доказательством секретности одноразового блокнота методами современной классической теории информации был сделан в работе Клода Элвуда Шеннона (C.E. Shannon) "Communication Theory of Secrecy Systems" [20]. Работа



Редакция журнала „ЭЛЕКТРИЧЕСТВО"

Москва, В. Кадашевская, д. 27, Энергетический Институт Академии Наук СССР им. Г. М. Кржижановского
Адрес для корреспонденции: МОСКВА, Главный почтамт, почтовый ящик № 648

Тел. редакции: Б 3-30-79
Тел. ответ. редактора: Б 3-30-78

Тов. КОТЕЛЬНИКОВУ В.А. 11/X 1936 г.
№ 678/1
Москва, ул. Горького 17
Научно-Исследоват. Ин-т Электросвязи.

Уваж. Тов.!
Редакция журнала "Электричество" возвращает Вам статью "О пропускной способности эфира и проволоки в электросвязи", так как из-за перегруженности портфеля и узкого интереса данной статьи удовлетворить ее не сможем.
Приложение: Статья на 24 стр. и 4 рис.

Отв. Редактор журнала "Электричество" /В.А. Климовицкий/
Зав. редакцией /М.Г. Башкова/

Тип. ОНТИ. 353

Рис. 1. Отказ редакции в публикации работы В.А. Котельникова, в которой была доказана знаменитая теорема об отсчётах, положившая начало цифровой эры.

была выполнена в лаборатории Bell Labs (США) в 1945 г. и рассекречена в 1948 г. Некоторые американские криптографы считают, что это было сделано ошибочно, по недосмотру (см. замечание У. Диффи в предисловии к монографии Брюса Шнайера *Прикладная криптография* [21]). После данной работы Шеннона такой способ получил название "шифрование с одноразовыми ключами" — *one time pad* — шифрование в режиме одноразового блокнота. Благодаря работам Котельникова и Шеннона возникло чёткое понимание, каким свойствам должен удовлетворять совершенный шифр, а именно:

— ключ должен быть случайным,

— длина ключа в битах должна быть не меньше длины сообщения,

— ключ должен использоваться только один раз.

Понятие *совершенной секретности* криптосистемы вводится в рамках теоретико-вероятностной модели, связывающей между собой открытые сообщения $m \in M$, ключи $k \in K$ и шифрованные сообщения $c \in C$ в виде совместного распределения $P(m,k,c)$. Для совершенной секретности требуется, чтобы апостериорные вероятности открытых сообщений, полученных после перехвата шифр-сообщения, были равны априорным вероятностям тех же сообщений до перехвата. Несложно проверить выполнение свойства *совершенной секретности* для криптосистемы, в которой:

— открытое сообщение m и ключ k являются двоичными последовательностями длины N,

— шифр-сообщение $c = m \oplus k$ — сумма по модулю 2 двоичных знаков открытого сообщения и ключа,

— ключ выбирается случайно и равновероятно из всего пространства двоичных последовательностей длины N.

Тогда условная вероятность

$$P(m|c) = \frac{P(m)P(c|m)}{P(c)} = \frac{P(m)\ \Pr\{k : m \oplus k = c\}}{\sum_{m'} P(m')\ \Pr\{k : m' \oplus k = c\}} = \\ = \frac{P(m)2^{-N}}{2^{-N}\sum_{m'} P(m')} = P(m)\,.$$

Здесь необходимо сделать комментарий, что понимается под "открытым" сообщением. Поскольку любой язык имеет избыточность, то обычно на практике для текстовых сообщений предварительно используется сжатие сообщений, для того чтобы приблизить сжатый текст к случайной битовой последовательности. Если речь идёт о продвижении, например, внешнего ключа по квантовой сети с шифрованием на ключах, полученных в КРК, то под "открытым" сообщением понимается внешний ключ — случайная битовая строка. Случайную битовую строку уже не требуется сжимать.

Резюмируем. Системы шифрования, которые невозможно взломать даже теоретически, существуют. Что нужно для реализации таких систем?

1. Нужен общий секретный ключ – случайная битовая строка 0 и 1 у Алисы и Боба.

2. Длина ключа — число битовых позиций 0 и 1 — должна быть не меньше длины отрытого сообщения — числа позиций текста в виде 0 и 1.

3. Ключ используется только один раз, на каждое новое сообщение нужен новый ключ.

4. Зашифрование происходит побитовым сложением по модулю 2 позиций текста с позициями ключа — возникает зашифрованный текст — битовая строка 0 и 1.

Расшифрование, производится аналогично побитовым сложением по модулю 2 позиций шифр-текста с позициями ключа на приёмной стороне. В образовательных целях интересно привести фото первого аппарата, который использовал *бегущие ключи* (рис. 2).

На рисунке 3 приведён исторический пример того, как выглядел одноразовый блокнот в середине XX века.

По утверждению [22], применялось двухстадийное шифрование.

На первой стадии использовалась кодовая книга-словарь, когда каждому слову в сообщении была сопоставлена группа из четырёх цифр, не зависимых от одноразового блокнота (см. табл. 1, кодовая книга-словарь).

Например:

1. Пусть открытый текст такой:

konheim delivered report about rockets.

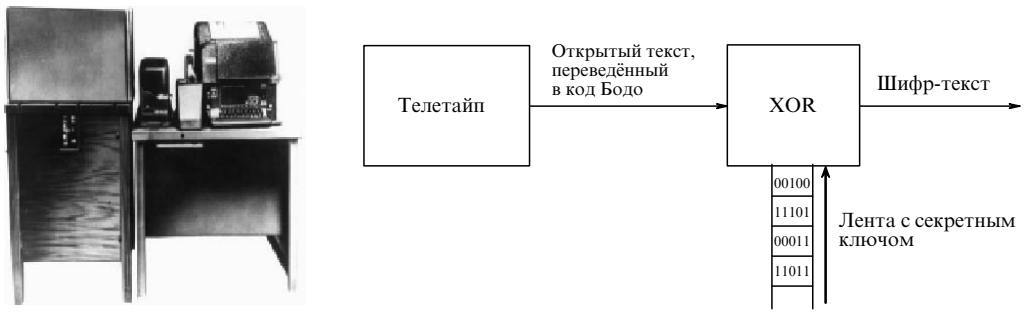


Рис. 2. Полиалфавитный телетайп Вернама с "бегущими ключами". Хранится в Агентстве национальной безопасности США [22].

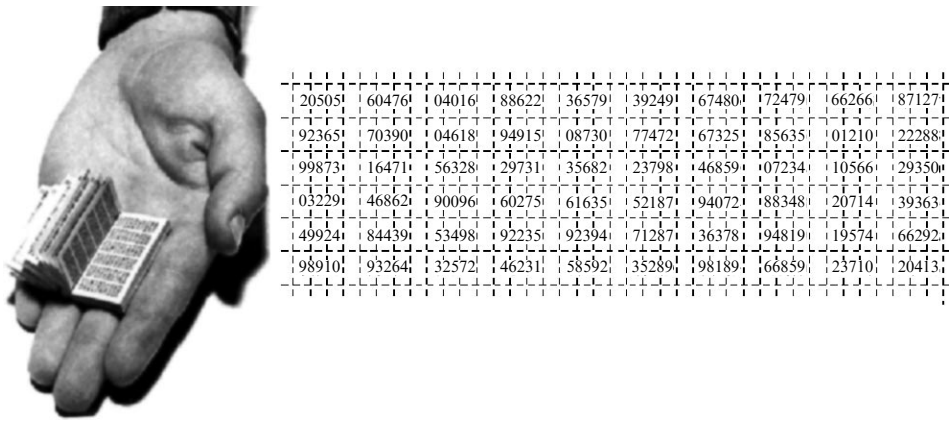


Рис. 3. Одноразовый блокнот легендарного советского разведчика Рудольфа Ивановича Абеля (Уильяма Фишера), захваченный ФБР 21 июня 1957 г. в результате предательства. Блокнот состоял из страниц с 60 блоками из пяти десятичных цифр. Хранится в Агентстве национальной безопасности США [22]. Способ генерации случайных чисел никогда не был приведён в открытой литературе.

Таблица 1

Слово открытого текста	Кодовая комбинация цифр
Conact	7652
...	...
endspell	1653
...	...
pay	6781
...	...
spell	5411

2. Часть "подозрительных слов" (rockets) открытого текста заменяется другими "неподозрительными словами" (grades):

teacher delivered report about grades.

Например, Юлиус Розенберг и его супруга Этель (Julius Rosenberg, Ethel Rosenberg) обозначались кодовым словом — LIBERAL. Атомная бомба — ENORMOZ.

3. Слова в изменённом открытом тексте заменялись группой из четырёх цифр из кодовой книги-словаря:

7394 2157 1139 3872 2216

4. Кодовые группы из четырёх цифр перегруппировываются в группы по пять цифр:

73942 15711 39387 22216.

5. Из одноразового блокнота используются шесть, ранее не использованных групп по пять цифр — одноразовый ключ шифрования. Первые пять цифр из кодовой книги отвечают за порядок и тип сообщения:

16471 56328 29731 35682 23798 46659.

6. Последние пять цифр служат получателю для проверки числа групп цифр.

7. Сообщение 5 зашифровывается одноразовым блокнотом — сложением одноразового ключа и изменённого текста по модулю 10 без переноса в старший разряд:

		73942	15711	39387	22216	
+ mod 10	16471	56328	29731	35682	23798	46659
	16471	25660	34442	64969	45854	46659.

8. В конце сообщения добавляется группа из пяти цифр: первые три цифры отвечают за номер сообщения, последние две — за дату:

16471 25660 34442 64969 45854 46659 21210.

9. Наконец, все цифры в сообщении переводятся в буквы

IETWI UREEO ZTTTU ETPEP TRART TEERP UIOIO

в соответствии с табл. 2.

Таблица 2

0	1	2	3	4	5	6	7	8	9
O	*I*	*U*	*Z*	*T*	*R*	*E*	*W*	*A*	*P*

Описанный процесс шифрования с одноразовым блокнотом обеспечивает абсолютную секретность даже при условии, что кодовая книга-словарь станет известна злоумышленнику. Естественно, одноразовый блокнот должен использоваться однократно.

В цифровой век одноразовый ключ является битовой строкой.

Перейдём к квантовому распределению ключей. Базовой конфигурацией в квантовой криптографии при распределении ключей является конфигурация точка–точка. В информационных сетях узлы сети могут соединяться в различные структуры. При этом структура квантовой сети — соединение различных узлов квантовыми каналами, по которым происходит квантовое распределение ключей, может отличаться от структуры классической сети. Иначе говоря, не каждая пара узлов сети может быть непосредственно соединена квантовым каналом связи, по которому происходит квантовое распределение ключей. Общий ключ можно распределить только между узлами, которые непосредственно соединены квантовым каналом. Для передачи защищённой информации требуется иметь общий секретный ключ между любой парой узлов сети. Для согласования ключей между любой парой узлов сеть должна иметь соединение квантовым каналом любой пары узлов через промежуточные доверенные узлы.

На промежуточных доверенных узлах имеется передающая и приёмная аппаратура для квантового распределения ключей между данным узлом и узлами, которые с ним соединены квантовым каналом связи. Естественно, при этом на промежуточных доверенных узлах имеется несколько ключей, которые возникают при распределении ключей между разными сегментами сети.

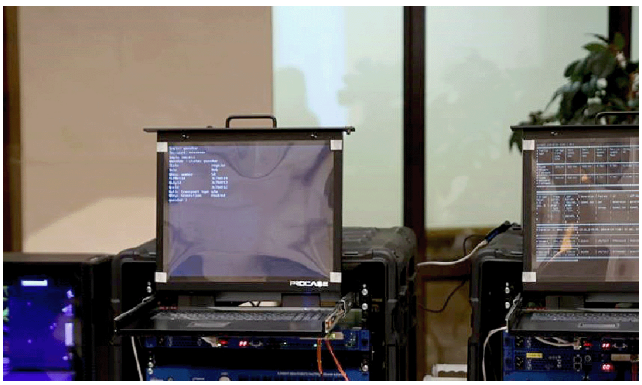


Рис. 4. Квантовый телефон, разработанный совместно российской IT компанией ИнфоТекс и Центром квантовых технологий МГУ.

В связи с этим возникает вопрос, как согласовать ключи — получить общий секретный ключ между любой парой узлов, не связанных непосредственно квантовым каналом связи. Исследование вопроса согласования ключей на разных сегментах сети проводилось в работе [23].

Пример аппаратуры квантовой сети, которая была названа "квантовым телефоном", для иллюстрации приведён на рис. 4 (см. подробности в [4]).

1.1. Зачем нужны системы квантовой криптографии — системы квантового расширения стартового ключа?

Казалось бы, что проблема абсолютно защищённых коммуникаций решена. Остаётся дело за малым. Нужно передавать (точнее, распределять) на каждое сообщение секретный ключ либо заранее иметь большой запас секретных ключей у Алисы и Боба на все последующие сообщения, которые также нужно как-то передать, а затем ещё и хранить, чтобы до них не добрался злоумышленник.

Однако в этом месте возникает порочный круг или, эквивалентно, так называемая проблема "яйца и курицы" — что было раньше? Для передачи секретных ключей нужен защищённый канал связи, который сам реализуется с помощью секретных ключей, или канал связи с курьерами, секретность которого базируется на честности и надёжности курьеров и технических организационных мерах.

До сих пор носитель секретного ключа не был важен, но неявно подразумевалось, что носителем является классический объект — курьер, классический сигнал и пр.

Возникает вопрос, что может появиться принципиально нового, если носителем ключа будет квантовый объект, например, квантовое состояние фотонов?

В этом месте возникает переход в квантовый мир. Оказывается, что квантовая механика разрывает порочный круг.

Исходная идея использовать законы квантовой механики для защиты информации была высказана в работе Стивена Виснера (Stephen Wiesner). Годом позднее [24] Чарльзом Беннетом (C.H. Bennett) и Джилом Брассардом (G. Brassard) был предложен первый протокол квантовой криптографии, который получил название BB84, по именам авторов.

В каком смысле и как квантовая природа микромира разрывает данный круг?

Для того чтобы не потерять общую логику событий, приведём утверждения, которые буду уточняться и детализироваться далее.

Утверждения.

1. Квантовая механика позволяет секретным образом распределять ключи через открытый, доступный для прослушивания и модификации квантовый канал связи посредством передачи квантовых состояний, в которые кодируются биты будущего ключа. В качестве квантового канала связи используется стандартное оптическое волокно либо атмосферный канал связи, через которые передаются квантовые состояния света — в идеале однофотонные состояния, либо когерентное сильно ослабленное до квазиоднофотонного уровня излучение стандартного телекоммуникационного лазера.

2. Кроме квантового канала связи требуется вспомогательный открытый и доступный для прослушивания аутентичный классический канал связи. Как будет видно далее, аутентичность классического канала связи играет принципиальную роль в обеспечении секретности распределяемых ключей.

Таким образом, квантовая механика, используя передачу квантовых состояний через открытый квантовый канал связи и дополнительный открытый аутентичный классический канал связи, позволяет получить общий секретный ключ.

По сути, квантовая криптография является процедурой согласования двух независимых случайных последовательностей на стороне Алисы и Боба. Согласование независимых последовательностей происходит посредством посыла квантовых состояний Алисой в определённом базисе, в соответствии со своей случайной последовательностью. На приёмной стороне Боб выбирает измерения в своём базисе в соответствии со своей случайной последовательностью. Вспомогательный аутентичный канал связи используется для согласования базисов измерения, оценки вероятности ошибки, коррекции ошибок, усиления секретности и передачи других вспомогательных открытых классических сообщений (см. детали далее).

Если допустить, что общий ключ каким-то способом распределён и не известен третьей стороне, то системы шифрования в режиме одноразового блокнота являются *теоретико-информационно* стойкими. Теоретико-информационная стойкость означает, что стойкость шифрования не зависит от технических и вычислительных возможностей подслушивателя.

Существуют системы асимметричной криптографии с открытыми ключами [26], в которых нет заранее распределённого общего секрета. Общий ключ появляется в результате выполнения участниками специального протокола. Системы асимметричной криптографии являются лишь *вычислительно-стойкими*. Стойкость базируется на предположениях об ограниченности технических и вычислительных возможностей подслушивателя. Фактически вычислительная стойкость базируется на вере в то, что никому не известен быстрый (полиномиальный) классический алгоритм нахождения ключа. Однако не доказано, что такой быстрый алгоритм не существует. Известные алгоритмы требуют больших вычислительных затрат — число шагов алгоритма экспоненциально велико по длине ключа. Для квантового вычислителя такой полиномиальный алгоритм известен — это алгоритм Шора [25].

Принципиальное различие вычислительной и теоретико-информационной стойкости состоит в том, что при вычислительной стойкости при проведении алгоритма (пусть даже экспоненциально затратного по числу вычислительных шагов) вероятность вскрытия шифра равна единице. В системах с теоретико-информационной стойкостью, например, для одноразового блокнота, вероятность вскрытия шифра не зависит от технических и вычислительных возможностей. По этой причине распределения ключей, базирующиеся лишь на вычислительно-стойких методах (например, методе Диффи–Хелмана [26]), являются более уязвимыми, поскольку данные методы потенциально неустойчивы относительно определения (вскрытия) ключа при его распределении.

В классической области проблема распределения ключей, если не использовать способы распределения ключей, основанные на вычислительно-стойких методах, "выносится за скобки", в том смысле, что эта проблема в каждом случае решается своими организационно-техническими методами, поэтому секретность одноразовых ключей базируется на "стойкости организационных методов". Так или иначе, каждый раз нужен новый ключ на каждое сообщение или множество ключей на все последующие сообщения, которые где-то нужно хранить и использовать по мере появления сообщений.

Возникает принципиальный вопрос: можно ли реализовать шифрование в режиме одноразового блокнота, используя только один первичный — стартовый — ключ? На первый взгляд, даже сама постановка вопроса выглядит абсурдной.

В классической области, когда носителями информации являются классические сигналы, ответ на данный вопрос является отрицательным.

В квантовой области ответ оказывается положительным. Технология квантовой криптографии — КРК — позволяет, используя только один предварительно распределённый стартовый ключ, распределять секретные ключи, которые могут быть использованы для шифрования в режиме одноразового блокнота, практически сколь угодно долго. Причём гарантируется, что секретность ключей базируется на фундаментальных законах Природы, а не на предположениях о технических и вычислительных возможностях подслушивателя. Принципиальное отличие от классического случая состоит в том, что в классическом случае нужно обеспечивать секретность каждого ключа, распределяемого организационными методам. В квантовом случае достаточно распределить только один короткий первичный стартовый ключ, используя организационные методы. Последующие ключи получаются при квантовом распределении, и их секретность гарантируется фундаментальными законами Природы — ключи являются теоретико-информационно стойкими (точные определения будут приведены далее).

Для обеспечения теоретико-информационно стойкой аутентификации требуется один общий предварительно распределённый стартовый ключ. Последующие ключи получаются как результат квантового распределения. Часть нового квантового ключа используется для обеспечения аутентичного канала связи в последующих сеансах, а остальная часть может использоваться как одноразовый ключ для шифрования.

В этой ситуации фундаментальная теорема об одноразовых ключах [14, 16, 20] приобретает новый смысл: для множества одноразовых ключей достаточно распределить один стартовый ключ, в отличие от классического случая, где нужно распределять ключ на каждое сообщение.

Аутентичность классического канала означает обеспечение целостности (неизменяемости) передаваемых открытых (доступных всем) классических сообщений. Аутентичность принципиально важна для достижения секретности распределяемых квантовых ключей.

Если целостность классических сообщений нарушена, то нарушитель может производить атаку *Man-in-the-Middle* (человек посредине), которая не обнаруживается легитимными пользователями (рис. 5).

Поскольку легитимные пользователи контролируют только свою передающую (Алиса) и приёмную (Боб) аппаратуру и не контролируют ни квантовый, ни классический каналы связи, то нарушитель может разорвать оба канала связи (см. рис. 5).

Алиса будет посылать квантовые состояния и классические сообщения к нарушителю. Аналогично нарушитель будет посылать свои квантовые состояния и классические сообщения к Бобу. При этом нарушитель не производит ошибок на стороне Боба. В итоге Алиса и Боб будут считать, что взаимодействуют друг с другом и имеют общий ключ, хотя они имеют общие ключи с нарушителем.

Без аутентичного классического канала связи такая атака не детектируется, нарушитель знает ключ, точнее имеет одинаковые ключи с Алисой и Бобом, система не обеспечивает секретность распределяемых ключей. При аутентичном классическом канале связи такая атака будет обнаружена.

Поскольку квантовая криптография по исходному замыслу должна обеспечивать безусловную секретность (unconditional security) распределяемых ключей, которая основана на фундаментальных законах квантовой механики, а не на предположениях о вычислительных или технических возможностях подслушивателя, то и аутентификация классического канала связи должна быть теоретико-информационно стойкой.

В криптографии существуют классические методы расширения ключей, которые также требуют стартового ключа. Расширение, продвижение и перешифрование ключей происходит и в классических информационных сетях без технологии квантовой криптографии с использованием первичного мастер-ключа и классических криптографических методов.

Естественный вопрос состоит в том, зачем использовать квантовую криптографию, если существуют классические методы? Ниже будет показано, что используя фундаментальные законы Природы — квантовой механики, удаётся получить фундаментальные ограничения на связь секретности квантовых ключей и числа допустимых сеансов КРК. Причём данные фундаментальные ограничения не зависят от технических или вычислительных возможностей нарушителя и не зависят от наличия у нарушителя квантового вычислителя.

В квантовой криптографии удаётся получить явные ограничения на число одноразовых ключей в виде аналитических формул, которые базируются только на фундаментальных законах Природы.

2. Качество распределяемых ключей

Неформально говоря, при шифровании в режиме одноразового блокнота нарушитель "видит" в канале каждое зашифрованное сообщение как случайную битовую строку, которая статистически не зависит от сообщения [16, 20]. Если одноразовый ключ представляет собой идеальную случайную битовую строку, где каждая позиция равновероятна и не зависит от другой, то в этой ситуации у нарушителя нет других вариантов, кроме как пытаться угадать ключ. При идеальных ключах вероятность угадать истинный ключ есть $1/2^n$, где n — длина ключа/сообщения.

Доказательства секретности квантового распределения ключей являются достаточно сложными. Секретность определяется в терминах, которые отличаются от требований, предъявляемых к ключам в классической криптографии.

В квантовой криптографии секретность ключей формулируется в терминах различимости квантовых состояний — матриц плотности $\rho^{\,\mathrm{Real}}$ и $\rho^{\,\mathrm{Ideal}}$, отвечающих *реальной* и *идеальной* ситуациям при квантовом распределении ключей. Метрикой близости двух квантовых состояний является следовая метрика.

В классической криптографии секретность ключей понимается в терминах, например, сложности перебора ключей при наличии побочной информации. В квантовой криптографии побочной информацией для подслушивателя является вся совокупность информации о ключах, полученная как из квантового, так и из классического каналов.

Тот факт, что математический аппарат при доказательстве секретности ключей в классической и квантовой криптографии существенно различается, приводит к недопониманию и эмоциональным дискуссиям [27, 28].

Рассмотрим квантовые состояния, отвечающие различным ситуациям.

Идеальная ситуация — это ситуация, когда отсутствует вторжение в квантовый и классический каналы связи.

В реальной ситуации имеются атаки на квантовый и классический каналы связи.

В квантовой криптографии ключи называются ε-секретными, если имеет место соотношение

$$D(\rho^{\,\mathrm{Real}}, \rho^{\,\mathrm{Ideal}}) = ||\rho^{\,\mathrm{Real}} - \rho^{\,\mathrm{Ideal}}||_1 \leqslant \varepsilon\,, \tag{1}$$

$$||\rho^{\,\mathrm{Real}} - \rho^{\,\mathrm{Ideal}}||_1 = \mathrm{Tr}\left\{|\rho^{\,\mathrm{Real}} - \rho^{\,\mathrm{Ideal}}|\right\} = \mathrm{Tr}\left\{\sqrt{(\rho^{\,\mathrm{Real}} - \rho^{\,\mathrm{Ideal}})^{+}(\rho^{\,\mathrm{Real}} - \rho^{\,\mathrm{Ideal}})}\right\},$$

где $(...)^{+}$ — символ эрмитова сопряжения.

Математически секретность ключей формулируется в терминах различимости квантовых состояний [29]. Пара квантовых состояний считается ε-неразличимой, если *никакими измерениями* невозможно отличить одно квантовое состояние от другого с вероятностью успеха, превышающей вероятность простого угадывания более, чем на ε.

Для секретных ключей, используемых в различных алгоритмах шифрования, предъявляются требования, которые формулируются совершенно в других терминах. Шенноном [20] был введён критерий практической секретности криптосистемы, который понимается как "*The average amount of work to determine the key for a cryptogram...*". Данный критерий не был формализован, поэтому в зависимости от ситуации возможны различные критерии средней работы (трудоёмкости) по определению ключа. Само понятие трудоёмкости фактически связано с перебором (опробованием) ключей до определения истинного ключа. Причём перебор может быть как полным — по всему пространству ключей, так и частичным — по части ключевого пространства. Такой перебор может иметь место как в отсутствие побочной информации о ключе, так и при наличии дополнительной информации.

Применительно к ключам, полученным в результате квантового распределения ключей, побочная информация о ключе возникает у подслушивателя при измерениях над квантовой системой, коррелированной с истинным ключом легитимных пользователей.

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

Ранее в работах [30–33] была установлена прямая связь между критерием секретности, основанным на различимости пары квантовых состояний, и различными критериями, использующими понятие трудоёмкости — сложности перебора по экспоненциально большому (по длине ключа) пространству в классической криптографии.

В практической криптографии важной характеристикой является средняя трудоёмкость Q частичного перебора ключей при заданной вероятности успеха (нахождения ключа) π, не меньшей π_0 [30–33]. Перебор осуществляется по множеству наиболее вероятных ключей мощности M, для которых $\pi(M) > \pi_0$.

Трудоёмкость Q — среднее число опробуемых ключей до нахождения истинного ключа — связана с ε-секретностью ключей. Для нижней границы трудоёмкости частичного перебора имеет место неравенство

$$Q(\varepsilon, \pi_0) > \left(1 - \frac{\varepsilon}{\pi_0}\right)\left(\frac{N(1-4\varepsilon)+1}{2}\right), \tag{2}$$

где $N = 2^n$ — размер ключевого пространства.

Таким образом, качество ключей (близость их к идеальным в смысле следового расстояния) напрямую связано с трудоёмкостью по взлому шифра — нахождением истинного ключа шифрования.

Предположим, что нам удастся определить величину ε для первого запуска системы с использованием первичного стартового ключа для аутентификации. Кроме того, если будет установлено, как изменяется величина ε в последующих сеансах, то это даст ответ на вопрос: сколько сеансов квантового распределения ключей мы можем себе позволить до следующего перезапуска системы, пока качество распределяемых ключей ещё не достигает критического уровня, при котором их использование станет неприемлемым.

3. Зачем нужен аутентичный классический канал связи при квантовом распределении ключей?

Аутентичность классического канала означает обеспечение целостности (неизменяемости) передаваемых открытых (доступных всем) классических сообщений. Аутентичность принципиально важна для достижения секретности распределяемых квантовых ключей. Если целостность классических сообщений нарушена, то нарушитель может производить атаку *Man-in-the-Middle* (человек посредине), которая не обнаруживается легитимными пользователями (см. рис. 5) [34–37].

Поскольку легитимные пользователи контролируют только свою передающую (Алиса) и приёмную (Боб) аппаратуру и не контролируют ни квантовый, ни классический каналы связи, то нарушитель (Ева) может разорвать оба канала связи (см. рис. 5).

Алиса будет посылать квантовые состояния и классические сообщения к нарушителю. Аналогично нарушитель будет посылать свои квантовые состояния и классические сообщения к Бобу. При этом нарушитель не производит ошибок на стороне Боба. В итоге Алиса и Боб будут считать, что взаимодействуют друг с другом и имеют общий ключ, хотя они имеют общие ключи с нарушителем.

Без аутентичного классического канала связи такая атака не детектируется, нарушитель знает ключ, точнее имеет одинаковые ключи с Алисой и Бобом, система не обеспечивает секретность распределяемых ключей. При аутентичном классическом канале связи такая атака будет обнаружена.

Поскольку квантовая криптография по исходному замыслу должна обеспечивать безусловную секретность (unconditional security) распределяемых ключей, которая основана на фундаментальных законах квантовой механики, а не на предположениях о вычислительных или технических возможностях подслушивателя, то и аутентификация классического канала связи должна быть теоретико-информационно стойкой.

В фундаментальной работе Wegman и Carter [38] было показано, что теоретико-информационно стойкая аутентификация может быть достигнута с использованием класса специальных хэш-функций [39 – 52].

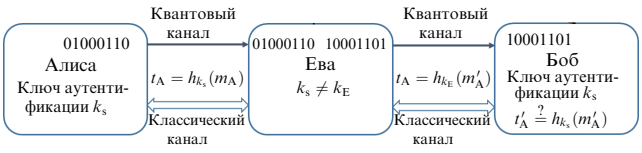


Рис. 5. Иллюстрация атаки *Man-in-the-Middle*. Нарушитель разрывает квантовый и классический каналы связи и генерирует отдельные ключи Алиса – Ева и Ева – Боб. Такая атака не обнаруживается, если классический канал не обеспечивает аутентичность — *неизменяемость* открытых классических сообщений. Алиса и Боб имеют общий секретный ключ аутентификации k_s. Алиса посылает открытые сообщения m и их "дайджест" — хэш-значения $t_A = h_{k_s}(m_A)$. Ева, не зная секретного ключа k_s, хочет подменить сообщения Алисы на свою пару $t'_A = h_{k_E}(m'_A)$. Хэш-значение t'_A подменного m'_A Ева вычисляет с использованием своего ключа k_E, который, вообще говоря, не совпадает с истинным ключом k_s. Боб проверяет истинность сообщения и тега с ключом k_s. Если $t'_A \neq h_{k_s}(m'_A)$, то сеанс КРК прерывается. Если Ева угадала ключ, то аутентификация будет принята. Вероятность такого события при теоретико-информационной аутентификации не зависит от технических и вычислительных возможностей Евы, а определяется только структурой хэш-функций.

Теоретико-информационно стойкая аутентификация обеспечивает обнаружение вторжений в классический канал связи независимо от технических возможностей подслушивателя (например, даже при наличии у него полномасштабного квантового компьютера).

Для теоретико-информационной стойкой аутентификации требуется общий секретный ключ у Алисы и Боба, поэтому при первом запуске системы Алисе и Бобу должен быть доставлен общий стартовый ключ.

Из представленного выше следует, что системы квантовой криптографии, по сути, представляют собой системы расширения исходного стартового ключа.

В криптографии существуют классические методы расширения ключей, которые также требуют стартового ключа. Расширение, продвижение и перешифрование ключей происходят и в классических информационных сетях без технологии квантовой криптографии с использованием первичного мастер-ключа и классических криптографических методов.

Естественный вопрос состоит в том, зачем использовать квантовую криптографию, если существуют классические методы?

Принципиальная разница заключается в том, что, в отличие от квантовой криптографии, стойкость классических методов расширения ключей основывается на предположениях о технических или вычислительных возможностях нарушителя. По этой причине в классическом случае невозможно предъявить фундаментальные ограничения на допустимое число сеансов расширения ключей и их качество. В квантовой криптографии удаётся получить явные ограничения в виде аналитических формул, которые базируются только на фундаментальных законах Природы.

4. Идеология абстрактной криптографии — различимость квантовых состояний

Как обсуждалось в разделе 1.1, после квантового распределения ключей часть ключа может использоваться для аутентификации в последующем сеансе, а часть — для шифрования одноразовым блокнотом.

При этом возникает принципиальный вопрос: каково будет качество ключей в каждом из последующих процессов, если известно качество входного ключа? В нашем случае таким входным ключом является стартовый ключ аутентификации при первом запуске системы.

Ответ на поставленный вопрос даётся в рамках подхода, называемого *абстрактной криптографией*.

Идеология абстрактной криптографии для классического случая была высказана в [53, 54], в квантовой области данная идея развивалась в ряде работ [55, 56] (обзор последних работ см. в [55]).

По сути, идеология абстрактной криптографии сводится к вычислению расстояния в определённой метрике между различными ситуациями. Каждой ситуации отвечает определённое квантовое состояние. Мерой близости различных ситуаций — квантовых состояний — является следовое расстояние [57].

Реальная ситуация — реальный сеанс квантового распределения ключей с вторжением нарушителя в кванто-

вый канал связи и реальная аутентификация, при которой возможна подмена сообщений в классическом канале связи.

Идеальная ситуация — идеальный сеанс квантового распределения ключей без вторжения в квантовый канал связи и идеальная аутентификация без подмены сообщений в классическом канале связи.

Каждой ситуации отвечает квантовое состояние — матрица плотности всех трёх участников протокола Алиса – Боб – Ева, ρ^{Real} отвечает реальной ситуации, ρ^{Ideal} — идеальной ситуации.

Как понять, какая ситуация имеет место быть?

Для этого вводится третья сторона (*Distinguisher*), которая имеет доступ ко всем подсистемам составного квантового состояния Алиса – Боб – Ева. Напомним, что Алиса, Боб, Ева имеют доступ только к своей квантовой подсистеме. *Distinguisher* умозрительно (по этой причине такой подход назван абстрактной криптографией) имеет доступ к квантовым состояниям, отвечающим реальной и идеальной ситуациям. Задача *Distinguisher* сводится к различению двух ситуаций посредством квантово-механических измерений.

Оказывается, что для оптимальных измерений — оптимальных в смысле минимизации ошибки при различении двух квантовых состояний — максимальная вероятность $\Pr_{OK}$ правильного различения двух квантовых состояний ρ^{Real} и ρ^{Ideal} равна

$$\Pr{}_{OK} = \frac{1}{2}\left(1 + \frac{1}{2}\,||\rho^{\text{Real}} - \rho^{\text{Ideal}}||_1\right) = \frac{1}{2}(1+\varepsilon)\,,$$

где $\frac{1}{2}||\rho^{\text{Real}} - \rho^{\text{Ideal}}||_1 \leqslant \varepsilon$. По определению, $||\rho||_1 = \operatorname{Tr}\{\sqrt{\rho^{+}\rho}\}$. В этом случае реальная и идеальная ситуации называются ε-неразличимыми. Аналогично ключи, полученные в двух ситуациях, являются ε-секретными.

5. Секретность криптографических композиций — Composable security

Абстрактный критерий секретности, основанный на следовой метрике, обладает одним важным и удобным свойством. Оказывается, что критерий секретности может быть разложен на критерии секретности между отдельными элементарными процессами. Для отдельных процессов можно вычислить следовое расстояние, тогда следовое расстояние между составными реальными и идеальными процессами оказывается ограничено суммой следовых расстояний между отдельными процессами.

В этом случае значения ε от (неидеальных) последовательных процессов складываются. Секретность нескольких процессов называется составной секретностью — composable security.

Дальнейшая логика действий будет сводиться к следующему. Пусть проводится текущий сеанс квантового распределения ключей, который состоит из следующих стадий:

1) передача и измерение квантовых состояний;

2) постобработка: согласование базисов, оценка вероятности ошибок, коррекция ошибок, усиление секретности очищенных ключей.

Все процедуры постобработки происходят без аутентификации. Если сеанс успешен — следовое расстояние между реальной и идеальной ситуацией для текущего сеанса меньше ε, то в конце сеанса проводится проверка аутентичности всех накопленных классических сообщений при постобработке.

Если сеанс неудачен — не достигнут нужный уровень секретности ключа в смысле следового расстояния, то данный сеанс отбраковывается и проводится следующий.

При успешном сеансе проводится аутентификация, которая считается успешной — пройденной, если не обнаружена подмена сообщений. Если при аутентификации обнаружена подмена сообщений, то сеанс отбрасывается.

Для дальнейшего нам потребуются квантовые состояния, описывающие отдельные реальные и идеальные ситуации. При аутентификации выбор хэш-функций текущего сеанса происходит посредством выбора части неидеального ключа, полученного в предыдущем сеансе и обладающего свойством ε-секретности.

Поскольку аутентификация проводится после сеанса квантового распределения ключей, то из-за атаки *Man-in-the-Middle* Алиса и Боб могут "видеть" различные квантовые состояния – матрицы плотности, соответственно, разные ключи. Пока не проведена аутентификация сообщений по открытому каналу связи подслушиватель может разорвать квантовый и классический каналы связи и провести отдельные сеансы КРК с Алисой и Бобом. После всех процедур КРК, но до аутентификации, Алиса и Боб будут иметь различные матрицы плотности, соответственно, разные ключи.

Пусть у Алисы и Боба после КРК имеется набор, вообще говоря, разных классических сообщений из-за атаки подслушивателя. У Алисы — (m), у Боба — (m'). Такой же набор классических сообщений имеется у подслушивателя.

Затем Алиса и Боб проводят сеанс аутентификации, состоящий в том, что Алиса посылает Бобу пару $(t = h_{k_s}(m), m)$, здесь $h_{k_s}(m)$ — ключевая хэш-функция, k_s — ключ аутентификации.

Подслушиватель имеет доступ к каналу и может подменять сообщения Алисы $(t, m) \to (t', m')$ при переносе их Бобу. Однако подслушиватель не имеет секретного ключа k_s для аутентификации, который имеют Алиса и Боб. Имея m' и k_s, Боб проверяет справедливость равенства $t' = h_{k_s}(m')$. Если окажется, что $t' \neq h_{k_s}(m')$, то аутентификация провалена — сеанс отбрасывается.

Если аутентификация успешна — сеанс принимается.

Аналогичный процесс аутентификации имеет место при посылке классических сообщений от Боба к Алисе. Набор сообщений при двусторонних обменах классическими сообщениями зависит от типа используемого протокола КРК.

Для дальнейшего нам потребуются квантовые состояния, описывающие отдельные *реальные* и *идеальные* ситуации.

Введём обозначения:

$\rho_{\text{ABE}}^{R_A R_B R_Q}$ — матрица плотности после реального квантового распределения ключей R_Q с нарушителем в квантовом канале связи, реальной аутентификацией сообщений Алиса – Боб R_A и реальной аутентификацией сообщений Боб – Алиса R_B с возможной подме-

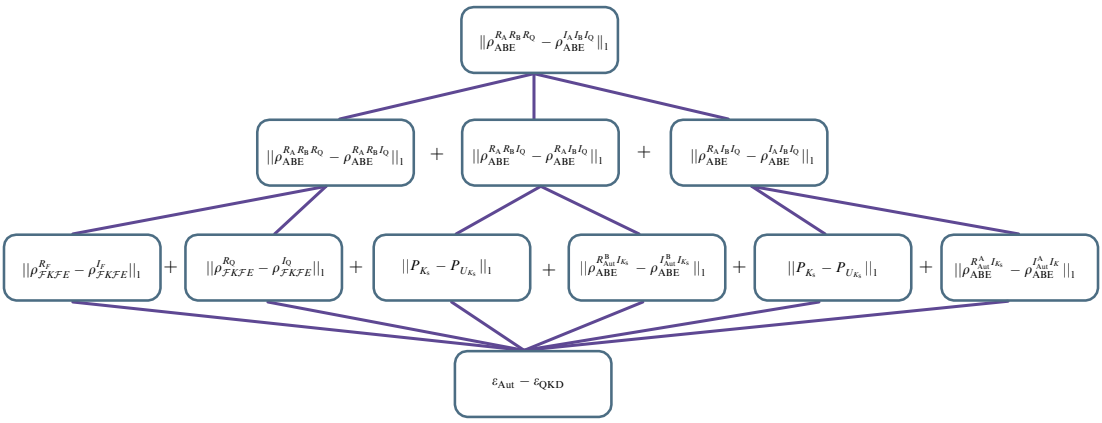


Рис. 6. Диаграмма, иллюстрирующая разложение реального процесса КРК с теоретико-информационной аутентификацией на элементарные процессы.

ной сообщений в аутентичном классическом канале связи,

$\rho_{\mathrm{ABE}}^{R_\mathrm{A}R_\mathrm{B}I_\mathrm{Q}}$ — матрица плотности после идеального квантового распределения ключей I_Q без нарушителя в квантовом канале связи, с реальной аутентификацией сообщений Алиса – Боб R_A и реальной аутентификацией сообщений Боб – Алиса R_B с возможной подменой сообщений в аутентичном классическом канале связи,

$\rho_{\mathrm{ABE}}^{R_\mathrm{A}I_\mathrm{B}I_\mathrm{Q}}$ — матрица плотности после идеального квантового распределения ключей I_Q без нарушителя в квантовом канале связи, с реальной аутентификацией сообщений Алиса – Боб R_A с возможной подменой сообщений в аутентичном классическом канале связи и идеальной аутентификацией Боб – Алиса I_B без подмены сообщений в аутентичном классическом канале связи,

$\rho_{\mathrm{ABE}}^{I_\mathrm{A}I_\mathrm{B}I_\mathrm{Q}}$ — матрица плотности после идеального квантового распределения ключей I_Q без нарушителя в квантовом канале связи, с идеальной аутентификацией сообщений Алиса – Боб I_A и идеальной аутентификацией Боб – Алиса I_B без подмены сообщений в аутентичном классическом канале связи.

Далее нас будет интересовать расстояние между двумя ситуациями при каждом сеансе КРК — реальной ситуацией с вторжением в квантовый и классический каналы связи $\rho_{\mathrm{ABE}}^{R_\mathrm{A}R_\mathrm{B}R_\mathrm{Q}}$ и идеальной ситуацией без вторжения в квантовый и классический каналы связи $\rho_{\mathrm{ABE}}^{I_\mathrm{A}I_\mathrm{B}I_\mathrm{Q}}$. Пусть расстояние между $\rho_{\mathrm{ABE}}^{R_\mathrm{A}R_\mathrm{B}R_\mathrm{Q}}$ и $\rho_{\mathrm{ABE}}^{I_\mathrm{A}I_\mathrm{B}I_\mathrm{Q}}$ есть ε, тогда ключи, которые получаются в реальной ситуации, которой отвечает квантовое состояние $\rho_{\mathrm{ABE}}^{R_\mathrm{A}R_\mathrm{B}R_\mathrm{Q}}$, будут ε-секретными. То есть использование реальных ключей и идеальных ключей, которые получаются в ситуации с квантовым состоянием $\rho_{\mathrm{ABE}}^{I_\mathrm{A}I_\mathrm{B}I_\mathrm{Q}}$, нельзя отличить с вероятностью лучшей, чем ε.

Соответственно, если данные ключи используются для шифрования, то трудоёмкость нахождения ключей — вскрытия шифра — будет определяться величиной ε.

Нашей целью будет выяснить, как зависит параметр секретности от номера сеанса КРК и от качества стартового ключа аутентификации — близости стартового ключа к идеальному — равновероятному. Тем самым будет выяснено, сколько сеансов можно провести без потери криптографического качества ключей, которые используются для шифрования в режиме одноразового блокнота.

Для расстояния между различными ситуациями – квантовыми состояниями — имеем

$$\|\rho_{\mathrm{ABE}}^{R_\mathrm{A}R_\mathrm{B}R_\mathrm{Q}} - \rho_{\mathrm{ABE}}^{I_\mathrm{A}I_\mathrm{B}I_\mathrm{Q}}\|_1 \leqslant \tag{3}$$

$$\leqslant \|\rho_{\mathrm{ABE}}^{R_\mathrm{A}R_\mathrm{B}R_\mathrm{Q}} - \rho_{\mathrm{ABE}}^{R_\mathrm{A}R_\mathrm{B}I_\mathrm{Q}}\|_1 + \tag{4}$$

$$+ \|\rho_{\mathrm{ABE}}^{R_\mathrm{A}R_\mathrm{B}I_\mathrm{Q}} - \rho_{\mathrm{ABE}}^{R_\mathrm{A}I_\mathrm{B}I_\mathrm{Q}}\|_1 + \tag{5}$$

$$+ \|\rho_{\mathrm{ABE}}^{R_\mathrm{A}I_\mathrm{B}I_\mathrm{Q}} - \rho_{\mathrm{ABE}}^{I_\mathrm{A}I_\mathrm{B}I_\mathrm{Q}}\|_1 . \tag{6}$$

В (3) – (6) использовано неравенство треугольника для следового расстояния [57].

Следовое расстояние (3) мажорируется суммой расстояний между отдельными элементарными процессами. Вычислить напрямую расстояние между сложным реальным и идеальным процессом – сложными квантовыми состояниями — невозможно. В парадигме абстрактной криптографии расстояние между сложными процессами разбивается на сумму расстояний между элементарными процессами (квантовыми состояниями), которые могут быть вычислены явно.

Расстояние между квантовыми состояниями $\rho_{\mathrm{ABE}}^{R_\mathrm{A}R_\mathrm{B}R_\mathrm{Q}}$ и $\rho_{\mathrm{ABE}}^{I_\mathrm{A}I_\mathrm{B}I_\mathrm{Q}}$ представляется суммой простых состояний. Для удобства разложение сложного процесса на элементарные приведено на рис. 6.

В следующих разделах будет проведено вычисление расстояний для отдельных процессов.

5.1. Конкретные представления матриц плотности для различных процессов

В этом разделе займёмся вычислением следового расстояния. Для этого потребуются матрицы плотности для квантовых состояний, отвечающих различным ситуациям, описанным в предыдущем разделе.

Матрица плотности для процесса $R_\mathrm{A}R_\mathrm{B}R_\mathrm{Q}$ имеет вид

$$\rho_{\mathrm{ABE}}^{R_\mathrm{A}R_\mathrm{B}R_\mathrm{Q}} = \sum_{k_\mathrm{A}}\sum_{k_\mathrm{B}} P_{K_\mathrm{A}K_\mathrm{B}}(k_\mathrm{A},k_\mathrm{B})|k_\mathrm{A}\rangle_{K_\mathrm{A}\,K_\mathrm{A}}\langle k_\mathrm{A}| \otimes$$

$$\otimes\, |k_\mathrm{B}\rangle_{K_\mathrm{B}\,K_\mathrm{B}}\langle k_\mathrm{B}| \otimes g^{R_\mathrm{A}m_{k_\mathrm{A}}} \otimes g^{R_\mathrm{B}m_{k_\mathrm{B}}} \otimes \rho_{\mathrm{E}}^{k_\mathrm{A}k_\mathrm{B}}. \tag{7}$$

Поясним введённые обозначения.

После КРК с возможным вторжением в квантовый канал связи и аутентификацией через классический канал с возможной подменой классических сообщений и атакой *Man-in-the-Middle* Алиса и Боб имеют финальные ключи

k_A и k_B, $P_{K_\mathrm{A}K_\mathrm{B}}(k_\mathrm{A},k_\mathrm{B})$ — совместное распределение ключей. Ключи Алисы и Боба совпадают с вероятностью, близкой к единице (см. детали далее).

Удобно каждому ключу — битовой строке длиной ℓ — сопоставить ортогональное квантовое состояние:

$$k_\mathrm{A}=(k_{i_1\mathrm{A}},k_{i_2\mathrm{A}},\ldots,k_{i_\ell\mathrm{A}})\to$$
$$\to|k_\mathrm{A}\rangle=|k_{i_1\mathrm{A}}\rangle\otimes|k_{i_2\mathrm{A}}\rangle\otimes\ldots\otimes|k_{i_\ell\mathrm{A}}\rangle\,,\quad k_{i_j\mathrm{A}}=0,1\,,$$
$$k_\mathrm{B}=(k_{i_1\mathrm{B}},k_{i_2\mathrm{B}},\ldots,k_{i_\ell\mathrm{B}})\to$$
$$\to|k_\mathrm{B}\rangle=|k_{i_1\mathrm{B}}\rangle\otimes|k_{i_2\mathrm{B}}\rangle\otimes\ldots\otimes|k_{i_\ell\mathrm{B}}\rangle\,,\quad k_{i_j\mathrm{B}}=0,1\,.$$

В общем случае Ева, из-за возможной атаки *Man-in-the-Middle* на квантовый и классический каналы связи, имеет в своём распоряжении квантовое состояние $\rho_\mathrm{E}^{k_\mathrm{A}k_\mathrm{B}}$, "привязанное" к каждой паре ключей k_A и k_B, т.е. коррелированное с ключами.

Набору классических сообщений (битовой строке) от Алисы к Бобу с возможной подменой истинных сообщений также удобно сопоставить ортогональные (по ключам k_A) квантовые состояния $g^{R_\mathrm{A}m_{k_\mathrm{A}}}$, которые "привязаны" к ключам после сеанса КРК, в том смысле, что набор классических сообщений после КРК зависит от сеанса КРК.

Набору классических сообщений (битовой строке) от Боба к Алисе сопоставляем ортогональные квантовые состояния $g^{R_\mathrm{B}m_{k_\mathrm{B}}}$.

Более подробный вид $\rho_\mathrm{ABE}^{R_\mathrm{A}R_\mathrm{B}R_\mathrm{Q}}$ будет приведён ниже.

Матрица плотности для процесса $R_\mathrm{A}R_\mathrm{B}I_\mathrm{Q}$ имеет вид

$$\rho_\mathrm{ABE}^{R_\mathrm{A}R_\mathrm{B}I_\mathrm{Q}}=\sum_{k_\mathrm{A}}\sum_{k_\mathrm{B}}\frac{1}{|K_\mathrm{A}|}\,\delta_{k_\mathrm{A},k_\mathrm{B}}|k_\mathrm{A}\rangle_{K_\mathrm{A}\,K_\mathrm{A}}\langle k_\mathrm{A}|\otimes|k_\mathrm{B}\rangle_{K_\mathrm{B}\,K_\mathrm{B}}\langle k_\mathrm{B}|\otimes$$
$$\otimes\,g^{R_\mathrm{A}m_{k_\mathrm{A}}}\otimes g^{R_\mathrm{B}m_{k_\mathrm{B}}}\otimes\rho_\mathrm{E}\,,\qquad(8)$$
$$\rho_\mathrm{E}=\sum_{k'_\mathrm{A}}\sum_{k'_\mathrm{B}}P_{K_\mathrm{A}K_\mathrm{B}}(k'_\mathrm{A},k'_\mathrm{B})\,\rho_\mathrm{E}^{k'_\mathrm{A}k'_\mathrm{B}}\,.$$

Отличие (7) от (8) состоит в том, что процесс КРК является идеальным, что отвечает индексу I_Q. Кроме того, ключи Алисы и Боба строго одинаковы ($\delta_{k_\mathrm{A},k_\mathrm{B}}$ — символ Кронекера), т.е. одинаковы с вероятностью единица, равновероятны, и квантовое состояние Евы ρ_E "отвязано" от ключей, т.е. не коррелировано с ключами. Передача классических сообщений от Алисы к Бобу и от Боба к Алисе происходит через реальный классический канал связи с возможной подменой классических сообщений, $g^{R_\mathrm{A}m_{k_\mathrm{A}}}$, $g^{R_\mathrm{B}m_{k_\mathrm{B}}}$ — соответствующие квантовые состояния.

Матрица плотности для процесса $R_\mathrm{A}I_\mathrm{B}I_\mathrm{Q}$ имеет вид

$$\rho_\mathrm{ABE}^{R_\mathrm{A}I_\mathrm{B}I_\mathrm{Q}}=\sum_{k_\mathrm{A}}\sum_{k_\mathrm{B}}\frac{1}{|K_\mathrm{A}|}\,\delta_{k_\mathrm{A},k_\mathrm{B}}\,|k_\mathrm{A}\rangle_{K_\mathrm{A}\,K_\mathrm{A}}\langle k_\mathrm{A}|\otimes|k_\mathrm{B}\rangle_{K_\mathrm{B}\,K_\mathrm{B}}\langle k_\mathrm{B}|\otimes$$
$$\otimes\,g^{R_\mathrm{A}m_{k_\mathrm{A}}}\otimes g^{I_\mathrm{B}m_{k_\mathrm{B}}}\otimes\rho_\mathrm{E}\,.\qquad(9)$$

В этом процессе КРК происходит через идеальный квантовый канал связи, аналогично предыдущему процессу в (8).

Передача классических сообщений от Боба к Алисе также происходит через идеальный аутентичный канал связи, $g^{I_\mathrm{B}m_{k_\mathrm{B}}}$ — соответствующее квантовое состояние.

Передача классических сообщений от Алисы к Бобу происходит через реальный канал связи с возможной подменой сообщений, $g^{R_\mathrm{A}m_{k_\mathrm{A}}}$ — соответствующее квантовое состояние.

Матрица плотности для процесса $I_\mathrm{A}I_\mathrm{B}I_\mathrm{Q}$ имеет вид

$$\rho_\mathrm{ABE}^{I_\mathrm{A}I_\mathrm{B}I_\mathrm{Q}}=\sum_{k_\mathrm{A}}\sum_{k_\mathrm{B}}\frac{1}{|K_\mathrm{A}|}\,\delta_{k_\mathrm{A},k_\mathrm{B}}\,|k_\mathrm{A}\rangle_{K_\mathrm{A}\,K_\mathrm{A}}\langle k_\mathrm{A}|\otimes|k_\mathrm{B}\rangle_{K_\mathrm{B}\,K_\mathrm{B}}\langle k_\mathrm{B}|\otimes$$
$$\otimes\,g^{I_\mathrm{A}m_{k_\mathrm{A}}}\otimes g^{I_\mathrm{B}m_{k_\mathrm{B}}}\otimes\rho_\mathrm{E}\,.\qquad(10)$$

Данное квантовое состояние отвечает ситуации, когда КРК проходило через идеальный квантовый канал связи без вторжения в него. Классический канал связи также является идеальным, все классические сообщения от Алисы к Бобу и наоборот проходят без подмены.

6. Следовое расстояние между реальным и идеальным процессом квантового распределения ключей

Вычислим следовые расстояния для отдельных элементарных процессов. Поскольку

$$\rho_\mathrm{ABE}^{R_\mathrm{A}R_\mathrm{B}R_\mathrm{Q}}-\rho_\mathrm{ABE}^{R_\mathrm{A}R_\mathrm{B}I_\mathrm{Q}}=\sum_{k_\mathrm{A}}\sum_{k_\mathrm{B}}P_{K_\mathrm{A}K_\mathrm{B}}(k_\mathrm{A},k_\mathrm{B})|k_\mathrm{A}\rangle_{K_\mathrm{A}\,K_\mathrm{A}}\langle k_\mathrm{A}|\otimes$$
$$\otimes\,|k_\mathrm{B}\rangle_{K_\mathrm{B}\,K_\mathrm{B}}\langle k_\mathrm{B}|\otimes g^{R_\mathrm{A}m_{k_\mathrm{A}}}\otimes g^{R_\mathrm{B}m_{k_\mathrm{B}}}\otimes\rho_\mathrm{E}^{k_\mathrm{A}k_\mathrm{B}}-$$
$$-\sum_{k_\mathrm{A}}\sum_{k_\mathrm{B}}\frac{1}{|K_\mathrm{A}|}\,\delta_{k_\mathrm{A},k_\mathrm{B}}|k_\mathrm{A}\rangle_{K_\mathrm{A}\,K_\mathrm{A}}\langle k_\mathrm{A}|\otimes|k_\mathrm{B}\rangle_{K_\mathrm{B}\,K_\mathrm{B}}\langle k_\mathrm{B}|\otimes$$
$$\otimes\,g^{R_\mathrm{A}m_{k_\mathrm{A}}}\otimes g^{R_\mathrm{B}m_{k_\mathrm{B}}}\otimes\rho_\mathrm{E}=$$
$$=\sum_{k_\mathrm{A}}\sum_{k_\mathrm{B}}\big(|k_\mathrm{A}\rangle_{K_\mathrm{A}\,K_\mathrm{A}}\langle k_\mathrm{A}|\big)\otimes\big(|k_\mathrm{B}\rangle_{K_\mathrm{B}\,K_\mathrm{B}}\langle k_\mathrm{B}|\big)\otimes$$
$$\otimes\,g^{R_\mathrm{A}m_{k_\mathrm{A}}}\otimes g^{R_\mathrm{B}m_{k_\mathrm{B}}}\otimes$$
$$\otimes\left(P_{K_\mathrm{A}K_\mathrm{B}}(k_\mathrm{A},k_\mathrm{B})\otimes\rho_\mathrm{E}^{k_\mathrm{A}k_\mathrm{B}}-\frac{1}{|K_\mathrm{A}|}\,\delta_{k_\mathrm{A},k_\mathrm{B}}\,\rho_\mathrm{E}\right),$$

а квантовые состояния $g^{R_\mathrm{A}m_{k_\mathrm{A}}}$, $g^{R_\mathrm{B}m_{k_\mathrm{B}}}$ для фиксированной пары $(k_\mathrm{A},k_\mathrm{B})$ достоверно различимы (коммутативность – ортогональность), то прямым вычислением получаем, что

$$||\rho_\mathrm{ABE}^{R_\mathrm{A}R_\mathrm{B}R_\mathrm{Q}}-\rho_\mathrm{ABE}^{R_\mathrm{A}R_\mathrm{B}I_\mathrm{Q}}||_1=$$
$$=\sum_{k_\mathrm{A}}\sum_{k_\mathrm{B}}\mathrm{Tr}\left\{\left|P_{K_\mathrm{A}K_\mathrm{B}}(k_\mathrm{A},k_\mathrm{B})\rho_\mathrm{E}^{k_\mathrm{A}k_\mathrm{B}}-\delta_{k_\mathrm{A},k_\mathrm{B}}\,\frac{1}{|K_\mathrm{A}|}\,\rho_\mathrm{E}\right|\right\}=$$
$$=||\rho_\mathrm{ABE}^{R_\mathrm{Q}}-\rho_\mathrm{ABE}^{I_\mathrm{Q}}||_1\,.\qquad(11)$$

Здесь

$$\rho_\mathrm{ABE}^{R_\mathrm{Q}}=\operatorname*{Tr}_{R_\mathrm{A}R_\mathrm{B}}\big(\rho_\mathrm{ABE}^{R_\mathrm{A}R_\mathrm{B}R_\mathrm{Q}}\big)=\sum_{k_\mathrm{A}}\sum_{k_\mathrm{B}}P_{K_\mathrm{A}K_\mathrm{B}}(k_\mathrm{A},k_\mathrm{B})\times$$
$$\times\,\big(|k_\mathrm{A}\rangle_{K_\mathrm{A}\,K_\mathrm{A}}\langle k_\mathrm{A}|\big)\otimes\big(|k_\mathrm{B}\rangle_{K_\mathrm{B}\,K_\mathrm{B}}\langle k_\mathrm{B}|\big)\otimes\rho_\mathrm{E}^{k_\mathrm{A}k_\mathrm{B}}\,,$$
$$\rho_\mathrm{ABE}^{I_\mathrm{Q}}=\operatorname*{Tr}_{R_\mathrm{A}R_\mathrm{B}}\big(\rho_\mathrm{ABE}^{R_\mathrm{A}R_\mathrm{B}I_\mathrm{Q}}\big)=$$
$$=\sum_{k_\mathrm{A}}\sum_{k_\mathrm{B}}\frac{1}{|K_\mathrm{A}|}\,\delta_{k_\mathrm{A},k_\mathrm{B}}\big(|k_\mathrm{A}\rangle_{K_\mathrm{A}\,K_\mathrm{A}}\langle k_\mathrm{A}|\big)\otimes\big(|k_\mathrm{B}\rangle_{K_\mathrm{B}\,K_\mathrm{B}}\langle k_\mathrm{B}|\big)\otimes\rho_\mathrm{E}\,.$$

Полученное равенство является также следствием того факта, что матрица плотности имеет квантово-классическую структуру. Это означает, что классические сообщения после сеанса КРК с атакой *Man-in-the-Middle* относятся к разным сеансам "штатного" КРК и поэтому различимы.

Можно сказать, что на языке квантовых состояний полученное равенство есть следствие достоверной различимости (коммутативности – ортогональности) матриц плотности $g^{R_A m_{k_A}}$, $g^{R_B m_{k_B}}$ для пар (k_A, k_B) из разных сеансов КРК.

Матрица плотности $\rho_{ABE}^{R_Q}$ является финальной матрицей плотности после КРК, которая получается из исходной матрицы плотности после коррекции ошибок и усиления секретности. Принципиально то, что финальные ключи (k_A, k_B) могут не совпадать с заданной сколь угодно малой вероятностью, определяемой процедурой исправления ошибок.

Процесс КРК имеет несколько стадий.

После передачи и регистрации квантовых состояний происходит стадия коррекции ошибок. Возникает квантовое состояние, отвечающее так называемому просеянному ключу.

Затем проводится коррекция ошибок в просеянном ключе, возникает очищенный ключ. При этом длина очищенного ключа такая же, как длина просеянного ключа. Данной ситуации также отвечает своя матрица плотности.

Далее проводится проверка идентичности очищенного ключа. Очищенные ключи Алисы и Боба совпадают с определённой вероятностью, которая задаётся процедурой проверки.

В результате возникает очищенный и одинаковый (с заданной вероятностью) ключ у Алисы и Боба. Ева имеет частичную информацию об очищенном ключе, которую она получила при атаке на квантовый канал связи, а также классическую информацию из открытых сообщений, передаваемых Алисой к Бобу и Бобом к Алисе при коррекции ошибок.

Финальная стадия — усиление секретности очищенного ключа. Данная процедура приводит к сжатию очищенного ключа. Сжатие реализуется универсальными хэш-функциями второго порядка [38] через открытый классический канал связи. Данная информация доступна Еве. Для выбора хэш-функции $f \in \mathcal{F}$, которая сама является случайной величиной, Алиса выбирает случайную битовую строку. В итоге возникает финальная матрица плотности $\rho_{ABE}^{R_Q}$, фигурирующая в (11).

В реальности выбор хэш-функции происходит в соответствии с распределением $\varepsilon_{\mathcal{F}}$, близким к равновероятному. Данный факт будет учтён в разделе 7.

6.1. Корректность распределения ключей

Таким образом, следовое расстояние между процессами разбивается на сумму следовых расстояний между отдельными составными процессами в (11).

С некоторой вероятностью ключи Алисы и Боба отличаются друг от друга. Это формализуется видом матрицы плотности:

$$\rho_{ABE}^{R_Q} = \sum_{k_A \in \{0,1\}^\ell} \sum_{k_B \in \{0,1\}^\ell} P_{K_A K_B}(k_A, k_B) |k_A\rangle_{A\,A}\langle k_A| \otimes \\ \otimes |k_B\rangle_{B\,B}\langle k_B| \otimes \rho_E^{k_A k_B}. \tag{12}$$

Введём матрицу плотности следующего вида:

$$\overline{\rho_{ABE}^{R_Q}} = \sum_{k_A \in \{0,1\}^\ell} \sum_{k_B \in \{0,1\}^\ell} P_{K_A K_B}(k_A, k_B) \big(|k_A\rangle_{A\,A}\langle k_A|\big) \otimes \\ \otimes \big(|k_A\rangle_{B\,B}\langle k_A|\big) \otimes \rho_E^{k_A k_B}. \tag{13}$$

В (13) фигурируют одинаковые состояния $|k_A\rangle_A$ и $|k_A\rangle_B$.

Используя неравенство треугольника для (11), можно оценить следовое расстояние как

$$||\rho_{ABE}^{R_Q} - \rho_{ABE}^{I_Q}||_1 \leqslant \\ \leqslant ||\rho_{ABE}^{R_Q} - \overline{\rho_{ABE}^{R_Q}}||_1 + ||\overline{\rho_{ABE}^{R_Q}} - \rho_{ABE}^{I_Q}||_1. \tag{14}$$

Матрицу плотности, отвечающую квантовому распределению ключей через идеальный квантовый канал связи, можно представить в виде

$$\rho_{ABE}^{I_Q} = \rho_{UAB}^{I_Q} \otimes \rho_E, \tag{15}$$

$$\rho_{UAB}^{I_Q} = \frac{1}{|K_A|} \sum_{k_A} |k_A\rangle_{A\,A}\langle k_A| \otimes |k_A\rangle_{B\,B}\langle k_A|,$$

$$\rho_E = \sum_{k_A} \sum_{k_B} P_{K_A K_B}(k_A, k_B)\, \rho_E^{k_A k_B}.$$

Используя связь следового расстояния и фиделити [29, 57], получаем, что следовое расстояние

$$||\rho_{ABE}^{R_Q} - \overline{\rho_{ABE}^{R_Q}}||_1 = \\ = \mathrm{Tr}\left\{\left| \sum_{k_A \in \{0,1\}^\ell} \sum_{k_B \in \{0,1\}^\ell} P_{K_A K_B}(k_A, k_B) |k_A\rangle_{A\,A}\langle k_A| \otimes \rho_E^{k_A k_B} \otimes \right.\right. \\ \left.\left. \otimes \big(|k_B\rangle_{B\,B}\langle k_B| - |k_A\rangle_{B\,B}\langle k_A|\big) \right|\right\} = \\ = \sum_{k_A \in \{0,1\}^\ell} \sum_{k_B \in \{0,1\}^\ell} P_{K_A K_B}(k_A, k_B) \times \\ \times \frac{1}{2}\,\mathrm{Tr}\left\{||k_B\rangle_{B\,B}\langle k_B| - |k_A\rangle_{B\,B}\langle k_A||\right\} = \\ = \sum_{k_A \in \{0,1\}^\ell} \sum_{k_B \in \{0,1\}^\ell} P_{K_A K_B}(k_A, k_B) \sqrt{1 - \big|{}_B\langle k_B|k_A\rangle_B\big|^2} = \\ = \sum_{k_A, k_B \in \{0,1\}^\ell, k_A \neq k_B} P_{K_A K_B}(k_A, k_B).$$

Таким образом получаем, что вероятность того, что ключ Алисы k_A отличается от ключа Боба k_B, равна

$$\Pr(k_A \neq k_B) = ||\rho_{ABE}^{R_Q} - \overline{\rho_{ABE}^{R_Q}}||_1 = \\ = \sum_{k_A, k_B \in \{0,1\}^\ell, k_A \neq k_B} P_{K_A K_B}(k_A, k_B) \leqslant \varepsilon_{\mathrm{corr}} \tag{16}$$

и не превышает $\varepsilon_{\mathrm{corr}}$ — параметра протокола. Данная вероятность определяется выбором кода коррекции ошибок и процедурой проверки идентичности очищенного ключа.

Иначе говоря, формула (16) означает, что после коррекции ошибок и проверки идентичности очищенных ключей ключи одинаковы у Алисы и Боба с вероятностью не менее $1 - \varepsilon_{\mathrm{corr}}$.

В этом случае говорят, что протокол КРК является $\varepsilon_{\mathrm{corr}}$-корректным.

Далее, с учётом (13) и (15), прямым вычислением убеждаемся, что

$$
\begin{aligned}
&||\overline{\rho_{\mathrm{ABE}}^{R_{\mathrm{Q}}}} - \rho_{\mathrm{ABE}}^{I_{\mathrm{Q}}}||_1 = \\
&= \mathrm{Tr}\left\{\left|\sum_{k_{\mathrm{A}}\in\{0,1\}^{\ell}}\sum_{k_{\mathrm{B}}\in\{0,1\}^{\ell}} P_{K_{\mathrm{A}}K_{\mathrm{B}}}(k_{\mathrm{A}},k_{\mathrm{B}})\big(|k_{\mathrm{A}}\rangle_{\mathrm{A}\,\mathrm{A}}\langle k_{\mathrm{A}}|\big)\otimes\right.\right. \\
&\otimes\big(|k_{\mathrm{A}}\rangle_{\mathrm{B}\,\mathrm{B}}\langle k_{\mathrm{A}}|\big)\otimes\rho_{\mathrm{E}}^{k_{\mathrm{A}}k_{\mathrm{B}}} - \\
&\left.\left.-\frac{1}{|K_{\mathrm{A}}|}\sum_{k_{\mathrm{A}}}|k_{\mathrm{A}}\rangle_{\mathrm{A}\,\mathrm{A}}\langle k_{\mathrm{A}}|\otimes|k_{\mathrm{A}}\rangle_{\mathrm{B}\,\mathrm{B}}\langle k_{\mathrm{A}}|\otimes\rho_{\mathrm{E}}\right|\right\} = \\
&= \sum_{k_{\mathrm{A}}\in\{0,1\}^{\ell}}\mathrm{Tr}\left\{\left|\sum_{k_{\mathrm{B}}}P_{K_{\mathrm{A}}K_{\mathrm{B}}}(k_{\mathrm{A}},k_{\mathrm{B}})\,\rho_{\mathrm{E}}^{k_{\mathrm{A}}k_{\mathrm{B}}} - \frac{1}{|K_{\mathrm{A}}|}\,\rho_{\mathrm{E}}\right|\right\} = \\
&= \sum_{k_{\mathrm{A}}\in\{0,1\}^{\ell}}\mathrm{Tr}\left\{\left|P_{K_{\mathrm{A}}}(k_{\mathrm{A}})\,\rho_{\mathrm{E}}^{k_{\mathrm{A}}} - \frac{1}{|K_{\mathrm{A}}|}\,\rho_{\mathrm{E}}\right|\right\} = \\
&= ||\overline{\rho_{\mathrm{AE}}^{R_{\mathrm{Q}}}} - \rho_{\mathrm{AE}}^{I_{\mathrm{Q}}}||_1 = ||\rho_{\mathrm{AE}}^{R_{\mathrm{Q}}} - \rho_{\mathrm{AE}}^{I_{\mathrm{Q}}}||_1 \leqslant \varepsilon_{\mathrm{QKD}}\,, \qquad (17)
\end{aligned}
$$

где

$$
\rho_{\mathrm{AE}}^{I_{\mathrm{Q}}} = \rho_{\mathrm{UA}}\otimes\rho_{\mathrm{E}}\,,\quad \rho_{\mathrm{UA}} = \operatorname*{Tr}_{\mathrm{B}}\{\rho_{\mathrm{UAB}}\}\,,\quad \rho_{\mathrm{AE}}^{R_{\mathrm{Q}}} = \operatorname*{Tr}_{\mathrm{B}}\{\rho_{\mathrm{ABE}}^{R_{\mathrm{Q}}}\}\,, \qquad (18)
$$

а $\varepsilon_{\mathrm{QKD}}$ — параметр ε-секретности квантового ключа, которая фигурирует в доказательствах секретности протоколов КРК при

1) идеальном аутентичном канале классической связи,

2) при условии, что финальные квантовые ключи совпадают,

3) при идеальном выборе хэш-функции.

Таким образом, расстояние между неидеальным и идеальным распределением (17) позволяет исключить из рассмотрения Боба и оставить только состояния Алисы и Евы.

7. Расстояние между матрицами плотности после усиления секретности ключей

Теперь, учитывая (17), мы можем рассматривать только состояния исходного очищенного ключа Алисы, которые являются эталонными. Очищенный ключ Боба совпадает с вероятностью не менее, чем $1-\varepsilon_{\mathrm{corr}}$, с ключом Алисы.

Обозначим исходную эталонную битовую строку Алисы как $|k\rangle = |k_1\rangle\otimes|k_2\rangle\otimes\ldots\otimes|k_n\rangle$, где $k_i = 0,1$ — битовые позиции очищенного ключа, число позиций в нём n.

Обозначим матрицу плотности Алиса–Ева после коррекции ошибок — матрицу плотности с очищенным ключом, но до усиления секретности очищенного ключа (индекс А далее для краткости опускаем) через

$$
\rho_{K\mathrm{E}}^{R_{\mathrm{Q}}} = \sum_{k\in\{0,1\}^n} P_K(k)|k\rangle\langle k|\otimes\rho_{\mathrm{E}}^{k}\,, \qquad (19)
$$

соответственно, матрица плотности для идеальной ситуации есть

$$
\begin{aligned}
&\rho_{K\mathrm{E}}^{I_{\mathrm{Q}}} = \rho_{\mathrm{U}}\otimes\hat{\rho}_{\mathrm{E}}\,,\quad \rho_{\mathrm{U}} = \frac{1}{|\mathcal{K}|}\sum_{k\in\{0,1\}^n}|k\rangle\langle k|\,, \\
&\hat{\rho}_{\mathrm{E}} = \sum_{k\in\{0,1\}^n} P_K(k)\,\rho_{\mathrm{E}}^{k}\,.
\end{aligned} \qquad (20)
$$

После усиления секретности длина секретного финального ключа становится меньше и равна ℓ бит. Соответственно, квантовое состояние, отвечающее финальному секретному ключу, имеет вид

$$
|k_{\mathrm{A}}\rangle_{\mathrm{A}} = |k_{1\mathrm{A}}\rangle_{\mathrm{A}}\otimes|k_{2\mathrm{A}}\rangle_{\mathrm{A}}\otimes\ldots\otimes|k_{\ell\mathrm{A}}\rangle_{\mathrm{A}}\,,
$$

где $\ell < n$ — длина финального секретного ключа.

7.1. Универсальные хэш-функции второго порядка

При усилении секретности (privacy amplification) используются универсальные хэш-функции второго порядка U_2 (two-universal hash functions [38]).

В идеальном случае хэш-функция $\{f\colon\{0,1\}^n\to\{0,1\}^{\ell}\}$ выбирается случайно и равновероятно из соответствующего множества хэш-функций.

Тогда для любых битовых строк x и x', $x\neq x'$ длиной n имеет место неравенство

$$
\Pr\left[f\colon f(x)=f(x')\right] \leqslant \sum_{f\colon f(x)=f(x')}\frac{1}{2^n} = \frac{1}{2^{\ell}}\,. \qquad (21)
$$

7.1.1. Пример реализации универсальных хэш-функций второго порядка. Процедура случайного выбора хэш-функции состоит в следующем.

Сжимаемой битовой строке $x = (x_0, x_1, \ldots, x_{n-1}) \in \in \{0,1\}^n$ сопоставляется полином

$$
P_{n-1}(y) = x_0 + x_1 y + x_2 y^2 + \ldots + x_n y^{n-1}
$$

$P_{n-1}(y)$ степени $n-1$ как элемент поля Галуа $GF(2^n)$.

Генерируется случайная битовая строка $z = (z_0, z_1, \ldots, z_n) \in \{0,1\}^n$, которой сопоставляется соответствующий элемент поля — полином

$$
R_{n-1}(y) = z_0 + z_1 y + z_2 y^2 + \ldots + z_n y^{n-1}\,.
$$

Вычисляется произведение полиномов $P_{n-1}(y)$ и $R_{n-1}(y)$ в поле $GF(2^n)$ как остаток от деления произведения многочленов на неприводимый полином $IR_n(y)$:

$$
\mathrm{Res}_{n-1}(y) = P_{n-1}(y)R_{n-1}(y)\bmod IR_n(y)\,.
$$

Обозначим коэффициенты полинома $\mathrm{Res}_{n-1}(y)$ через $k = (k_0, k_1, \ldots, k_{n-1}) \in \{0,1\}^n$.

Из этой битовой строки оставляются ℓ младших позиций, которые и представляют результат сжатия хэш-функцией

$$
\mathcal{F} = \left\{f\colon\{0,1\}^n\to\{0,1\}^{\ell}\right\}.
$$

7.2. Следовое расстояние после усиления секретности

Поскольку выбор хэш-функции требует случайной битовой строки, которая также является неидеально случайной, то следовое расстояние (17) включает в себя также неидеальность случайной строки при выборе хэш-функций.

Матрица плотности после реального сеанса КРК и усиления секретности при реальном выборе хэш-функций в соответствии с распределением $P_{\mathcal{F}}^{R}(f)$ равна

$$
\rho_{\mathrm{AE}}^{R_{\mathrm{Q}}} = \rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{R_{\mathcal{F}}R_{\mathrm{Q}}} = \sum_{f\in\mathcal{F}} P_{\mathcal{F}}^{R}(f)\,|f\rangle_{FF}\langle f|\otimes\rho_{f\mathrm{E}}\,, \qquad (22)
$$

$$
\rho_{f\mathrm{E}} = \sum_{k_{\mathrm{A}}\in\{0,1\}^{\ell}} P_{K_{\mathrm{A}}}(k_{\mathrm{A}})|k_{\mathrm{A}}\rangle\langle k_{\mathrm{A}}|\otimes\rho_{\mathrm{E}}^{k_{\mathrm{A}}}\,,
$$

$$P_{K_\mathrm{A}}(k_\mathrm{A}) = \sum_{\{k:\, k\in f^{-1}(k_\mathrm{A})\in\{0,1\}^n\}} P_K(k)\,,$$

$$k_\mathrm{A} = f(k)\,,$$

$$\rho_\mathrm{E}^{k_\mathrm{A}} = \sum_{\{k:\, k\in f^{-1}(k_\mathrm{A})\in\{0,1\}^n\}} \frac{P_K(k)}{P_{K_\mathrm{A}}(k_\mathrm{A})}\,\rho_\mathrm{E}^k\,,$$

где в (22) набору хэш-функции f сопоставлены ортогональные квантовые состояния $|f\rangle_F$.

Матрица плотности после идеального сеанса КРК и усиления секретности при реальном выборе хэш-функций в соответствии с реальным распределением $P_\mathcal{F}^R(f)$ имеет вид

$$\rho_\mathrm{AE}^{I_\mathrm{Q}} = \rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{R_\mathcal{F} I_\mathrm{Q}} = \sum_{f\in\mathcal{F}} P_\mathcal{F}^R(f)\,|f\rangle_{FF}\langle f|\otimes\rho_{f\mathrm{U}}\otimes\overline{\rho_\mathrm{E}}\,, \quad (23)$$

$$\rho_{f\mathrm{U}} = \sum_{k_\mathrm{A}\in\{0,1\}^\ell}\left(\sum_{\{k:\, k\in f^{-1}(k_\mathrm{A})\in\{0,1\}^n\}}\frac{1}{|\mathcal{K}|}\right)|k_\mathrm{A}\rangle\langle k_\mathrm{A}|\,,$$

$$\overline{\rho_\mathrm{E}} = \sum_{k_\mathrm{A}\in\{0,1\}^\ell} P_{K_\mathrm{A}}(k_\mathrm{A})\,\rho_\mathrm{E}^{k_\mathrm{A}} = \sum_{\{k\in\{0,1\}^n\}} P_K(k)\,\rho_\mathrm{E}^k\,.$$

Матрица плотности после реального сеанса КРК и усиления секретности при идеальном равновероятном выборе хэш-функций в соответствии с равновероятным распределением $P_\mathcal{F}^I(f) = 1/|\mathcal{F}|$ принимает вид

$$\rho_\mathrm{AE}^{R_\mathrm{Q}} = \rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{I_\mathcal{F} R_\mathrm{Q}} = \sum_{f\in\mathcal{F}} P_\mathcal{F}^I(f)\,|f\rangle_{FF}\langle f|\otimes\rho_{f\mathrm{E}}\,, \quad (24)$$

$$P_\mathcal{F}^I(f) = \frac{1}{|\mathcal{F}|}\,.$$

Матрица плотности после идеального сеанса КРК и усиления секретности при реальном выборе хэш-функций в соответствии с равновероятным распределением $P_\mathcal{F}^I(f)$ равна

$$\rho_\mathrm{AE}^{I_\mathrm{Q}} = \rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{I_\mathcal{F} I_\mathrm{Q}} = \sum_{f\in\mathcal{F}} P_\mathcal{F}^I(f)\,|f\rangle_{FF}\langle f|\otimes\rho_{f\mathrm{U}}\otimes\overline{\rho_\mathrm{E}}\,. \quad (25)$$

Неидеальность при выборе хэш-функции даётся следовым расстоянием между реальным $P_\mathcal{F}^R(f)$ и идеальным $P_\mathcal{F}^I(f)$ распределениями:

$$||P_\mathcal{F}^R - P_\mathcal{F}^I||_1 = \sum_{f\in\mathcal{F}}\left|P_\mathcal{F}^R(f) - P_\mathcal{F}^I(f)\right| \leqslant \varepsilon_F\,. \quad (26)$$

До сжатия очищенного ключа k Ева "видит" состояния ρ_E^k — к каждому очищенному ключу k "привязано" состояние Евы ρ_E^k. После сжатия очищенного ключа: $k\in\{0,1\}^n \to k_\mathrm{A}\in\{0,1\}^\ell$ к каждому финальному ключу k_A "привязано" состояние Евы $\rho_\mathrm{E}^{k_\mathrm{A}}$ в (22).

Квантовое состояние $\rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{R_\mathcal{F} R_\mathrm{Q}}$ отвечает ситуации после усиления секретности, которая проводится для реальной матрицы плотности Алиса – Ева с вторжением Евы в квантовый канал связи и сжатием очищенных ключей с использованием реального (не строго равновероятного) распределения при выборе хэш-функций.

Второе состояние $\rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{I_\mathcal{F} I_\mathrm{Q}}$ отвечает идеальной ситуации КРК без вторжений Евы в квантовый канал, с последующим сжатием очищенного ключа и выбором хэш-функций в соответствии с равновероятным распределением.

Тогда прямым вычислением с учётом (22)–(26) получаем, что

$$\begin{aligned}
||\rho_\mathrm{AE}^{R_\mathrm{Q}} - \rho_\mathrm{AE}^{I_\mathrm{Q}}||_1 &= ||\rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{R_\mathcal{F} R_\mathrm{Q}} - \rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{I_\mathcal{F} I_\mathrm{Q}}||_1 \leqslant\\
&\leqslant ||\rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{R_\mathcal{F} R_\mathrm{Q}} - \rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{I_\mathcal{F} R_\mathrm{Q}}||_1 + ||\rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{I_\mathcal{F} R_\mathrm{Q}} - \rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{I_\mathcal{F} I_\mathrm{Q}}||_1 =\\
&= ||\rho_{(\mathcal{F}K)}^{R_\mathcal{F}} - \rho_{(\mathcal{F}K)}^{I_\mathcal{F}}||_1 + ||\rho_{(\mathcal{F}\mathrm{E})}^{R_\mathrm{Q}} - \rho_{(\mathcal{F}\mathrm{E})}^{I_\mathrm{Q}}||_1 =\\
&= ||P_\mathcal{F}^R - P_\mathcal{F}^I||_1 + ||\rho_{(\mathcal{F}\mathrm{E})}^{R_\mathrm{Q}} - \rho_{(\mathcal{F}\mathrm{E})}^{I_\mathrm{Q}}||_1 \leqslant\\
&\leqslant \varepsilon_F + ||\rho_{(\mathcal{F}\mathrm{E})}^{R_\mathrm{Q}} - \rho_{(\mathcal{F}\mathrm{E})}^{I_\mathrm{Q}}||_1\,, \qquad (27)
\end{aligned}$$

где

$$\rho_{(\mathcal{F}K)}^{R_\mathcal{F}} = \operatorname*{Tr}_{R_\mathrm{Q}}\left\{\rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{R_\mathcal{F} R_\mathrm{Q}}\right\},\quad \rho_{(\mathcal{F}K)}^{I_\mathcal{F}} = \operatorname*{Tr}_{R_\mathrm{Q}}\left\{\rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{I_\mathcal{F} R_\mathrm{Q}}\right\},$$

$$\rho_{(\mathcal{F}\mathrm{E})}^{R_\mathrm{Q}} = \operatorname*{Tr}_{I_\mathcal{F}}\left\{\rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{I_\mathcal{F} R_\mathrm{Q}}\right\},\quad \rho_{(\mathcal{F}\mathrm{E})}^{I_\mathrm{Q}} = \operatorname*{Tr}_{I_\mathcal{F}}\left\{\rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{I_\mathcal{F} I_\mathrm{Q}}\right\}.$$

Для оценки величины $||\rho_{(\mathcal{F}\mathrm{E})}^{R_\mathrm{Q}} - \rho_{(\mathcal{F}\mathrm{E})}^{I_\mathrm{Q}}||_1$ нам понадобится понятие сглаженной квантовой min-энтропии.

7.3. Сглаженная квантовая min-энтропия и лемма об остатке хэширования

Введём определение относительной min-энтропии [57].

Пусть ρ_AB и σ_B — матрицы плотности. Тогда

$$H_\mathrm{min}(\rho_\mathrm{AB}|\sigma_\mathrm{B}) = -\log\lambda\,, \quad (28)$$

где λ — минимальное число такое, что оператор

$$\lambda I_\mathrm{A}\otimes\sigma_\mathrm{B} - \rho_\mathrm{AB} > 0\,. \quad (29)$$

Как правило, в задачах квантовой информатики точный вид матриц плотности неизвестен.

Сглаженная условная min-энтропия определяется как

$$H_\mathrm{min}^\varepsilon(\rho_\mathrm{AB}|\sigma_\mathrm{B}) = \sup_{\tilde\rho_\mathrm{AB}} H_\mathrm{min}(\tilde\rho_\mathrm{AB}|\sigma_\mathrm{B})\,, \quad (30)$$

где верхняя грань берётся по квантовым состояниям таким, что матрицы плотности $\tilde\rho_\mathrm{AB}$ лежат в шаре

$$\mathcal{B}^\varepsilon(\rho_\mathrm{AB}) = \left\{\tilde\rho_\mathrm{AB} : ||\rho_\mathrm{AB} - \tilde\rho_\mathrm{AB}||_1 \leqslant \varepsilon\right\},$$

т.е. оценка $\tilde\rho_\mathrm{AB}$ близка к истинной матрице плотности ρ_AB в смысле малости расстояния $||\rho_\mathrm{AB} - \tilde\rho_\mathrm{AB}||_1 \leqslant \varepsilon$.

Здесь мы изучаем $||\rho_{(\mathcal{F}\mathrm{E})}^{R_\mathrm{Q}} - \rho_{(\mathcal{F}\mathrm{E})}^{I_\mathrm{Q}}||_1$ — следовое расстояние между реальной ситуацией при КРК (с учётом вторжения Евы) и идеальной ситуацией при идеальном выборе хэш-функции.

Пусть для некоторого ε' имеет место оценка истинной матрицы плотности (до сжатия и после коррекции ошибок):

$$||\rho_{K\mathrm{E}}^{R_\mathrm{Q}} - \tilde\rho_{K\mathrm{E}}^{R_\mathrm{Q}}||_1 \leqslant \varepsilon'\,.$$

Введём

$$\tilde\rho_{(\mathcal{F}\mathrm{E})}^{R_\mathrm{Q}} = \operatorname*{Tr}_{I_\mathcal{F}}\left\{\tilde\rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{I_\mathcal{F} R_\mathrm{Q}}\right\},\quad \tilde\rho_{(\mathcal{F}\mathrm{E})}^{I_\mathrm{Q}} = \operatorname*{Tr}_{I_\mathcal{F}}\left\{\tilde\rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{I_\mathcal{F} I_\mathrm{Q}}\right\}.$$

Матрица плотности $\tilde\rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{I_\mathcal{F} R_\mathrm{Q}}$ будет принадлежать шару размером не более ε'. А именно, поскольку любое хэширование является сжимающим отображением, то

имеет место неравенство

$$||\tilde{\rho}^{R_{\rm Q}}_{(\mathcal{F}{\rm E})} - \rho^{R_{\rm Q}}_{(\mathcal{F}{\rm E})}||_1 \leqslant ||\rho^{I_{\mathcal{F}}R_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})} - \tilde{\rho}^{I_{\mathcal{F}}R_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})}||_1 \leqslant$$
$$\leqslant ||\rho^{R_{\rm Q}}_{K{\rm E}} - \tilde{\rho}^{R_{\rm Q}}_{K{\rm E}}||_1 \leqslant \varepsilon'. \qquad (31)$$

Размер шара для матрицы $\tilde{\rho}^{I_{\mathcal{F}}I_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})}$ будет определён ниже. Введём матрицу плотности

$$\rho_{\mathcal{F}({\rm U}K)} = \sum_{f\in\mathcal{F}} P^I_{\mathcal{F}}(f)\,|f\rangle_{FF}\langle f|\otimes\rho_{f{\rm U}}\,.$$

Заметим, что

$$\rho^{I_{\mathcal{F}}I_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})} = \rho_{\mathcal{F}({\rm U}K)}\otimes\rho^{I_{\rm Q}}_{(\mathcal{F}{\rm E})}\,.$$

Тогда, используя неравенство треугольника, с учётом (31) получаем

$$||\rho^{R_{\rm Q}}_{(\mathcal{F}{\rm E})} - \rho^{I_{\rm Q}}_{(\mathcal{F}{\rm E})}||_1 = ||\rho^{I_{\mathcal{F}}R_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})} - \rho^{I_{\mathcal{F}}I_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})}||_1 \leqslant$$
$$\leqslant ||\,\rho^{I_{\mathcal{F}}R_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})} - \tilde{\rho}^{I_{\mathcal{F}}R_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})}||_1 +$$
$$+ ||\,\tilde{\rho}^{I_{\mathcal{F}}R_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})} - \rho_{\mathcal{F}({\rm U}K)}\otimes\tilde{\rho}^{I_{\rm Q}}_{(\mathcal{F}{\rm E})}||_1 +$$
$$+ ||\,\rho_{\mathcal{F}({\rm U}K)}\otimes\tilde{\rho}^{I_{\rm Q}}_{(\mathcal{F}{\rm E})} - \rho^{I_{\mathcal{F}}I_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})}||_1 =$$
$$= ||\,\rho^{I_{\mathcal{F}}R_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})} - \tilde{\rho}^{I_{\mathcal{F}}R_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})}||_1 +$$
$$+ ||\,\tilde{\rho}^{I_{\mathcal{F}}R_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})} - \rho_{\mathcal{F}({\rm U}K)}\otimes\tilde{\rho}^{I_{\rm Q}}_{(\mathcal{F}{\rm E})}||_1 + ||\,\tilde{\rho}^{I_{\rm Q}}_{(\mathcal{F}{\rm E})} - \rho^{I_{\rm Q}}_{(\mathcal{F}{\rm E})}||_1 \leqslant$$
$$\leqslant \varepsilon' + ||\,\tilde{\rho}^{I_{\mathcal{F}}R_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})} - \rho_{\mathcal{F}({\rm U}K)}\otimes\tilde{\rho}^{I_{\rm Q}}_{(\mathcal{F}{\rm E})}||_1 + ||\,\tilde{\rho}^{I_{\rm Q}}_{(\mathcal{F}{\rm E})} - \rho^{I_{\rm Q}}_{(\mathcal{F}{\rm E})}||_1\,. \qquad (32)$$

Мы стремимся получить минимальную верхнюю оценку для $||\rho^{R_{\rm Q}}_{(\mathcal{F}{\rm E})} - \rho^{I_{\rm Q}}_{(\mathcal{F}{\rm E})}||_1$. Поэтому в последнем неравенстве мы ищем минимальную верхнюю оценку для $||\tilde{\rho}^{I_{\mathcal{F}}R_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})} - \rho_{\mathcal{F}({\rm U}K)}\otimes\tilde{\rho}^{I_{\rm Q}}_{(\mathcal{F}{\rm E})}||_1$. Для оценки второго слагаемого в (32) воспользуемся квантовым вариантом знаменитой *Left over Hash Lemma* (см. детали в [57]). Получаем

$$||\,\tilde{\rho}^{I_{\mathcal{F}}R_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})} - \rho_{\mathcal{F}({\rm U}K)}\otimes\tilde{\rho}^{I_{\rm Q}}_{(\mathcal{F}{\rm E})}||_1 \leqslant$$
$$\leqslant \mathbf{E}_f\left[\left|\left|\sum_{k_{\rm A}\in\{0,1\}^\ell}|k_{\rm A}\rangle\langle k_{\rm A}|\left(\tilde{\rho}_{f{\rm E}} - \frac{1}{|\mathcal{K}_{\rm A}|}\,\overline{\tilde{\rho}_{\rm E}}\right)\right|\right|_1\right] =$$
$$= \sum_f P^I_F(f)\left[\left|\left|\sum_{k_{\rm A}\in\{0,1\}^\ell}|k_{\rm A}\rangle\langle k_{\rm A}|\left(\tilde{\rho}_{f{\rm E}} - \frac{1}{|\mathcal{K}_{\rm A}|}\,\overline{\tilde{\rho}_{\rm E}}\right)\right|\right|_1\right] \leqslant$$
$$\leqslant 2^{-(1/2)\left[H_{\min}(\tilde{\rho}_{K{\rm E}}|\tilde{\rho}_{\rm E}C)-\ell\right]}\,, \qquad (33)$$

где введены обозначения:

$$\overline{\tilde{\rho}_{\rm E}} = \sum_{k_{\rm A}\in\{0,1\}^\ell} P_{K_{\rm A}}(k_{\rm A})\,\tilde{\rho}^{k_{\rm A}}_{\rm E} = \sum_{\{k\in\{0,1\}^n\}} P_K(k)\,\tilde{\rho}^{k}_{\rm E}\,,$$

C — полное количество битов информации, передаваемой Алисой и Бобом через открытый аутентичный классический канал связи при исправлении ошибок, проверке корректности ключа и др., ℓ — длина финального секретного ключа после сжатия.

Для минимальной энтропии $H_{\min}(\tilde{\rho}_{K{\rm E}}|\tilde{\rho}_{\rm E}C)$ справедливо неравенство [57]

$$H_{\min}(\tilde{\rho}_{K{\rm E}}|\tilde{\rho}_{\rm E}C) \geqslant H_{\min}(\tilde{\rho}_{K{\rm E}}|\tilde{\rho}_{\rm E}) - C\,.$$

Поскольку неравенство (33) выполняется для любой $\tilde{\rho}_{K{\rm E}}$ из шара радиуса ε', то с учётом определения *сглаженной* min-энтропии (30) получаем, что

$$||\,\tilde{\rho}^{I_{\mathcal{F}}R_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})} - \rho_{\mathcal{F}({\rm U}K)}\otimes\tilde{\rho}^{I_{\rm Q}}_{(\mathcal{F}{\rm E})}||_1 \leqslant$$
$$\leqslant \min_{\tilde{\rho}_{K{\rm E}}}\left\{2^{-(1/2)[H_{\min}(\tilde{\rho}_{K{\rm E}}|\tilde{\rho}_{\rm E})-C-\ell]}\right\} =$$
$$= 2^{-(1/2)\left[\max_{\tilde{\rho}_{K{\rm E}}} H_{\min}(\tilde{\rho}_{K{\rm E}}|\tilde{\rho}_{\rm E})-C-\ell\right]} =$$
$$= 2^{-(1/2)\left[H^{\varepsilon'}_{\min}(\rho_{K{\rm E}}|\rho_{\rm E})-C-\ell\right]}\,. \qquad (34)$$

Обозначение $\mathbf{E}_f$ в (33) означает взятие математического ожидания — среднего по случайному выбору хэш-функции в соответствии с равновероятным распределением

$$P^I_F(f) = \frac{1}{|\mathcal{F}|}\,,\quad \mathbf{E}_f(\ldots) = \sum_{f\in\mathcal{F}}\frac{1}{|\mathcal{F}|}(\ldots)\,.$$

По сути, сглаженная условная min-энтропия $H^{\varepsilon'}_{\min}(\rho_{K{\rm E}}|\rho_{\rm E})$ имеет смысл *дефицита* информации Евы относительно битовой строки Алисы при условии, что Ева имеет в своём распоряжении квантовую систему $\rho_{\rm E}$.

Величина сглаженной условной min-энтропии содержит в себе всю информацию об атаках Евы на квантовый канал связи, включая утечку информации к Еве по побочным каналам [58].

Перейдём к оценке $||\tilde{\rho}^{I_{\rm Q}}_{(\mathcal{F}{\rm E})} - \rho^{I_{\rm Q}}_{(\mathcal{F}{\rm E})}||_1$ в (32).

Имеем

$$||\tilde{\rho}^{I_{\rm Q}}_{(\mathcal{F}{\rm E})} - \rho^{I_{\rm Q}}_{(\mathcal{F}{\rm E})}||_1 = \left|\left|\sum_{k_{\rm A}\in\{0,1\}^\ell} P_{K_{\rm A}}(k_{\rm A})\left(\tilde{\rho}^{k_{\rm A}}_{\rm E} - \rho^{k_{\rm A}}_{\rm E}\right)\right|\right|_1 \leqslant$$
$$\leqslant \sum_{k_{\rm A}\in\{0,1\}^\ell}\left|\left|P_{K_{\rm A}}(k_{\rm A})(\tilde{\rho}^{k_{\rm A}}_{\rm E} - \rho^{k_{\rm A}}_{\rm E})\right|\right|_1 =$$
$$= \left|\left|\sum_{k_{\rm A}\in\{0,1\}^\ell} P_{K_{\rm A}}(k_{\rm A})|k_{\rm A}\rangle\langle k_{\rm A}|\otimes(\rho^{k_{\rm A}}_{\rm E} - \tilde{\rho}^{k_{\rm A}}_{\rm E})\right|\right|_1 =$$
$$= \left|\left|\rho^{I_{\mathcal{F}}R_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})} - \tilde{\rho}^{I_{\mathcal{F}}R_{\rm Q}}_{(\mathcal{F}K)(\mathcal{F}{\rm E})}\right|\right|_1 \leqslant \left|\left|\rho^{R_{\rm Q}}_{K{\rm E}} - \tilde{\rho}^{R_{\rm Q}}_{K{\rm E}}\right|\right|_1 \leqslant \varepsilon'\,. \qquad (35)$$

Окончательно из (32) и оценок (34), (35) получаем для $||\rho^{R_{\rm Q}}_{(\mathcal{F}{\rm E})} - \rho^{I_{\rm Q}}_{(\mathcal{F}{\rm E})}||_1$ неравенство

$$||\rho^{R_{\rm Q}}_{(\mathcal{F}{\rm E})} - \rho^{I_{\rm Q}}_{(\mathcal{F}{\rm E})}||_1 \leqslant 2\varepsilon' + 2^{-(1/2)\left[H^{\varepsilon'}_{\min}(\rho_{K{\rm E}}|\rho_{\rm E})-C-\ell\right]}\,.$$

Величина $H^{\varepsilon'}_{\min}(\rho_{K{\rm E}}|\rho_{\rm E})$ возрастает с увеличением длины n очищенного ключа $k\in K$. При подходящем выборе n можно сделать величину

$$2\varepsilon' + 2^{-(1/2)\left[H^{\varepsilon'}_{\min}(\rho_{K{\rm E}}|\rho_{\rm E})-C-\ell\right]} \leqslant \overline{\varepsilon}\,.$$

7.4. Вычисление условной сглаженной min-энтропии

Сглаженная условная min-энтропия вычисляется на матрицах плотности $\tilde{\rho}^{R_{\rm Q}}_{K{\rm E}}$, ε'-близких в смысле следового расстояния $||\rho^{R_{\rm Q}}_{K{\rm E}} - \tilde{\rho}^{R_{\rm Q}}_{K{\rm E}}||_1 < \varepsilon'$ к матрице плотности $\rho^{R_{\rm QKD}}_{K{\rm E}}$.

Собирая вместе предыдущие результаты, получаем неравенство для следового расстояния между реальным и идеальным квантовым распределением ключей:

$$||\rho^{R_{\rm Q}}_{\rm ABE} - \rho^{I_{\rm Q}}_{\rm ABE}||_1 \leqslant \varepsilon_{\rm corr} + \overline{\varepsilon} + \varepsilon_F = \varepsilon_{\rm QKD}\,. \qquad (36)$$

Таким образом, расстояние $\bar{\varepsilon}$ между квантовым реальным распределением ключей с вторжением в квантовый канал связи и последующим усилением секретности увеличивается на $\varepsilon_{\text{corr}} + \varepsilon_F$, где:

— ε_F отвечает выбору хэш-функции второго порядка с использованием неидеальных ключей,

— $\varepsilon_{\text{corr}}$ — вероятность того, что финальные ключи Алисы и Боба не совпадают.

8. Расстояние между реальной и идеальной ситуациями при аутентификации

Прежде, чем перейти к вычислению расстояний $||\rho_{\text{ABE}}^{R_\text{A}R_\text{B}I_\text{Q}} - \rho_{\text{ABE}}^{R_\text{A}I_\text{B}I_\text{Q}}||_1$ в (5) и $||\rho_{\text{ABE}}^{R_\text{A}I_\text{B}I_\text{Q}} - \rho_{\text{ABE}}^{I_\text{A}I_\text{B}I_\text{Q}}||_1$ в (6), приведём необходимые для дальнейшего данные о классе хэш-функций, которые используются при теоретико-информационной аутентификации [47, 49, 50]. Данный класс составляют ключевые хэш-функции, которые используют при аутентификации секретный ключ k_s.

8.1. Определение хэш-функций для теоретико-информационно стойкой аутентификации

Пусть m — классическое сообщение, представляемое битовой строкой произвольной длины. Хэш-функция производит отображение любой строки m в битовую строку t фиксированной длины.

Функция хэширования $h_{k_\text{s}}(m)$, зависящая от секретного ключа k_s, называется ε-ASU_2 хэш-функцией, если при равновероятном выборе ключей k_s выполняются следующие условия.

1. Для любых m и t число хэш-функций (ключей k_s) таких, что $t = h_{k_\text{s}}(m)$, равно

$$\frac{|\mathcal{K}_\text{s}|}{|\mathcal{T}|}\,,$$

где $\mathcal{K}_\text{s}$, $\mathcal{T}$ — множество ключей и множество хэш-значений (тегов), $k_\text{s} \in \{0,1\}^{\log|\mathcal{K}_\text{s}|}$, $t \in \{0,1\}^{\log|\mathcal{T}|}$.

Пусть нарушитель выбирает произвольную пару (t,m) и пытается подобрать ключ k_s, при котором выполняется равенство $t = h_{k_\text{s}}(m)$. Вероятность навязывания (имитации, impersonation) по всем ключам есть

$$\Pr_{k_\text{s}}\left\{t = h_{k_\text{s}}(m)\right\} = \frac{1}{|\mathcal{T}|}\,. \tag{37}$$

Фактически из формулы (37) следует, что при любых (t,m) и равновероятном выборе ключей k_s число хэш-функций (ключей k_s), для которых выполняется равенство $t = h_{k_\text{s}}(m)$, равно $|\mathcal{K}_\text{s}|/|\mathcal{T}|$. Поэтому вероятность попасть в это подмножество при равновероятном выборе ключей k_s выражается как

$$\frac{|\mathcal{K}_\text{s}|}{|\mathcal{T}|}\,\frac{1}{|\mathcal{K}_\text{s}|} = \frac{1}{|\mathcal{T}|}\,.$$

2. Для любых $m \neq m'$ и любых t и t' (возможно, равных) и равновероятном выборе ключей k_s число хэш-функций, для которых $t = h_{k_\text{s}}(m)$ и $t' = h_{k_\text{s}}(m')$, составляет не более $\varepsilon|\mathcal{K}_\text{s}|/|\mathcal{T}|$.

Пусть нарушитель имеет легитимную пару (t,m), $t = h_{k_\text{s}}(m)$, не знает секретного ключа аутентификации k_s и хочет подменить тег и сообщение (t,m) на свою пару (t',m'). Вероятность подмены (substitution) по всем ключам удовлетворяет неравенству

$$P_{k_\text{s}}\left[t = h_{k_\text{s}}(m), t' = h_{k_\text{s}}(m')\right] < \frac{\varepsilon}{|\mathcal{T}|}\,. \tag{38}$$

В конечном счёте формула (38) отражает тот факт, что при любых (t,m), (t',m') ($m \neq m'$ и любых t и t') и равновероятном выборе ключей k_s число таких хэш-функций, для которых выполняется одновременно $t = h_{k_\text{s}}(m)$, $t' = h_{k_\text{s}}(m')$, не более $\varepsilon|\mathcal{K}_\text{s}|/|\mathcal{T}|$. Поэтому вероятность попасть в это подмножество при равновероятном выборе ключей k_s не более

$$\varepsilon\,\frac{|\mathcal{K}_\text{s}|}{|\mathcal{T}|}\,\frac{1}{|\mathcal{K}_\text{s}|} = \varepsilon\,\frac{1}{|\mathcal{T}|}\,.$$

Данные хэш-функции обеспечивают теоретико-информационную аутентификацию в том смысле, что, исходя из определений ε-ASU_2 хэш-функций, следует, что условная вероятность подмены (substitution) при условии наблюдения пары (m,t) не зависит от вычислительных возможностей подслушивателя, а зависит только от свойств множества хэш-функций $\mathcal{K}_\text{s}$ и не превосходит

$$P_{k_\text{s}}\left[t' = h_{k_\text{s}}(m') | t = h_{k_\text{s}}(m)\right] < \varepsilon\,. \tag{39}$$

8.2. Теоретико-информационная аутентификация в квантовом распределении ключей

Теперь подготовлен весь инструментарий, необходимый для вычисления расстояний между процессами аутентификации через реальный классический канал с возможной подменой сообщений нарушителем и процессами аутентификации через идеальный канал связи без подмены сообщений.

Вспомогательные классические сообщения в сеансе КРК передаются как от Алисы к Бобу, так и наоборот. Следовое расстояние между процессами $\rho_{\text{ABE}}^{R_\text{A}R_\text{B}I_\text{Q}}$ и $\rho_{\text{ABE}}^{R_\text{A}I_\text{B}I_\text{Q}}$ с учётом квантово-классической структуры состояний равно

$$||\rho_{\text{ABE}}^{R_\text{A}R_\text{B}I_\text{Q}} - \rho_{\text{ABE}}^{R_\text{A}I_\text{B}I_\text{Q}}||_1 = ||\rho_{\text{ABE}}^{R_\text{B}} - \rho_{\text{ABE}}^{I_\text{B}}||_1\,. \tag{40}$$

Аналогично для состояний $\rho_{\text{ABE}}^{R_\text{A}I_\text{B}I_\text{Q}}$ и $\rho_{\text{ABE}}^{I_\text{A}I_\text{B}I_\text{Q}}$ находим

$$||\rho_{\text{ABE}}^{R_\text{A}I_\text{B}I_\text{Q}} - \rho_{\text{ABE}}^{I_\text{A}I_\text{B}I_\text{Q}}||_1 = ||\rho_{\text{ABE}}^{R_\text{A}} - \rho_{\text{ABE}}^{I_\text{A}}||_1\,. \tag{41}$$

Задача фактически сводится к вычислению расстояния только между процессом, отвечающим передаче сообщений через классический канал с теоретико-информационной аутентификацией с возможной подменой состояний, и процессом передачи сообщений через канал без подмены сообщений.

Как будет видно далее, при теоретико-информационной аутентификации для следовых расстояний имеют место неравенства

$$||\rho_{\text{ABE}}^{R_\text{A}} - \rho_{\text{ABE}}^{I_\text{A}}||_1 \leqslant \varepsilon_{\text{Aut}}, \quad ||\rho_{\text{ABE}}^{R_\text{B}} - \rho_{\text{ABE}}^{I_\text{B}}||_1 \leqslant \varepsilon_{\text{Aut}}\,, \tag{42}$$

где ε_{Aut} — параметр секретности при аутентификации, явное выражение для которого будет приведено ниже.

В (42) достаточно оценить только первое следовое расстояние, оценка второго проводится аналогично.

Как уже отмечалось, теоретико-информационная аутентификация требует стартового секретного ключа k_s, который, вообще говоря, не является идеальным —

строго равновероятным, а лишь ε_{k_s}-близким к идеальному в смысле следового расстояния:

$$||P_{K_s} - P_{U_{K_s}}||_1 = \\ = \sum_{k_s \in \mathcal{K}_s} \left|P_{K_s}(k_s) - P_{U_{K_s}}(k_s)\right| \leqslant \varepsilon_{k_s}\,, \quad P_{U_{K_s}} = \frac{1}{|\mathcal{K}_s|}\,, \quad (43)$$

где параметр ε_{k_s} неидеальности ключа аутентификации определяется генератором случайных чисел, генерирующим стартовый ключ аутентификации.

Введём обозначение $\rho_{\text{ABE}}^{R_{\text{Aut}}^{\text{A}} R_{K_s}} = \rho_{\text{ABE}}^{R_{\text{A}}}$ — матрица плотности после аутентификации сообщений Алисы в реальном канале на реальных ключах аутентификации, $\rho_{\text{ABE}}^{I_{\text{Aut}}^{\text{A}} I_{K_s}} = \rho_{\text{ABE}}^{I_{\text{A}}}$ — матрица плотности после аутентификации сообщений Алисы в идеальном канале на идеальных ключах аутентификации. Для оценки первого следового расстояния в (42) нам потребуется ещё одно квантовое состояние, которое обозначим как $\rho_{\text{ABE}}^{R_{\text{Aut}}^{\text{A}} I_{K_s}}$ — матрица плотности после аутентификации сообщений Алисы в реальном канале на идеальных ключах аутентификации. Ниже покажем, что $||\rho_{\text{ABE}}^{R_{\text{Aut}}^{\text{A}} I_{K_s}} - \rho_{\text{ABE}}^{I_{\text{Aut}}^{\text{A}} I_{K_s}}||_1 < \varepsilon$ — параметра в определении ε-ASU_2 хэш-функции.

Тогда первое следовое расстояние в (42) с учётом (43) оценивается как

$$||\rho_{\text{ABE}}^{R_{\text{A}}} - \rho_{\text{ABE}}^{I_{\text{A}}}||_1 \leqslant \\ \leqslant ||\rho_{\text{ABE}}^{R_{\text{Aut}}^{\text{A}} R_{K_s}} - \rho_{\text{ABE}}^{R_{\text{Aut}}^{\text{A}} I_{K_s}}||_1 + ||\rho_{\text{ABE}}^{R_{\text{Aut}}^{\text{A}} I_{K_s}} - \rho_{\text{ABE}}^{I_{\text{Aut}}^{\text{A}} I_{K_s}}||_1 = \\ = ||P_{K_s} - P_{U_{K_s}}||_1 + ||\rho_{\text{ABE}}^{R_{\text{Aut}}^{\text{A}} I_{K_s}} - \rho_{\text{ABE}}^{I_{\text{Aut}}^{\text{A}} I_{K_s}}||_1 \leqslant \\ \leqslant \varepsilon_{k_s} + \varepsilon = \varepsilon_{\text{Aut}}\,. \quad (44)$$

Таким образом, стойкость теоретико-информационной аутентификации определяется параметром секретности ε_{Aut}, который включает в себя как параметр ε-ASU_2 хэш-функции, так и неидеальность ключа аутентификации.

Используя представление

$$\rho_{\text{ABE}}^{R_{\text{A}} R_{\text{B}} R_{\text{Q}}} = \sum_{k_{\text{A}}} \sum_{k_{\text{B}}} P_{K_{\text{A}} K_{\text{B}}}(k_{\text{A}}, k_{\text{B}}) |k_{\text{A}}\rangle_{K_{\text{A}} K_{\text{A}}} \langle k_{\text{A}}| \otimes \\ \otimes |k_{\text{B}}\rangle_{K_{\text{B}} K_{\text{B}}} \langle k_{\text{B}}| \otimes g^{R_{\text{A}} R_{K_s} m_{k_{\text{A}}}} \otimes g^{R_{\text{B}} R_{K_s} m_{k_{\text{B}}}} \otimes \rho_{\text{E}}^{k_{\text{A}} k_{\text{B}}}\,,$$

получаем, что

$$\rho_{\text{ABE}}^{R_{\text{A}}} = \rho_{\text{ABE}}^{R_{\text{Aut}}^{\text{A}} R_{K_s}} = \\ = \operatorname*{Tr}_{R_{\text{B}} R_{\text{Q}}} \{\rho_{\text{ABE}}^{R_{\text{A}} R_{\text{B}} R_{\text{Q}}}\} = \sum_{k_{\text{A}}} P_{K_{\text{A}}}(k_{\text{A}}) g^{R_{\text{A}} R_{K_s} m_{k_{\text{A}}}}\,.$$

Аналогично можно записать

$$\rho_{\text{ABE}}^{R_{\text{Aut}}^{\text{A}} I_{K_s}} = \sum_{k_{\text{A}}} P_{K_{\text{A}}}(k_{\text{A}}) g^{R_{\text{A}} I_{K_s} m_{k_{\text{A}}}}\,,$$

$$\rho_{\text{ABE}}^{I_{\text{Aut}}^{\text{A}} I_{K_s}} = \sum_{k_{\text{A}}} P_{K_{\text{A}}}(k_{\text{A}}) g^{I_{\text{A}} I_{K_s} m_{k_{\text{A}}}}$$

Данные матрицы плотности имеют прозрачную статистическую интерпретацию и смысл. Обсудим это на примере $\rho_{\text{ABE}}^{R_{\text{Aut}}^{\text{A}} I_{K_s}}$, аналогично для состояния $\rho_{\text{ABE}}^{I_{\text{Aut}}^{\text{A}} I_{K_s}}$.

Пусть проводится множество сеансов КРК. После каждого сеанса КРК Алиса имеет ключ k_{A}, который в каждом сеансе возникает с вероятностью $P_{K_{\text{A}}}(k_{\text{A}})$.

К каждому ключу в сеансе "привязан" набор классических сообщений, которому отвечает матрица плотности $g^{R_{\text{A}} I_{K_s} m_{k_{\text{A}}}}$. В каждом сеансе классические сообщения и их теги от Алисы к Бобу (m, t) и подменные сообщения (m', t') от Евы к Бобу задаются совместным условным распределением вероятностей $P_{MTM'T'}^{R_{\text{A}} I_{K_s}}(m, t, m', t' \,|\, k_{\text{A}})$ (см. следующую формулу) при заданном ключе k_{A} в каждом сеансе.

Как будет показано далее, следовое расстояние не зависит от конкретного вида распределения вероятностей, что является следствием использования ε-ASU_2 хэш-функций при аутентификации.

Учитывая сказанное, матрицу плотности $g^{R_{\text{A}} I_{K_s} m_{k_{\text{A}}}}$ для сообщений в канале аутентификации можно записать как

$$g^{R_{\text{A}} I_{K_s} m_{k_{\text{A}}}} = \sum_{k_s} \frac{1}{|\mathcal{K}_s|} |k_s\rangle_{K_s K_s} \langle k_s| \otimes \\ \otimes \sum_{((m,t),(m',t')) \in ((\mathcal{MT}),(\mathcal{M}'\mathcal{T}'))_{OK}} P_{MTM'T'}^{R_{\text{A}} I_{K_s}}(m, t, m', t' \,|\, k_{\text{A}}) \\ |m\rangle_{M\,M} \langle m| \otimes |t\rangle_{T\,T} \langle t| \otimes |m'\rangle_{M'\,M'} \langle m'| \otimes |t'\rangle_{T'\,T'} \langle t'|$$

и, следовательно,

$$\rho_{\text{ABE}}^{R_{\text{Aut}}^{\text{A}} I_{K_s}} = \sum_{k_s} \frac{1}{|\mathcal{K}_s|} |k_s\rangle_{K_s K_s} \langle k_s| \otimes \\ \otimes \sum_{((m,t),(m',t')) \in ((\mathcal{MT}),(\mathcal{M}'\mathcal{T}'))_{OK}} P_{MTM'T'}^{R_{\text{A}} I_{K_s}}(m, t, m', t') \\ |m\rangle_{M\,M} \langle m| \otimes |t\rangle_{T\,T} \langle t| \otimes |m'\rangle_{M'\,M'} \langle m'| \otimes |t'\rangle_{T'\,T'} \langle t'|\,, \quad (45)$$

где

$$P_{MTM'T'}^{R_{\text{A}} I_{K_s}}(m, t, m', t') = \sum_{k_{\text{A}}} P_{K_{\text{A}}}(k_{\text{A}}) P_{MTM'T'}^{R_{\text{A}} I_{K_s}}(m, t, m', t' \,|\, k_{\text{A}}).$$

Верхний индекс $R_{\text{A}} I_{K_s}$ в распределении вероятностей $P_{MTM'T'}^{R_{\text{A}} I_{K_s}}(m, t, m', t')$ отвечает ситуации реального канала аутентификации с подменой на идеальных ключах аутентификации.

Аналогично записывается матрица плотности:

$$\rho_{\text{ABE}}^{I_{\text{Aut}}^{\text{A}} I_{K_s}} = \sum_{k_s} \frac{1}{|\mathcal{K}_s|} |k_s\rangle_{K_s K_s} \langle k_s| \otimes \\ \otimes \sum_{((m,t),(m',t')) \in ((\mathcal{MT}),(\mathcal{M}'\mathcal{T}'))_{OK}} P_{MTM'T'}^{I_{\text{A}} I_{K_s}}(m, t, m', t') \\ |m\rangle_{M\,M} \langle m| \otimes |t\rangle_{T\,T} \langle t| \otimes |m'\rangle_{M'\,M'} \langle m'| \otimes |t'\rangle_{T'\,T'} \langle t'|\,. \quad (46)$$

Верхний индекс $I_{\text{A}} I_{K_s}$ в распределении вероятностей $P_{MTM'T'}^{I_{\text{A}} I_{K_s}}(m, t, m', t')$ отвечает ситуации идеального канала аутентификации без подмены на идеальных ключах аутентификации.

Учитывая (45) и (46), получаем для следового расстояния

$$||\rho_{\text{ABE}}^{R_{\text{A}}} - \rho_{\text{ABE}}^{I_{\text{A}}}||_1 = ||\rho_{\text{ABE}}^{R_{\text{Aut}}^{\text{A}} I_{K_s}} - \rho_{\text{ABE}}^{I_{\text{Aut}}^{\text{A}} I_{K_s}}||_1 = \quad (47)$$

$$= \Big|\Big| \sum_{k_s} \frac{1}{|\mathcal{K}_s|} |k_s\rangle_{K_s K_s} \langle k_s| \otimes \\ \otimes \sum_{((m,t),(m',t')) \in ((\mathcal{MT}),(\mathcal{M}'\mathcal{T}'))_{OK}} \big(P_{MTM'T'}^{R_{\text{A}} I_{K_s}}(m, t, m', t') -$$

$$
\begin{aligned}
&- P^{I_A I_{K_s}}_{MTM'T'}(m,t,m',t')\big) \\
&\quad |m\rangle_{MM}\langle m| \otimes |t\rangle_{TT}\langle t| \otimes |m'\rangle_{M'M'}\langle m'| \otimes |t'\rangle_{T'T'}\langle t'|\Big|\Big|_1 = \\
&= \sum_{k_s} \frac{1}{|\mathcal{K}_s|} \sum_{((m,t),(m',t'))\in((\mathcal{MT}),(\mathcal{M'T'}))_{OK}} \Big| P_{MT}(m,t) \times \\
&\times \left(P^{R_A I_{K_s}}_{M'T'|MT}(m',t'|m,t) - P^{I_A I_{K_s}}_{M'T'|MT}(m',t'|m,t)\right)\Big| \leqslant \\
&\leqslant \sum_{k_s} \frac{1}{|\mathcal{K}_s|} \sum_{(m'\neq m),((m,t),(m',t'))\in((\mathcal{MT}),(\mathcal{M'T'}))_{OK}} P^{R_A I_{K_s}}_{MTM'T'}(m,t,m',t'). \qquad (48)
\end{aligned}
$$

При переходе к последнему неравенству использован тот факт, что распределения для идеальной и реальной ситуаций совпадают при $m' = m$ (отсутствует подмена), $P_{MT}(m,t)$ — распределение вероятностей открытых сообщений и тегов (m,t), поступающих в классический канал связи от легитимного пользователя.

В формулах (45)–(48) индекс суммирования

$$\big((m,t),(m',t')\big) \in \big((\mathcal{MT}),(\mathcal{M'T'})\big)_{OK}$$

означает суммирование по элементам $(m,t),(m',t')$ множества $(\mathcal{MT}),(\mathcal{M'T'})$, где $t = h_{k_s}(m)$, $t' = h_{k_s}(m')$.

Иначе говоря, суммирование происходит по множеству сообщений и их тегов, которые отвечают прохождению проверки при аутентификации.

В оценке следового расстояния вероятности событий (исходов), которые не прошли проверку на аутентификацию, не учитываются.

Затем верхний индекс $R_A I_{K_s}$ для краткости заменяем на k_s, имея в виду зависимость вероятности $P^{R_A I_{K_s}}_{MTM'T'}(m,t,m',t')$ от ключа аутентификации.

Далее, аналогично работе [35], удобно вместо переменных m, t, m', t' ввести новые переменные m, m', $y = (m,t)$, $y' = (m',t')$ при фиксированном ключе аутентификации k_s.

Вероятность в (48) может быть переписана в эквивалентном виде с учётом новых переменных:

$$
\begin{aligned}
P^{k_s}_{MTM'T'}(m,t,m',t') &= P^{k_s}_{MT}(m,t) P^{k_s}_{MT|M'T'}(m',t'|m,t) = \\
&= P^{k_s}_{MYM'Y'}\big(m,(m,t),m',(m',t')\big) = \\
&= P_M(m) P^{k_s}_{Y|M}\big((m,t)|m\big) P^{k_s}_{Y'|MY}\big((m',t')|m,(m,t)\big) \\
&\quad P^{k_s}_{M'|MYY'}\big(m'|m,(m,t),(m't')\big). \qquad (49)
\end{aligned}
$$

Условные вероятности в (49) зависят от типа используемых хэш-функций. При фиксированном значении k_s условные вероятности в (49) могут быть представлены в эквивалентном виде:

$$P^{k_s}_{Y|M}\big((m,t)|m\big) = P^{k_s}_{T|M}(t|m) = P^{k_s}\big[t = h_{k_s}(m)\big], \qquad (50)$$

$$P^{k_s}_{Y'|MY}\big((m',t')|m,(m,t)\big) = P^{k_s}_{M'T'|MT}(m',t'|m,t), \qquad (51)$$

$$
\begin{aligned}
&P^{k_s}_{M'|MYY'}\big(m'|m,(m,t),(m',t')\big) = \\
&\qquad = P^{k_s}\big[t' = h_{k_s}(m')|t = h_{k_s}(m)\big]. \qquad (52)
\end{aligned}
$$

Вероятности $P^{k_s}[t = h_{k_s}(m)] \neq 0$, поскольку при суммировании по $(m,t),(m',t')$ отличные от нуля слагаемые появляются только для индексов $((m,t),(m',t')) \in ((\mathcal{MT}),(\mathcal{M'T'}))_{OK}$.

Вычисление следового расстояния по формулам (47), (48) с использованием (49)–(52) и определение ε-ASU_2 хэш-функции дают

$$
\begin{aligned}
&||\rho^{R_A}_{ABE} - \rho^{I_A}_{ABE}||_1 = \\
&= \sum_{k_s} \frac{1}{|\mathcal{K}_s|} \sum_{(m'\neq m),((m,t),(m',t'))\in((\mathcal{MT}),(\mathcal{M'T'}))_{OK}} P^{k_s}_{MTM'T'}(m,t,m',t') = \\
&= \sum_{m,t,m'\neq m,t'} P_M(m) P_{M'T'|MT}(m',t'|m,t) \times \\
&\times \left(\sum_{k_s} \frac{1}{|\mathcal{K}_s|} P^{k_s}\big[t = h_{k_s}(m)\big] P^{k_s}\big[t' = h_{k_s}(m')|t = h_{k_s}(m)\big]\right) = \\
&= \sum_{(m'\neq m),((m,t),(m',t'))\in((\mathcal{MT}),(\mathcal{M'T'}))_{OK}} P_M(m) P_{M'T'|MT}(m',t'|m,t) \times \\
&\times \left(\sum_{k} \frac{1}{|\mathcal{K}_s|} P^{k_s}\big[t' = h_{k_s}(m'), t = h_{k_s}(m)\big]\right) = \\
&= \sum_{(m'\neq m),((m,t),(m',t'))\in((\mathcal{MT}),(\mathcal{M'T'}))_{OK}} P_M(m) P_{M'T'|MT}(m',t'|m,t) \times \\
&\times P_{K_s}\big[t' = h_{k_s}(m'), t = h_{k_s}(m)\big] < \ldots \qquad (53)
\end{aligned}
$$

Для ε-ASU_2 хэш-функций, согласно (38), имеем

$$P_{K_s}\big[t' = h_{k_s}(m'), t = h_{k_s}(m)\big] < \frac{\varepsilon}{|\mathcal{T}|}, \qquad (54)$$

тогда, продолжая (53), получаем

$$
\begin{aligned}
\ldots &< \sum_t \sum_m P_M(m) \sum_{m',t'} P_{M'T'|MT}(m',t'|m,t) \frac{\varepsilon}{|\mathcal{T}|} = \\
&= \sum_t \frac{\varepsilon}{|\mathcal{T}|} = |\mathcal{T}| \frac{\varepsilon}{|\mathcal{T}|} = \varepsilon. \qquad (55)
\end{aligned}
$$

В (55) учтена нормировка распределений вероятностей

$$\sum_m P_M(m) = 1, \quad \sum_{m',t'} P_{M'T'|MT}(m',t'|m,t) = 1.$$

Собирая вместе (43), (44) и (55), получаем

$$||\rho^{R_A}_{ABE} - \rho^{I_A}_{ABE}||_1 = ||\rho^{R^A_{Aut} R_{K_s}}_{ABE} - \rho^{I^A_{Aut} I_{K_s}}_{ABE}||_1 \leqslant \varepsilon_{k_s} + \varepsilon = \varepsilon_{Aut}. \qquad (56)$$

Аналогично предыдущему, получаем

$$||\rho^{R_B}_{ABE} - \rho^{I_B}_{ABE}||_1 = ||\rho^{R^B_{Aut} R_{K_s}}_{ABE} - \rho^{I^B_{Aut} I_{K_s}}_{ABE}||_1 \leqslant \varepsilon_{k_s} + \varepsilon = \varepsilon_{Aut}. \qquad (57)$$

Таким образом, расстояние между реальной ε-стойкой теоретико-информационной аутентификацией с возможной подменой сообщений, использующей реальные ε_{k_s}-секретные ключи, и идеальной аутентификацией без подмены сообщений, использующей идеальные — строго равновероятные ключи, не превышает $\varepsilon_{k_s} + \varepsilon = \varepsilon_{Aut}$ (56), (57).

8.3. Пример реализации теоретико-информационно стойкой аутентификации

Для экономии одноразового ключа аутентификации можно использовать реализацию ε-ASU_2 хэш-функции как композицию ε-AXU_2 функции с постоянным (reused key) ключом для получения *промежуточного* тега и операцией XOR для получения *финального* тега.

Хэш-функция $t = h_k(m)$, $t \in \{0,1\}^{\log(|\mathcal{T}|)}$ является хэш-функцией ε-AXU$_2$, если для любых $m \neq m'$ и $c \in \{0,1\}^{\log(|\mathcal{T}|)}$ имеет место неравенство

$$\Pr_k \left[h_k(m) \oplus h_k(m') = c\right] \leqslant \varepsilon\,.$$

При $\varepsilon = 1/|\mathcal{T}|$ хэш-функция ε-AXU$_2$ становится (называется) ε-XU$_2$ хэш-функцией.

В свою очередь, функция ε-AXU$_2$ реализуется как композиция ε_1-AU$_2$ хэш-функции $h^{(1)}_{k_1}(...)$ и ε_2-XU$_2$ хэш-функции $h^{(2)}_{k_2}(...)$ с промежуточным тегом $t^{(1,2)} = h^{(2)}_{k_2}(h^{(1)}_{k_1}(m))$ и с постоянным ключом (k_1, k_2) (см. определение ниже).

Хэш-функция $t = h_{k_1}(m)$, $t \in \{0,1\}^{\log(|\mathcal{T}_1|)}$ является ε_1-AU$_2$ хэш-функцией, если для любых $m \neq m'$ имеет место неравенство

$$\Pr_{k_1} \left[h_{k_1}(m) = h_{k_1}(m')\right] \leqslant \varepsilon_1\,.$$

При $\varepsilon_1 = 1/|\mathcal{T}_1|$ хэш-функция ε_1-AU$_2$ становится U$_2$ хэш-функцией — универсальной хэш-функцией второго порядка (см. раздел 7.1).

Композиция двух ε_2-XU$_2$ и ε_1-AU$_2$ хэш-функций даёт $(\varepsilon_1 + \varepsilon_2)$-AXU$_2$ хэш-функцию с промежуточным тегом $t^{(1,2)}$.

Как будет показано, такая процедура приводит к довольно "щадящим" оценкам длины двоичного одноразового ключа для теоретико-информационной аутентификации.

8.3.1. Реализация ε-ASU$_2$ хэш-функции посредством композиции ε-AXU$_2$ хэш-функции с операцией XOR. Для хэш-функции ε-AXU$_2$ используется один и тот же ключ во время всех сеансов аутентификации. Ключ для шифрования промежуточного тега используется как одноразовый в каждом сеансе аутентификации.

Доказывается [52], что после шифрования одноразовым ключом k_s — применения операции XOR к промежуточному тегу $t^{(1,2)}$, а именно

$$t = t^{(1,2)} \oplus k_s = h^{(2)}_{k_2}(h^{(1)}_{k_1}(m)) \oplus k_s\,,$$

хэш-функция $t = h_{k_s}(m) = h^{(2)}_{k_2}(h^{(1)}_{k_1}(m)) \oplus k_s$ является ε-ASU$_2$ хэш-функцией.

Отсюда следует, что при равновероятном выборе ключей k_s имеет место неравенство

$$\Pr_{k_s,k_2,k_1} \left[t' = h^{(2)}_{k_2}(h^{(1)}_{k_1}(m')) \oplus k_s\,, t = h^{(2)}_{k_2}(h^{(1)}_{k_1}(m)) \oplus k_s\right] < \frac{\varepsilon}{|\mathcal{T}|}\,. \tag{58}$$

Ключи (k_1, k_2) являются одинаковыми во всех сеансах, ключ k_s — одноразовый ключ, который меняется в каждом сеансе.

Соответственно, условная вероятность при хэшировании ε-ASU$_2$ хэш-функцией, по определению, удовлетворяет неравенству

$$\Pr_{k_s,k_2,k_1} \left[t' = h^{(2)}_{k_2}(h^{(1)}_{k_1}(m')) \oplus k_s | t = h^{(2)}_{k_2}(h^{(1)}_{k_1}(m)) \oplus k_s\right] < \varepsilon\,. \tag{59}$$

8.3.2. Пример построения ε-ASU$_2$ хэш-функции как композиции ε-AU$_2$ и ε-XU$_2$ функций и операции XOR.

1. Реализация $h^{(1)}_{k_1}(...)$ как ε_1-AU$_2$ функции.

Используем полиномиальное хэширование PolyCW [44, 50].

Пусть сообщение — битовая строка длиной M, длина постоянного ключа — k_1 битов.

Если длина сообщения M не является степенью двойки, то сообщение дополняется так, чтобы

$$\frac{(M||1||0^m)}{k_1} = n_1 + 1 \tag{60}$$

было целым числом.

Далее для экономии обозначений будем считать, что M нацело делится на k_1.

В итоге возникает последовательность битовых блоков $(m_0, m_1, \ldots, m_n)$, каждый длиной k_1 битов.

Каждой паре блоков (k_1, m_i) сопоставляется полином степени $k_1 - 1$ по следующему правилу:

— берётся неприводимый полином $IP(2^{k_1})$ в поле $GF(2^{k_1})$,

— вычисляется

$$y = (m_0 k_1^n + m_1 k_1^{n-1} + \ldots + m_n k_1^0) \bmod IP_1(2^{k_1})\,. \tag{61}$$

Все указанные действия производятся в поле $GF(2^{k_1})$, где каждой битовой строке ставится в соответствие полином в этом поле.

В итоге возникает битовая строка y, число битовых позиций есть k_1.

Таким образом реализуется хэш-функция ε_1-AU$_2$ с параметром

$$\varepsilon_1 = \frac{n_1}{2^{k_1}}\,, \tag{62}$$

где n_1 определено в (60).

2. Реализация $h^{(2)}_{k_2}(...)$ как ε_2-XU$_2$ хэш-функции.

Для уменьшения длины одноразового ключа k_s производится сжатие y длиной k_1 битов до длины k_s битов, которые затем шифруются операцией XOR на одноразовом ключе k_s.

Мы строим хэш-функцию $h^{(2)}_{k_2}(...)$.

Положим длины $k_2 = k_1$. Возьмём неприводимый полином $IP_2(2^{k_1})$ в поле $GF(2^{k_1})$.

Выберем случайным образом полином $RP_2(2^{k_1})$ в поле $GF(2^{k_1})$ степени $k_1 - 1$. Вычисляем

$$z = y\, RP_2(2^{k_1}) \bmod IP_2(2^{k_1})\,. \tag{63}$$

Из результирующей битовой строки z длиной k_1 битов оставляем k_s младших битовых позиций — битовую строку z_{k_s}. Данная битовая строка длиной k_s битов шифруется одноразовым ключом k_s, получается тег t,

$$t = z_{k_s} \oplus k_s\,.$$

Результатом является реализация ε-ASU$_2 = (\varepsilon_1 + \varepsilon_2)$-ASU$_2$ функции, где

$$\varepsilon = \varepsilon_1 + \varepsilon_2 = \frac{n_1}{2^{k_1}} + \frac{1}{2^{k_s}} = \frac{n_1}{2^{k_1}} + \frac{1}{|\mathcal{T}|}\,. \tag{64}$$

Полная длина ключа аутентификации

$$k_{\text{Aut}} = 2\,k_1 + k_s\,, \tag{65}$$

где постоянный ключ (reused key) (k_1, k_2) длины $2k_1$ и одноразовый ключ в каждом сеансе k_s; здесь считаем, что $k_1 = k_2$.

Таким образом, вероятность подмены сообщений определяется ключом аутентификации (65), который состоит из двух ключей: постоянного ключа (k_1, k_2) — данный ключ одинаков во всех сеансах, и одноразового ключа k_s, который меняется в каждом сеансе КРК и берётся как часть ключа, полученного в предыдущем сеансе КРК.

9. Сколько сеансов квантового распределения ключей можно провести, имея один стартовый ключ аутентификации?

Курица не птица, логарифм не бесконечность
Биографы приписывают
данный афоризм А. Эйнштейну

Собирая вместе результаты предыдущих разделов, получаем, что после первого сеанса КРК следовое расстояние между 1) реальной ситуацией КРК с вторжением в квантовый канал связи вместе с реальной теоретико-информационной аутентификацией с возможной подменой классических сообщений и 2) соответствующей идеальной ситуацией, удовлетворяет неравенству

$$||\rho_{\mathrm{ABE}}^{R_{\mathrm{Aut}}^{\mathrm{A}} R_{\mathrm{Aut}}^{\mathrm{B}} R_{\mathrm{QKD}}^{\mathrm{AB}}} - \rho_{\mathrm{ABE}}^{I_{\mathrm{Aut}}^{\mathrm{A}} I_{\mathrm{Aut}}^{\mathrm{B}} I_{\mathrm{QKD}}^{\mathrm{AB}}}||_1 \leqslant \leqslant 2(\varepsilon_{k_s} + \varepsilon) + \varepsilon_{\mathrm{QKD}} = \varepsilon_{\mathrm{Aut}} + \varepsilon_{\mathrm{QKD}} . \quad (66)$$

Величина $\varepsilon_{\mathrm{Aut}} = 2(\varepsilon_{k_s} + \varepsilon)$ возникает при учёте неидеальности одноразовых ε_{k_s}-секретных ключей аутентификации, параметр ε определяет свойства ε-ASU_2 хэш-функций и не зависит от секретного ключа, коэффициент 2 возникает за счёт обмена классическими сообщениями от Алисы к Бобу и от Боба к Алисе.

Величина $\varepsilon_{\mathrm{QKD}} = \varepsilon_{\mathrm{corr}} + \varepsilon_F + \overline{\varepsilon}$ отвечает за все неидеальности при квантовом распределении ключей при идеальной аутентификации.

Далее введём обозначения $\overline{\varepsilon}_{k_s} = 2\varepsilon_{k_s}$, $\varepsilon_\Sigma = 2\varepsilon + \varepsilon_{\mathrm{QKD}}$.

После первого запуска системы КРК получаем $\varepsilon(1)$-секретный квантовый ключ, где

$$\varepsilon(1) = \overline{\varepsilon}_{k_s} + \varepsilon_\Sigma .$$

Во втором сеансе КРК для аутентификации используется часть $\varepsilon(1)$-секретного квантового ключа из первого сеанса. Важно отметить, что любая часть $\varepsilon(1)$-секретного квантового ключа также обладает свойством $\varepsilon(1)$-секретности.

После второго сеанса КРК получается $\varepsilon(2)$-секретный квантовый ключ, где

$$\varepsilon(2) = \varepsilon(1) + \varepsilon_\Sigma = \overline{\varepsilon}_{k_s} + 2\varepsilon_\Sigma .$$

Аналогичным образом, после N-го сеанса КРК получается $\varepsilon(N)$-секретный квантовый ключ, где

$$\varepsilon(N) = \overline{\varepsilon}_{k_s} + N\varepsilon_\Sigma = \overline{\varepsilon}_{k_s} + N\varepsilon_{\mathrm{corr}} + N\varepsilon_F + N\,2\varepsilon + N\overline{\varepsilon} .$$

Данный ключ включает в себя неидеальности всех процессов КРК.

Таким образом, "качество" квантового ключа ухудшается с ростом числа сеансов КРК, поскольку параметр секретности возрастает линейно от N.

Наша цель — обеспечить проведение заданного достаточно большого числа сеансов КРК N таким образом, чтобы на последнем сеансе параметр секретности ключа не превышал заданного критического значения $\varepsilon_{\mathrm{crit}}$.

Допустимое число сеансов находится из равенства

$$\overline{\varepsilon}_{k_s} + N\varepsilon_{\mathrm{corr}} + N\varepsilon_F + N\,2\varepsilon + N\overline{\varepsilon} = \varepsilon_{\mathrm{crit}} . \quad (67)$$

Как это можно сделать?

Слагаемые, входящие в левую часть равенства (67), имеют различный уровень влияния на механизм КРК при обеспечении финальной секретности $\varepsilon_{\mathrm{crit}}$.

Величина $\overline{\varepsilon}_{k_s} = 2\varepsilon_{k_s}$ входит в сумму однократно, величина ε_{k_s} отвечает за неидеальность стартового ключа аутентификации — (неравновероятность) выбора битовых строк — коэффициентов полиномов при построении ε-ASU_2 хэш-функций аутентификации и определяется, по существу, свойствами генератора случайных чисел (ГСЧ), т.е. внешними причинами, не относящимися непосредственно к КРК. Будем считать, что всегда можно добиться соотношения $\overline{\varepsilon}_{k_s} \ll \varepsilon_{\mathrm{crit}}$ и не учитывать величину $\overline{\varepsilon}_{k_s}$ при нахождении величины N.

Тогда, с учётом этих условий, перепишем равенство (67) в виде

$$\varepsilon_{\mathrm{corr}} + \varepsilon_F + 2\varepsilon + \overline{\varepsilon} = \frac{\varepsilon_{\mathrm{crit}}}{N} .$$

Далее зададимся величиной N и припишем, для определённости, каждому из четырёх слагаемых $\varepsilon_{\mathrm{corr}}$, ε_F, 2ε, $\overline{\varepsilon}$ равнозначный вклад по $\varepsilon_{\mathrm{crit}}/4N$ в общую сумму $\varepsilon_{\mathrm{crit}}/N$.

Рассмотрим слагаемые по отдельности.

1. Величина $\varepsilon_{\mathrm{corr}}$.

Параметр корректности — вероятность несовпадения ключей Алисы и Боба — определяется соотношением $\varepsilon_{\mathrm{corr}} = 2^{-v}$, где v — число контрольных битов чётности, вычисленных из битовых строк Алисы и Боба.

Из равенства $\varepsilon_{\mathrm{corr}} = \varepsilon_{\mathrm{crit}}/4N$ получаем соотношение

$$v = \log \frac{4N}{\varepsilon_{\mathrm{crit}}} .$$

2. Величина ε_F.

Параметр ε_F отвечает за неидеальность (неравновероятность) выбора битовой строки — коэффициентов полинома U_2 хэш-функции f процедуры усиления секретности. Параметр ε_F определяется свойствами ГСЧ — генератора случайных чисел, т.е. внешними причинами, не относящимися непосредственно к КРК. Будем считать, что равенство $\varepsilon_F = \varepsilon_{\mathrm{crit}}/4N$ может быть обеспечено при любых разумных $\varepsilon_{\mathrm{crit}}$ и N.

3. Величина 2ε.

Параметр ε задаёт свойство ε-ASU_2 хэш-функций аутентификации при равновероятном выборе битовых строк — коэффициентов полиномов при построении хэш-функций, при этом

$$\varepsilon = \frac{n_1}{2^{k_1}} + \frac{1}{2^{k_s}} ,$$

где n_1 — количество блоков в сообщении длины k_1, k_1 — длина постоянного (reused) ключа аутентификации, k_s — длина одноразового ключа аутентификации, $k_s < k_1$.

Длина постоянного ключа аутентификации k_1 может быть выбрана достаточно большой, так чтобы величина

$\varepsilon \approx 1/2^{k_s}$. Тогда из соотношения $2\varepsilon = \varepsilon_{\text{crit}}/4N$ получаем минимально необходимую длину одноразового ключа аутентификации

$$k_s = \log \frac{8N}{\varepsilon_{\text{crit}}} .$$

Величина k_s (битов) — это добавок к квантовому ключу длины ℓ_{cip}, используемому для шифрования. Суммарный квантовый ключ, который должен создаваться при КРК, должен иметь длину не менее $\ell = \ell_{\text{cip}} + k_s$.

4. Величина $\overline{\varepsilon}$.

Величина $\overline{\varepsilon}$ оценивает расстояние между квантовым реальным и идеальным распределением ключей после усиления секретности:

$$||\rho^{R_Q}_{(\mathcal{F}E)} - \rho^{I_Q}_{(\mathcal{F}E)}||_1 \leqslant 2\varepsilon' + 2^{-(1/2)\left[H^{\varepsilon'}_{\min}(\rho_{KE}|\rho_E) - C - \ell\right]} = \overline{\varepsilon}\,, \quad (68)$$

при этом для решения нашей задачи должно выполняться условие $\overline{\varepsilon} = \varepsilon_{\text{crit}}/4N$.

Малость величины $\overline{\varepsilon}$ определяется степенью сжатия (соотношением между n и ℓ) хэш-функции усиления секретности

$$f\colon \{0,1\}^n \to \{0,1\}^\ell .$$

Расчёт необходимого значения n даётся через нижнюю оценку сглаженной min-энтропии, которая содержит в себе все данные об утечке информации к нарушителю через квантовый канал связи и побочные каналы утечки. Оценка сглаженной min-энтропии для тензорного произведения $\rho^{n\otimes}_{KE}$ может быть получена через условную энтропию фон Неймана.

Согласно [57], имеем

$$H^{\varepsilon'}_{\min}(\rho_{KE}|\rho_E) \geqslant nH(\rho_{KE}|\rho_E) - \log(5)\sqrt{n\log\left(\frac{1}{\varepsilon'}\right)}\,, \quad (69)$$

где n — число зарегистрированных посылок квантовых состояний на приёмной стороне Боба и

$$H(\rho_{KE}|\rho_E) = H(\rho_{KE}) - H(\rho_E)\,,$$

$H(\rho_{KE})$, $H(\rho_E)$ — энтропии фон Неймана.

Положим в (68) величину $\varepsilon' = \overline{\varepsilon}/3 = \varepsilon_{\text{crit}}/12N$.

Тогда решение уравнения

$$2^{-(1/2)\left[nH(\rho_{KE}|\rho_E) - C - \log(5)\sqrt{n\log(12N/\varepsilon_{\text{crit}})} - \ell\right]} = \frac{\varepsilon_{\text{crit}}}{12N} \quad (70)$$

относительно n даст минимально необходимое число зарегистрированных посылок квантовых состояний на приёмной стороне, при котором будет обеспечиваться необходимый уровень секретности квантовых ключей.

Здесь

$C = \text{leak} + v = n\cdot\text{leak} + \log(4N/\varepsilon_{\text{crit}})$ — полное количество битов информации, передаваемой Алисой и Бобом через открытый аутентичный классический канал связи при исправлении ошибок и проверке корректности ключа,

$\ell = \ell_{\text{cip}} + k_s$, ℓ_{cip} — часть длины квантового ключа для шифрования, $k_s = \log(8N/\varepsilon_{\text{crit}})$ — часть длины квантового ключа для аутентификации.

Логарифмируя (70), получаем

$$n\Delta H - \log(5)\sqrt{n\log\frac{12N}{\varepsilon_{\text{crit}}}} - \left(2\log\frac{12N}{\varepsilon_{\text{crit}}} + \log\frac{8N}{\varepsilon_{\text{crit}}} + \log\frac{4N}{\varepsilon_{\text{crit}}} + \ell_{\text{cip}}\right) = 0\,, \quad (71)$$

$$\Delta H = H(\rho_{KE}|\rho_E) - \text{leak}\,.$$

Из (71) получаем $n(\Delta H, N, \varepsilon_{\text{crit}}, \ell)$ — необходимое число зарегистрированных посылок на приёмной стороне, чтобы обеспечить необходимый уровень секретности ключа (достичь величины $\varepsilon_{\text{crit}}$) после N сеансов квантового распределения ключей:

$$n(\Delta H, N, \varepsilon_{\text{crit}}, \ell_{\text{cip}}) = \left\{\frac{1}{2\Delta H}\left[\log(5)\sqrt{\log\frac{12N}{\varepsilon_{\text{crit}}}} + \left(\log^2(5)\,\log\frac{12N}{\varepsilon_{\text{crit}}} + 4\Delta H\left(2\log\frac{12N}{\varepsilon_{\text{crit}}} + \log\frac{8N}{\varepsilon_{\text{crit}}} + \log\frac{4N}{\varepsilon_{\text{crit}}} + \ell_{\text{cip}}\right)\right)^{1/2}\right]\right\}^2 . \quad (72)$$

Здесь важно отметить, что зависимость минимально необходимого числа зарегистрированных посылок квантовых состояний n на приёмной стороне от числа сеансов $N \gg 1$ при заданном критическом параметре секретности $\varepsilon_{\text{crit}} \ll 1$ является слабой — логарифмической:

$$n \propto \log\left(\frac{12N}{\varepsilon_{\text{crit}}}\right) \propto \log(N) + \log\left(\frac{1}{\varepsilon_{\text{crit}}}\right). \quad (73)$$

Афоризм, приведённый в начале данного раздела, как нельзя лучше отражает фактическую ситуацию. Неформально говоря, число физических ресурсов — число посланных квантовых состояний Алисой к Бобу, логарифмически зависит от требуемого числа сеансов КРК и уровня секретности ключей вплоть до последнего сеанса.

После N сеансов КРК потребуется новый перезапуск всей системы КРК, т.е. между Алисой и Бобом должен быть предраспределён (организационно-техническими или иными методами) новый стартовый ключ аутентификации для следующей серии сеансов КРК.

10. Длинный одноразовый ключ — одноразовый блокнот

В разделе 9 мы рассмотрели ситуацию, когда проводится N сеансов КРК, в каждом из которых распределяется одноразовый ключ, который, вплоть до последнего сеанса, является $\varepsilon_{\text{crit}}$-секретным. Рассмотрим ситуацию, когда требуется создать один длинный одноразовый ключ из всех сеансов.

Пусть проводится N сеансов КРК. В каждом сеансе получается квантовый ключ длиной ℓ_{cip} битов. Пусть в первом сеансе КРК квантовый ключ является $2\varepsilon_{\text{crit}}/N^2$-секретным. Эти ключи конкатенируются в один квантовый ключ длиной $\ell_N = N\ell_{\text{cip}}$. Из неравенства треугольника для следового расстояния следует, что составной ключ длиной ℓ_N будет $\varepsilon_{\text{crit}}(1 + 1/N)$, поскольку параметры секретности ключей при конкатенации складываются:

$$1\cdot\frac{2\varepsilon_{\text{crit}}}{N^2} + 2\cdot\frac{2\varepsilon_{\text{crit}}}{N^2} + \ldots + N\cdot\frac{2\varepsilon_{\text{crit}}}{N^2} = \varepsilon_{\text{crit}}\left(1 + \frac{1}{N}\right) \approx \varepsilon_{\text{crit}}\,.$$

Таким образом, для получения квантового ключа длиной $\ell_N = N\ell_{\text{cip}}$ достаточно, чтобы в первом сеансе КРК квантовый ключ был $2\varepsilon_{\text{crit}}/N^2$-секретным. Используя (73), нетрудно получить, что для обеспечения такого параметра секретности нужно зарегистрировать

$$n \propto \log\left(\frac{12N^2}{\varepsilon_{\text{crit}}/2}\right) \propto \log(N) + \log\left(\frac{1}{\varepsilon_{\text{crit}}}\right)$$

посылок квантовых состояний. Как мы видим, в данном случае число посланных квантовых состояний Алисой к Бобу также логарифмически зависит от величины требуемой длины ключа $\ell_N = N\ell_{\text{cip}}$ и параметра секретности $\varepsilon_{\text{crit}}$ составного одноразового ключа.

11. Некоторые численные примеры

В этом разделе мы приведём примеры расчётов, показывающих с практических позиций возможность формирования заданного большого числа N квантовых ключей длиной ℓ_{cip}, идущих на шифрование и имеющих заданное качество, с параметром секретности не хуже $\varepsilon_{\text{crit}}$.

Фактически, задаваясь достаточно большим значением величины N — числа сеансов КРК — и достаточно малым значением величины $\varepsilon_{\text{crit}}$ — параметра секретности квантового ключа, по формуле (71) мы оцениваем практически значимую величину n — числа посылок квантовых состояний, реально требующихся при реализации КРК.

Положим длину квантовых ключей шифрования $\ell_{\text{cip}} = 10^3$ и рассмотрим, в некотором смысле крайние, случаи, когда:

— $N = 10^6$, $\varepsilon_{\text{crit}} = 10^{-6}$, $\ell_{\text{cip}} = 10^3$;

— $N = 10^9$, $\varepsilon_{\text{crit}} = 10^{-9}$, $\ell_{\text{cip}} = 10^3$.

Расчёт по формуле (72) будет вполне корректным, если при оценке параметра

$$\varepsilon = \frac{n_1}{2^{k_1}} + \frac{1}{2^{k_s}} \tag{74}$$

хэш-функции аутентификации можно пренебречь первым слагаемым. Здесь n_1 — количество блоков длиной k_1 в сообщении, k_1 — длина постоянного (reused) ключа аутентификации, $k_s = \log(8N/\varepsilon_{\text{crit}})$ — длина одноразового ключа аутентификации.

Для рассматриваемых случаев длина $k_s = 42-63$. Выбирая длину постоянного (reused) ключа аутентификации $k_1 = 128$, нетрудно видеть, что первым слагаемым в (74) можно пренебречь при числе блоков $n_1 \leqslant 2^{64}$ или ограничении на длину открытых классических сообщений $M \leqslant 2^{64} \cdot 128$ битов. Такой длины с запасом хватает для оценки длины открытых сообщений в сеансе КРК.

Величина ΔH имеет смысл дефицита информации нарушителя в битах на одну зарегистрированную позицию после сеанса КРК, коррекции ошибок и усиления секретности.

Здесь принципиально важно отметить, что величина ΔH вычисляется исходя из фундаментальных законов квантовой теории и не зависит от предположений о технических и вычислительных возможностях нарушителя (см. детали, например, в [57, 58]).

Типичные значения при длине волоконной линии квантовой связи $L = 100$ км составляют величину $\Delta H \approx 0{,}1-0{,}5$ бит.

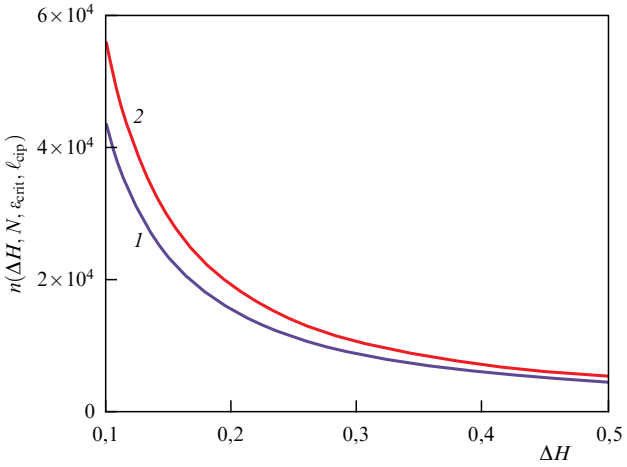


Рис. 7. Зависимости необходимого числа зарегистрированных состояний $n(\Delta H, N, \varepsilon_{\text{crit}}, \ell_{\text{cip}})$ в каждом сеансе КРК как функции нехватки информации нарушителя (ΔH) при заданном уровне секретности ($\varepsilon_{\text{crit}}$), числе сеансов ($N$) и длине ключа в сеансе (ℓ_{cip}). Параметры следующие: кривая *1* (синий цвет) — $N = 10^6$, $\varepsilon_{\text{crit}} = 10^{-6}$, $\ell_{\text{cip}} = 10^3$; кривая *2* (красный цвет) — $N = 10^9$, $\varepsilon_{\text{crit}} = 10^{-9}$, $\ell_{\text{cip}} = 10^3$.

Зависимости необходимого числа зарегистрированных состояний $n(\Delta H, N, \varepsilon_{\text{crit}}, \ell_{\text{cip}})$ в каждом сеансе КРК приведены на рис. 7.

Как следует из рис. 7, число регистрируемых квантовых состояний на приёмной стороне Боба слабо (логарифмически) зависит от финального (критического значения параметра секретности) $\varepsilon_{\text{crit}}$, а также от величины дефицита информации Евы (ΔH) относительно ключа Алисы. Это означает, что после инициализации системы КРК возможно практически сколь угодно долгое распределение секретных ключей, которые будут гарантированно ε-секретными с $\varepsilon \leqslant \varepsilon_{\text{crit}}$. Следовательно, трудоёмкость перебора при вскрытии шифра также будет гарантированно не меньше критической величины.

Приведём оценки времени передачи квантовых состояний.

При длине волоконной линии связи $L = 100$ км со стандартным коэффициентом потерь $\delta = 0{,}2$ дБ км$^{-1}$, с учётом потерь в канале ($T(L) = 10^{-\delta L/10}$ — коэффициент прохождения через линию связи длиной L), квантовой эффективности детекторов ($\eta \approx 0{,}1$), среднего числа фотонов в информационных состояниях ($\mu \approx 0{,}2-0{,}5$) и потерь в самой системе $\alpha \approx 0{,}1$), эффективность протокола составляет $\text{eff} = \alpha\eta\mu T^{-1}(L) \approx 10^{-5}$.

Отсюда следует, что для того, чтобы получить число зарегистрированных состояний $n \approx 10^5$ (см. рис. 7) требуется передать $n/\text{eff} \approx 10^{10}$ квантовых состояний со стороны Алисы.

При тактовой частоте 100 МГц (10^8 Гц) для каждого сеанса потребуется $10^{10}/10^8 = 10^2$ с, соответственно, при частоте 10 МГц (10^7 Гц) потребуется время $10^{10}/10^7 = 10^3$ с, т.е. порядка 1 ч на сеанс. При частоте 1 ГГц (10^9 Гц) для передачи 10^{10} состояний потребуется $10^{10}/10^9 = 10$ с, это означает, что каждые 10 с можно получать одноразовый ключ длиной 1000 битов заданного качества, число таких ключей — сеансов КРК — будет 10^6; разумеется, данные оценки по порядку величины.

12. Заключение

В настоящей статье решён принципиальный для квантовой криптографии вопрос — сколько сеансов квантового распределения ключей с момента запуска системы можно проводить до нового перезапуска системы — пока криптографические свойства квантовых ключей достигнут критического уровня, после которого их уже нельзя будет использовать для криптографических целей, и потребуется новый перезапуск системы квантовой криптографии.

Системы квантовой криптографии по сути являются системами расширения исходного стартового ключа, который требуется при старте системы для обеспечения теоретико-информационной стойкой аутентификации сообщений в классическом канале связи. В текущем сеансе возникает квантовый ключ, часть которого используется для аутентификации в следующем сеансе.

Получено явное выражение для необходимого числа зарегистрированных посылок при каждом сеансе квантового распределения ключей, чтобы после N сеансов параметр секретности распределяемых ключей оказался не хуже заданного уровня. Число допустимых сеансов N и финальный параметр секретности ε, которые выбираются легитимными пользователями, определяют выбор ε-ASU_2 хэш-функции для теоретико-информационной аутентификации, длину ключа аутентификации и исходный параметр секретности стартового ключа для инициализации системы. После N сеансов квантового распределения ключей требуется новый перезапуск системы, чтобы сохранить требуемый уровень качества ключей.

Технология квантовой криптографии — квантового распределения ключей позволяет, используя только один предварительно распределённый стартовый ключ, распределять секретные ключи практически сколь угодно долго. Эти секретные ключи могут быть использованы для шифрования в режиме одноразового блокнота, причём гарантируется, что секретность ключей базируется на фундаментальных законах Природы, а не на предположениях о технических и вычислительных возможностях подслушивателя, включая полномасштабный квантовый вычислитель.

Принципиальное отличие от классического случая состоит в том, что в классическом случае нужно обеспечивать секретность каждого ключа, распределяемого организационными методам. В системах КРК достаточно распределить только один короткий первичный стартовый ключ, используя организационные методы. Последующие ключи получаются при квантовом распределении, и их секретность гарантируется фундаментальными законами Природы.

Для достижения теоретико-информационной стойкости систем КРК требуются случайные битовые последовательности, которые должны получаться как результат работы квантовых генераторов случайных чисел [61]. Вопросы получения доказуемо случайных битовых последовательностей обсуждаются в работах [62 – 64].

Отметим, что вопрос о числе допустимых сегментов возникает и в сетях с квантовым распределением ключей с распределением ключей через доверенные узлы [23, 59, 60]. Для оценки допустимого числа сегментов квантовой сети можно воспользоваться результатами, представленными в настоящей работе. В этом случае под числом сеансов квантового распределения ключей N следует понимать допустимое число сегментов сети.

Полученные результаты показывают, что для экспериментально достижимых значений параметра секретности $\varepsilon_c \approx 10^{-9}$ при квантовом распределении ключей длина одноразового ключа k_s при аутентификации в каждом сеансе оказывается достаточно "щадящей''. Длина постоянного (reused) ключа также оказывается небольшой.

Допустимое число сеансов КРК $N = 10^9$ фактически означает, что после инициализации система КРК может работать "бесконечно долго". Например, пусть каждый сеанс КРК длится 1 с (что является весьма оптимистической оценкой), тогда за 100 лет работы будет проведено $N \approx 10^9$ сеансов, что на практике означает "бесконечно долгую" работу системы после инициализации.

Один из выводов из приведённого рассмотрения состоит в том, что следовое расстояние, на котором основана идеология абстрактной криптографии и которое даёт степень различимости пары квантовых состояний, отвечающих реальной и идеальной ситуациям, является адекватной и достаточной характеристикой, позволяющей найти нижние границы трудоёмкости (сложности) перебора — поиска фактических ключей шифрования в различных ситуациях их использования [30].

В заключение необходимо сделать принципиально важное замечание для систем квантового распределения ключей.

Квантовая механика является не только корректной — правильно описывающей явления в микромире, но и полной теорией [65 – 70]. Для квантовой криптографии важна не только корректность квантовой механики, но и её полнота.

Квантовая механика является наиболее экспериментально проверенной теорией. Более чем за 100 лет проверок огромного числа предсказаний квантовой теории не обнаружено никаких отклонений.

Применительно к квантовой криптографии законы квантовой механики дают фундаментальную верхнюю границу утечки информации к нарушителю при наблюдаемом возмущении квантовых состояний на приёмной стороне.

Полнота квантовой механики принципиально важна для секретности ключей в квантовой криптографии. Кратко и неформально говоря, полнота квантовой механики означает, что невозможно улучшить вероятностные предсказания теории, которые следуют из описания квантовых систем при помощи волновой функции — вектора состояний или матрицы плотности. Это означает, что в руках нарушителя нет никаких дополнительных ресурсов — скрытых параметров, которые могли бы улучшить результаты его измерений, соответственно, увеличить утечку информации о распределяемых ключах при том же самом наблюдаемом возмущении квантовых состояний, по сравнению с теми, которые следуют из описания квантовых систем при помощи волновой функции и в более общем случае при помощи матрицы плотности [68].

Благодарности. Выражаем благодарность С.П. Кулику, В.А. Кирюхину, сотрудникам Центра квантовых техно-

логий МГУ, а также коллегам из ИнфоТеКС и СФБ Лаборатории за интерес к работе и многочисленные обсуждения.

Список литературы

1. Bennett C H, Brassard H "Quantum cryptography: Public key distribution and coin tossing", in *Proc. of the IEEE Intern. Conf. on Computers, Systems, and Signal Processing, Bangalore, India, 10–12 December 1984* (Piscataway, NJ: IEEE, 1984) p. 175; *Theor. Comput. Sci.* **560** 7 (2014); arXiv:2003.06557
2. Zhang Q et al. *Opt. Express* **26** 24260 (2018)
3. Sasaki M et al. *Opt. Express* **19** 10387 (2011)
4. "Университетская квантовая сеть запущена. Видео-обзор торжественного открытия в МГУ" 21.02.2022. ИнфоТеКС, https://www.youtube.com/watch?v=0WAuDcYhKbo; https://rutube.ru/video/74c8fa47de0f5d111f1eb04bc532bb60/?r=wd
5. Scarani V et al. *Rev. Mod. Phys.* **81** 1301 (2009)
6. Xu F et al. *Rev. Mod. Phys.* **92** 025002 (2020)
7. Portmann Ch, Renner R *Rev. Mod. Phys.* **94** 025008 (2022)
8. Lu C-Y et al. *Rev. Mod. Phys.* **94** 035001 (2022)
9. Azuma K et al. *Rev. Mod. Phys.* **95** 045006 (2023)
10. Kahn D *The Codebreakers: The Story of Secret Writing* (New York: McMillan, 1967)
11. Bauer F L *Decrypted Secrets*: *Methods and Maxims of Cryptology* 3rd ed. rev. and updated (Berlin: Springer-Verlag, 2002)
12. Соболева Т А *История шифровального дела в России* (М.: ОЛМА-ПРЕСС, 2002)
13. Шампольон Ж-Ф *О египетском иероглифическом алфавите* (Сер. "Классики науки", пер., ред. и коммент. И Г Лившица) (М.–Л.: Изд-во АН СССР, 1950)
14. Vernam G S *J. Am. IEE* **45** 109 (1926); Reprint Bell Telephone Laboratories B-198, June 1926
15. Bellovin G S *Cryptologia* **35** 203 (2011)
16. Котельников В А "Основные положения автоматической шифровки", Отчет 19 июня 1941; публикуется в кн. Котельников В А *Собрание трудов* Т. 1 *Радиофизика, информатика, телекоммуникации* (М.: Физматлит, 2008) с. 153
17. Научная сессия Отделения физических наук Российской академии наук, посвящённая памяти академика Владимира Александровича Котельникова (22 февраля 2006 г.): Гуляев Ю В *УФН* **176** 751 (2006); Gulyaev Yu V *Phys. Usp.* **49** 725 (2006); Котельникова Н В *УФН* **176** 753 (2006); Kotel'nikova N V *Phys. Usp.* **49** 727 (2006); Арманд Н А *УФН* **176** 770 (2006); Armand N A *Phys. Usp.* **49** 744 (2006); Сачков В Н *УФН* **176** 775 (2006); Sachkov V N *Phys. Usp.* **49** 748 (2006); Молотков С Н *УФН* **176** 777 (2006); Molotkov S N *Phys. Usp.* **49** 750 (2006); Черток Б Е *УФН* **176** 788 (2006); Chertok B E *Phys. Usp.* **49** 761 (2006)
18. Котельников В А "О пропускной способности "эфира" и проволоки в электросвязи", в сб. *Всесоюзный энергетический комитет. Материалы к I Всесоюз. съезду по вопросам технической реконструкции дела связи и развития слаботочной промышленности, 1932, Москва* (М.: Управление связи РККА, 1933) с. 1; переиздание: Котельников В А *О пропускной способности "эфира" и проволоки в электросвязи* (М.: Ин-т радиотехники и электроники МЭИ (ТУ), 2003); Котельников В А *УФН* **176** 762 (2006); Kotel'nikov V A *Phys. Usp.* **49** 736 (2006)
19. Bissell Ch *IEEE Commun. Mag.* **47** (10) 24 (2009)
20. Shannon C E "A mathematical theory of cryptography", Bell System Technical Memo MM 45-110-02, dated Sept. 1 1945, p. 86, Part III of original document, https://www.iacr.org/museum/shannon/shannon45.pdf
21. Schneier B *Applied Cryptography. Protocols, Algorithms, and Source Code in C* (New York: John Wiley and Sons, 1996); Пер. на русск. яз.: Шнайер Б *Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си* (М.: Триумф, 2012)
22. Konheim A G *Computer Security and Cryptography* (Hoboken, NJ: John Wiley and Sons, 2007)
23. Арбеков И М, Молотков С Н *Математические вопросы криптографии* **14** (3) 9 (2023)
24. Wiesner S "Conjugate Coding", рукопись, около 1970 г.; впоследствии опубликовано в *ACM SIGACT News* **15** (1) 78 (1983)
25. Shor P W "Algorithms for quantum computation: discrete logarithms and factoring", in *Proc. of the 35th Annual Symp. on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994* (Ed. S Goldwasser) (Piscataway, NJ: IEEE Computer Society Press, 1994) p. 124, DOI: 10.1109/SFCS.1994.365700
26. Diffie W, Hellman M *IEEE Trans. Inform. Theory* **22** 644 (1976)
27. Yuen H P, arXiv:1109.2675
28. Renner R, arXiv:1209.2423
29. Wilde M M, arXiv:1106.1445v6, исправленная версия от 2 Dec. 2015
30. Арбеков И М, Молотков С Н *ЖЭТФ* **152** 62 (2017); Arbekov I M, Molotkov S N *J. Exp. Theor. Phys.* **125** 50 (2017)
31. Арбеков И М *Математические вопросы криптографии* **7** (1) 39 (2016)
32. Молотков С Н *ЖЭТФ* **150** 903 (2016); Molotkov S N *J. Exp. Theor. Phys.* **123** 784 (2016)
33. Арбеков И М *Элементарная квантовая криптография*: *для криптографов, не знакомых с квантовой механикой* (Основы защиты информации, № 23) (М.: URSS. ЛЕНАНД, 2022)
34. Cederlöf J, Larsson J-A *IEEE Trans. Inform. Theory* **54** 1735 (2008)
35. Abidin A, Larsson J-A *Int. J. Quantum Inform.* **7** 1047 (2009)
36. Peev M et al. *Int. J. Quantum Inform.* **7** 1401 (2009)
37. Pacher C et al. *Quantum Inform. Process.* **15** 327 (2016)
38. Wegman M N, Carter J L *J. Comput. Syst. Sci.* **22** 265 (1981)
39. Simmons G J *Proc. IEEE* **76** 603 (1988)
40. Atici M, Stinson D R "Universal hashing and multiple authentication", in *Advances in Cryptology, CRYPTO'96. 16th Annual Intern. Cryptology Conf., Santa Barbara, California, USA, August 18–22, 1996, Proc.* (Lecture Notes in Computer Science, Vol. 1109, Ed. N Koblitz) (Berlin: Springer-Verlag, 1996) p. 16, DOI: 10.1007/3-540-68697-5_2
41. Bierbrauer J et al. "On families of hash functions via geometric codes and concatenation", in *Advances in Cryptology, CRYPTO'93. 13th Annual Intern. Cryptology Conf., Santa Barbara, California, USA, August 22–26, 1993, Proc.* (Lecture Notes in Computer Science, Vol. 773, Ed. D R Stinson) (Berlin: Springer-Verlag, 1994) p. 331, DOI: 10.1007/3-540-48329-2_28
42. den Boer B *J. Comput. Security* **2** 65 (1993)
43. Krawczyk H "LFSR-based hashing and authentication", in *Advances in Cryptology, CRYPTO'94. 14th Annual Intern. Cryptology Conf., Santa Barbara, California, USA, August 21–25, 1994, Proc.* (Lecture Notes in Computer Science, Vol. 839, Ed. Y G Desmedt) (Berlin: Springer-Verlag, 1994) p. 129, DOI: 10.1007/3-540-48658-5_15
44. Krawczyk H "New hash functions for message authentication", in *Advances in Cryptology, EUROCRYPT'95. Intern. Conf. on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 21–25, 1995. Proc.* (Lecture Notes in Computer Science, Vol. 921, Eds L C Guillou, J-J Quisquater) (Berlin: Springer-Verlag, 1995) p. 301, DOI: 10.1007/3-540-49264-X_24
45. Stinson D R "Universal hashing and authentication codes", in *Advances in Cryptology, CRYPTO'91. Proc.* (Lecture Notes in Computer Science, Vol. 576 , Ed. J Feigenbaum) (Berlin: Springer, 1992) p. 74, DOI: 10.1007/3-540-46766-1_5
46. Stinson D R *J. Comput. Syst. Sci.* **48** 337 (1994)
47. Stinson D R *Congressus Numerantium* **114** 7 (1996)
48. Stinson D R *J. Combin. Math. Combin. Comput.* **42** 3 (2002)
49. Abidin A, Larsson J-Å "New universal hash functions", in *Research in Cryptology. 4th Western European Workshop, WEWoRC 2011, Weimar, Germany, July 20–22, 2011, Revised Selected Papers* (Lecture Notes in Computer Science, Vol. 7242, Eds F Armknecht, S Lucks) (Berlin: Springer, 2012) p. 99, DOI: 10.1007/978-3-642-34159-5_7
50. Rogaway P *J. Cryptology* **12** 91 (1999)
51. Abidin A, Larsson J-Å *Quantum Inform. Process.* **13** 2155 (2014)
52. Portmann Ch *IEEE Trans. Inform. Theory* **60** 4383 (2014)
53. Canetti R "Universally composable security: a new paradigm for cryptographic protocols", in *Proc. 42nd IEEE Symp. on Foundations of Computer Science, 08–11 October 2001, Newport Beach, CA, USA* (Piscataway, NJ: IEEE, 2001) p. 136, DOI: 10.1109/SFCS.2001.959888
54. Canetti R et al. "Universally composable security with global setup", in *Theory of Cryptography. 4th Theory of Cryptography*

Conf., TCC 2007, Amsterdam, The Netherlands, February 21–24, 2007, Proc. (Lecture Notes in Computer Science, Vol. 4392, Ed. S P Vadhan) (Berlin: Springer, 2007) p. 61, DOI: 10.1007/978-3-540-70936-7_4
55. Müller-Quade J, Renner R *New J. Phys.* **11** 085006 (2009)
56. Maurer U, Renner R "Abstract cryptography", in *Proc. of the Second Symp. on Innovations in Computer Science, ICS 2011, Beijing, China* (Beijing: Tsinghua Univ. Press, 2011) p. 1
57. Renner R "Security of quantum key distribution", PhD Thesis (Zürich: ETH, 2005)
58. Молотков С Н *ЖЭТФ* **160** 327 (2021); Molotkov S N *J. Exp. Theor. Phys.* **133** 272 (2021)
59. Molotkov S N *Laser Phys. Lett.* **19** 045201 (2022)
60. Molotkov S N *Laser Phys.* **34** 045202 (2024)
61. Herrero-Collantes M, Garcia-Escartin J C *Rev. Mod. Phys.* **89** 015004 (2017)
62. Арбеков И М, Молотков С Н *УФН* **191** 651 (2021); Arbekov I M, Molotkov S N *Phys. Usp.* **64** 617 (2021)
63. Арбеков И М, Молотков С Н *УФН* **194** 974 (2024); Arbekov I M, Molotkov S N *Phys. Usp.* **67** 919 (2024)
64. Балыгин К А, Кулик С П, Молотков С Н *Письма в ЖЭТФ* **119** 533 (2024); Balygin K A, Kulik S P, Molotkov S N *JETP Lett.* **119** 538 (2024)
65. Einstein A, Podolsky B, Rosen N *Phys. Rev.* **47** 777 (1935)
66. Bell J S *Physics* **1** 195 (1964)
67. Bell J S *Rev. Mod. Phys.* **38** 447 (1966)
68. Bell J S (Introduction by Aspect A) "Free variables and local causality", in *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy* 2nd ed. (Cambridge: Cambridge Univ. Press, 2004) pp. 100–104, Ch. 12
69. Kochen S, Specker E P *J. Math. Mech.* **17** 59 (1967) DOI: 10.1512/iumj.1968.17.17004
70. Colbeck R, Renner R *Nat. Commun.* **2** 411 (2011)

Vernam's, Kotelnikov's, and Shannon's one-time pad and quantum cryptography

I.M. Arbekov [(1,*)], **S.N. Molotkov** [(1,2,3,4,†)]
[(1)] *Academy of Cryptography of the Russian Federation, 119331 Moscow, PO Box 100, Russian Federation*
[(2)] *Osipyan Institute of Solid State Physics, Russian Academy of Sciences, ul. Akademika Osipyana 2, 142432 Chernogolovka, Moscow region, Russian Federation*
[(3)] *Lomonosov Moscow State University, Faculty of Computational Mathematics and Cybernetics, Leninskie gory 1, str. 52, 119991 Moscow, Russian Federation*
[(4)] *Quantum Technology Center, Lomonosov Moscow State University, Leninskie gory 1, str. 35, 119991 Moscow, Russian Federation*
E-mail: [(*)] *arbekov53@mail.ru*, [(†)] *molotkov@issp.ac.ru*

Quantum cryptography — quantum key distribution (QKD) — was one of the first fields of study of quantum information theory. It reached a mature scientific level and has been implemented in commercial systems for secure quantum communications. The key distribution problem is the central issue of symmetric cryptography. Quantum cryptography solves this problem on the basis of the fundamental laws of nature: the principles of quantum mechanics. Quantum key distribution is essentially matching two independent random sequences on the transmitting and receiving sides by exchanging quantum states. Required in addition to the quantum channel is an authentic classical communication channel. Both communication channels are open and vulnerable to a perpetrator's attack. To ensure the authenticity of the classical channel at initial system startup, a seed key is required, which is used to provide information-theoretic authentication. In essence, quantum cryptography systems are mechanisms for expanding this seed key. Subsequent sessions generate a quantum key, part of which is used for authentication, while another part is employed for other cryptographic purposes, such as encryption. An issue fundamental for quantum cryptography is the number of quantum key distribution sessions that can be conducted from the initial system launch until a new system reboot, when the cryptographic properties of the quantum keys reach a critical level, after which they can no longer be used for cryptographic purposes, and a new system reboot is needed. Although a number of reviews on quantum cryptography are currently available, this issue has not been discussed in detail. It is shown that for realistic parameters of quantum cryptography systems that are currently achievable, a QKD system can operate for virtually any length of time before the next reboot. This implies that QKD systems can implement a 'one-time pad' — a set of one-time keys using only a single seed key. A brief historical overview is also presented, outlining some facts little known to the general public. This review, which is intended for a general audience, is comprehensible to undergraduate and graduate students who have completed university courses on quantum information science. The authors hope that it will provide a deeper understanding of the cryptographic underpinnings of state-of-the-art quantum key distribution systems.

Keywords: quantum cryptography, one-time pad, secure communications, authentication

PACS numbers: 03.67.Dd, 03.67.Hk, **89.70.–a**

Bibliography — 70 references *Received 13 January 2025, revised 28 July 2025*

Uspekhi Fizicheskikh Nauk **195** (10) 1021–1046 (2025) *Physics–Uspekhi* **68** (10) (2025)

DOI: https://doi.org/10.3367/UFNr.2025.07.039972 DOI: https://doi.org/10.3367/UFNe.2025.07.039972