Письма в ЖЭТФ, том 117, вып. 6, с. 470 – 479

Перенос секретных ключей в квантовой сети с доверенными промежуточными узлами и шифрованием блочным шифром

С. Н. Молотков[1)]

Академия криптографии Российской Федерации, 121552 Москва, Россия

Институт физики твердого тела РАН, 142432 Черноголовка, Россия

Поступила в редакцию 16 января 2023 г.
После переработки 15 февраля 2023 г.
Принята к публикации 15 февраля 2023 г.

Технология квантовой криптографии позволяет распределять ключи на отдельных сегментах сети в конфигурации точка-точка, далее ключи на отдельных сегментах используются для защиты трафика между любыми узлами сети, напрямую не связанных квантовым каналом. В этой связи возникает вопрос о согласовании (продвижении) ключей по отдельным сегментам сети. В работе рассматривается вопрос о переносе независимого ключа через доверенные узлы квантовой сети, между которыми имеются ключи, полученные в результате квантового распределения ключей. Квантовые ключи используются для шифрования переносимого ключа. Шифрование переносимого ключа возможно как блочным шифром, так и одноразовым блокнотом. Показано, что трудоемкость (сложность перебора) по поиску продвигаемого по сети ключа зависит от неидеальности внешнего ключа и квантовых ключей, а также от неидеальности – средней вероятности коллизий блочного шифра. В случае шифрования переносимого ключа одноразовым блокнотом трудоемкость зависит только от неидеальности переносимого ключа и ключей шифрования. При идеальных ключах сохраняется идеальность переносимого ключа. В случае блочного шифра даже при идеальных ключах переносимый ключ перестает быть идеальным в меру отличия блочного шифра от одноразового блокнота. Показано также, что чем больше коллизий имеет блочный шифр, соответственно, накрывает меньшее множество шифр-текстов, тем меньшее число шагов перебора требуется для нахождения ключа.

DOI: 10.31857/S1234567823060125, EDN: qtpvtf

1. Введение. Базовым в квантовой криптографии является распределение ключей между передатчиком и приемником в конфигурации точка-точка. В существующих квантовых сетях (см., например, [1]) происходит обмен секретными ключами, полученными при квантовом распределении ключей, между узлами непосредственно не соединенных квантовым каналом. Такой обмен производится через промежуточные узлы.

Волоконные системы квантовой криптографии гарантируют секретность ключей, если длина каждого сегмента сети не превышает некоторой критической длины. Одним из способов увеличить дальность квантового распределения ключей является распределение ключей через промежуточные доверенные узлы. В этом случае длина каждого отрезка сети выбирается такой, чтобы вероятность ошибки за счет потерь в линии была меньше критической. При этом на каждом i-м отрезке мы получаем свой квантовый ключ[2)] k_i, обладающий свойством ε_i-секретности [2, 3]. В такой конфигурации сети пара квантовых ключей k_i, k_{i+1} присутствует (известна) на промежуточном узле, поэтому промежуточные узлы должны быть доверенными – пара ключей на каждом промежуточном узле должна быть недоступна подслушивателю.

Возникает вопрос, как получить общий секретный ключ между любой парой узлов, связанных в квантовой сети через промежуточные доверенные узлы.

Возможны два способа получения общего ключа.

1) Перенос *квантового* ключа, полученного на крайнем левом узле.

2) Перенос *внешнего* ключа, сгенерированного отдельно на крайнем левом узле.

В первом случае *квантовый* ключ, полученный на крайнем левом узле, играет роль *внешнего* ключа для следующего узла и, тем самым, оба способа

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

[2)]Для краткости для битовой строки k_1 используем термин – квантовый ключ, что отражает тот факт, что ключ получен в результате квантового распределения ключей.

становятся, по существу, идентичными по постановке задачи.

Если бы *внешний* ключ, а также *квантовые* ключи, возникающие при квантовом распределении ключей (КРК), были бы идеальными, т.е. отвечали бы равновероятному выбору, и неизвестными третьей стороне, то решение задачи *переноса* ключа с сохранением свойства равновероятности было бы довольно простым.

Однако ключи при квантовом распределении не являются идеальными. Все, что удается доказать про данные ключи, так это то, что ключи близки к идеальным в смысле определенного критерия – ключи являются ε-секретными [2, 3].

Принципиальный вопрос, который возникает при переносе или *согласовании* неидеальных ключей, звучит так – каким будет общий ключ, который возникнет в результате продвижения по сети? Иначе говоря, если исходные ключи являются ε-секретными, то сколь секретным будет ключ при продвижении через несколько промежуточных узлов?

Поскольку согласованный ключ будет использоваться в дальнейшем для шифрования, то возникает еще один принципиальный вопрос – как изменится сложность нахождения ключа, который возник при продвижении через несколько доверенных узлов? В данной работе будут даны ответы на эти вопросы.

При переносе ключа между доверенными узлами происходит шифрование переносимого ключа на общих ключах, сгенерированных на сегментах при квантовом распределении ключей. Возможны различные способы шифрования переносимого ключа.

Первый способ состоит в шифровании переносимого ключа одноразовым блокнотом на квантовых ключах на отдельных сегментах квантовой сети.

Второй способ состоит в шифровании переносимого ключа блочным шифром с использованием квантовых ключей на каждом сегменте.

После продвижения общего ключа по сети данный ключ используется для шифрования (защиты) трафика при передаче аудио и видео информации как, например, в сети [1].

Поскольку могут использоваться оба способа для шифрования переносимого ключа, то важно знать, как изменится трудоемкость по поиску проталкиваемого ключа через сегменты квантовой сети, когда шифрование внешнего ключа осуществляется на квантовых ключах на сегменте при шифровании блочным шифром и шифрованием одноразовым блокнотом? Какие характеристики блочного шифра нужно знать, чтобы ответить на предыдущий вопрос?

Одним из методов нахождения злоумышленником общего перенесенного ключа является опробование различных ключей с целью определения истинного ключа. Число шагов полного или частичного перебора ключей определяется трудоемкостью перебора.

Для более четкой постановки задачи удобно предварительно рассмотреть следующий пример (полное рассмотрение см. ниже).

Естественно, после продвижения ключа по сети, ключ в дальнейшем будет использоваться для шифрования сообщений при помощи алгоритма шифрования $\mathcal{F}$. Причем ключ используется неоднократно. "Качество" ключа, точнее близость вероятности распределения ключа к равновероятному, определяет сложность нахождения ключа.

Пусть в алгоритме шифрования $\mathcal{F}$ используется перенесенный ключ k. Данный ключ переносится между узлами с использованием шифрования на квантовом ключе k_1 на сегменте. Нарушитель "видит" зашифрованный $c(k_1, k)$ ключ k (c – алгоритм шифрования – одноразовый блокнот или блочный шифр). Если подслушиватель сможет найти ключ шифрования k_1, то узнает и переносимый ключ, расшифровывая шифр-текст $k = c^{-1}(k_1, c(k_1, k))$, где c^{-1} – функция расшифрования.

Опробовав различные ключи шифрования k_1, подслушиватель будет получать различные ключи $k = c^{-1}(k_1, c(k_1, k))$.

Вопрос – как нарушитель узнает, что ключ $k = c^{-1}(k_1, c(k_1, k))$ действительно истинный ключ?

Консервативно при использовании шифров считается, что возможна атака известный открытый текст – шифр-текст. Подслушиватель "подсовывает" известный открытый текст message, получает шифр-текст cipher, при этом ключ шифрования k неизвестен и его требуется найти.

Зашифрованный текст есть $cipher = \mathcal{F}(k, message)$ ($cipher, message$ – битовые строки). Теперь подслушиватель знает message и cipher – цель найти ключ k, который есть $k = c^{-1}(k_1, c(k_1, k))$ при данном ключе опробования k_1. Подслушиватель опробует последовательно ключи k_{1_i} до тех пор, пока не будет совпадения входа и выхода $cipher = \mathcal{F}(k_i, message)$, начиная с ключа с максимальной вероятностью. При полном переборе истинный ключ будет найден с вероятностью успеха равной единице (см. подробности ниже).

Таким образом, критерий истинности ключа k работает опосредованно через опробоваемые квантовые ключи шифрования k_1 на сегменте.

После нахождения ключа, все последующие сообщения, зашифрованные на этом ключе, будут прочитаны подслушивателем.

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

Отклонение вероятности распределения ключей от идеального равномерного распределения, а также побочная информация подслушивателя о ключах, могут уменьшить число шагов перебора (трудоемкость) для нахождения истинного ключа при различных атаках на алгоритм шифрования (атаки с известным открытым текстом, с избранным открытым текстом и т.д.).

Даже при предварительном рассмотрении можно увидеть разницу при шифровании переносимого ключа одноразовым блокнотом и блочным шифром. При шифровании одноразовым блокнотом равенство $c^{-1}(k_1, c(k_1, k)) = c^{-1}(k_1, c(k'_1, k))$ *возможно только при* $k'_1 = k_1$*, так как невозможны коллизии различных шифр-текстов на разных ключах шифрования (см. ниже). При шифровании блочным шифром равенство* $c^{-1}(k_1, c(k_1, k)) = c^{-1}(k_1, c(k'_1, k))$ *возможно и при* $k'_1 \neq k_1$ *– имеются коллизии шифр-текстов. Этот факт приводит к тому, что эффективное пространство перебора ключей* k_1 *уменьшается (даже при идеальных ключах), т.е., чтобы найти переносимый ключ, достаточно найти любой из ключей шифрования* k_1*, для которых удовлетворяется* $c^{-1}(k_1, c(k_1, k)) = c^{-1}(k_1, c(k'_1, k))$.

Имея в виду выше сказанное, для краткости далее будем называть опосредованный поиск ключа k как поиск проталкиваемого ключа.

В работе будет показано, что трудоемкость частичного перебора по поиску проталкиваемого внешнего ключа при шифровании блочным шифром выражается через следовое расстояние. Следовое расстояние в свою очередь выражается через инварианты (характеристики) блочного шифра. Такими инвариантами блочного шифра являются вероятности различных коллизий (парных, тройных и т.д.). Под коллизиями блочного шифра мы понимаем число совпадений шифр-текстов, которое имеет место при шифровании одного открытого текста на разных ключах.

2. Трудоемкость частичного перебора при шифровании внешнего ключа блочным шифром. Для секретных ключей, используемых в различных алгоритмах шифрования, предъявляются требования, которые формулируются не в терминах абстрактного следового расстояния между матрицами плотности, а в терминах сложности нахождения ключа.

К. Шенноном [4] был введен критерий практической секретности криптосистемы, который понимается как *"The average amount of work to determine the key for a cryptogram..."*. В зависимости от ситуации, возможны различные определения среднего объема работы (трудоемкости) по определению ключа. Само понятие трудоемкости фактически связано с перебором (опробованием) ключей до определения истинного ключа. Причем перебор может быть как полным – по всему пространству ключей, так и частичным – по части ключевого пространства [5, 6]. Такой перебор может иметь место как в отсутствии (дополнительной) побочной информации о ключе, так и при наличии побочной информации.

Применительно к ключам, полученным в результате квантового распределения ключей, побочная информация у Евы о ключе возникает при измерениях над квантовой системой, коррелированной с истинным ключом легитимных пользователей. В работах [5, 6] была установлена прямая связь между критерием секретности, основанном на различимости пары квантовых состояний, и критерием, использующим понятие трудоемкости.

Для вычисления трудоемкости по определению перенесенного ключа требуется знать распределение вероятностей ключей и наблюдаемых переменных. Наблюдаемые переменные Ева получает в результате измерений над квантовой системой, коррелированной с ключами на отдельном сегменте квантовой сети и над квантовым регистром, который содержит зашифрованный продвигаемый ключ.

После расшифрования легитимные пользователи имеют общий проталкиваемый ключ k, а Ева, в результате измерений над своей квантовой системой, имеет битовую строку y, коррелированную с истинным ключом k_1. Кроме этого, Ева имеет битовую строку $c_1 = c(k_1, k)$ – зашифрованный ключ k. Шифр-текст передается по открытому каналу между сегментами сети. Случайные величины c_1 и y можно рассматривать как совокупные наблюдения (побочные переменные) над ключом k, к которому Ева не имеет прямого доступа.

Сразу отметим, что в качестве шифрования $c(k_1, k)$ *может использоваться как блочный шифр, так и одноразовый блокнот. В этом случае будем обозначать зашифрованный ключ как* $c_{OTP}(k_1, k)$.

В реальной ситуации Ева не имеет прямого доступа к продвигаемому ключу k, но имеет побочную

информацию о ключе – случайную величину (битовую строку) $y \in \{0,1\}^n$, коррелированную с квантовым ключом k_1, и битовую строку $c_1(k_1,k) \in \{0,1\}^n$ – продвигаемый ключ k, зашифрованный блочным шифром на ключе k_1, полученным при квантовом распределении на сегменте.

Удобно перевыразить проталкиваемый ключ k через "видимый" шифр-текст $c_1(k_1,k)$ как $k = d(k_1,c_1)$, здесь d – функция расшифрования – однозначная при заданном ключе k_1 и шифр-тексте c_1.

В случае одноразового блокнота шифрование сообщения (в нашем случае продвигаемого ключа k) требует длины ключа шифрования (у нас это k_1) не менее длины сообщения. Если длина ключа (сообщения) k 256 бит, то длина k_1 тоже 256 бит.

Если иметь в виду длину ключа для блочных шифров (например, "Кузнечик"), то длина ключа шифрования у него 256 бит. Сообщения шифруются блоками по 128 бит на одном и том же ключе k_1 в 256 бит. В этом случае сообщение k разбивается на два блока $k = (k^{(1)}_{128}||k^{(2)}_{128})$, где $k^{(1)}_{128}$ – первые 128 бит, $k^{(2)}_{128}$ – вторые. Длина шифр-текста на выходе есть $c_1(k_1,k) = c_1(k_1,k^{(1)}_{128})||c_1(k_1,k^{(2)}_{128})$ – блоки конкатенируются (просто записываются один за другим – символ $||$). Здесь $c_1(k_1,k) = c_1(k_1,k^{(1)}_{128})$ – первый блок шифр-текста длиной 128 бит, $c_1(k_1,k^{(2)}_{128})$ – второй блок шифр-текста в 128 бит. Полная длина после конкатенации шифр-текста $c_1(k_1,k)$ равна 256 бит, также как и для одноразового блокнота.

В итоге длина ключа шифрования k_1 в одноразовом блокноте и блочном шифре одинаковы, длина шифруемого сообщения – продвигаемого ключа k, также одинакова, и шифр-тексты $c_1(k_1,k)$ также одинаковы, что позволяет сделать сравненние близости одноразового блокнота и блочного шифра.

Длина ключа шифрования 256 бит является достаточно типичной для многих современных шифров, длина блока шифрования в 128 бит также типична. При других соотношениях всегда можно привести одноразовый блокнот и блочный шифр к единому "знаменателю" для сравнения близости.

Наблюдения Евы $y, c_1(k_1,k)$ и продвигаемый ключ k связаны совместным распределением вероятностей $P^{\text{cip}}_{K_1KYC_1}(k_1,d(k_1,c_1),y,c_1)$. Индекс cip отражает факт шифрования продвигаемого ключа блочным шифром. Длина шифр-текста $c_1(k_1,k)$ совпадает с длиной ключа k_1 и k.

Вероятность $P^{\text{cip}}_{K_1KYC_1}(k_1,d(k_1,c_1),y,c_1)$ является функцией трех независимых переменных (k_1,y,c_1). Напомним, что ключ шифрования k_1 недоступен Еве и подлежит определению.

Введем обозначение

$$P^{\text{cip}}_{(K_1K)YC_1}(k_1,y,c_1) = P^{\text{cip}}_{K_1KYC_1}(k_1,d(k_1,c_1),y,c_1). \tag{1}$$

Пусть $|\mathcal{K}| = 2^n$, а ключи k_1 изначально упорядочены, например, в лексикографическом порядке. Обозначим условную вероятность

$$P^{\text{cip}}_{(K_1K)|YC_1}(k_1|y,c_1) = \frac{P^{\text{cip}}_{(K_1K)YC_1}(k_1,y,c_1)}{P^{\text{cip}}_{YC_1}(y,c_1)},\ k_1 = \overline{1,K} \tag{2}$$

– апостериорное распределение ключей при условии, что в результате наблюдений получена пара (y,c_1). Предположим в пользу Евы, что Ева, имея побочную информацию (y,c_1), может вычислить и упорядочить вероятности (1) в виде

$$P^{\text{cip}}_{(K_1K)|YC_1}(k_1|y,c_1) \geq \tag{3}$$

$$\geq P^{\text{cip}}_{(K_1K)|YC_1}(k_2|y,c_1)) \geq \ldots \geq P^{\text{cip}}_{(K_1K)|YC_1}(k_N|y,c_1)\,.$$

Здесь k_m – ключ из множества $K = \{1,2,\ldots,K\}$, оказавшийся в ряду (3) на m-м месте, $m = \overline{1,K}$, при этом $\{k_1,k_2,...,k_K\}$ является перестановкой исходных ключей $\{1,2,\ldots,K\}$, зависящей исключительно от пары (y,c_1).

Далее Ева опробует $1 \leq M \leq |\mathcal{K}|$ первых наиболее вероятных ключей, это так называемый усеченный алгоритм U.

Здесь необходимы пояснения. В каждом акте КРК случайно возникает ключ k_1 на сегменте с распределением вероятностей $P_{K_1}(k_1)$. В каждом акте КРК Ева имеет в своем распоряжении квантовую систему $\rho^{k_1}_E$, "привязанную" к ключу k_1. Над данной системой Ева делает измерения, результатом измерения является случайная битовая строка y – побочная переменная, неформально неточный "слепок" ключа k_1. Различные сеансы КРК описываются квантовым ансамблем – матрицей плотности ρ_{K_1E}.

Таким образом, в рассмотренном массовом эксперименте, Ева будет получать истинный ключ шифрования с некоторой вероятностью успеха, затрачивая определенную среднюю работу на нахождение ключа на один эксперимент.

Обозначим

$$p_m = \sum_{y,c_1} P^{\text{cip}}_{(K_1K)|YC_1}(k_m|y,c_1))\,P^{\text{cip}}_{YC_1}(y,c_1) \tag{4}$$

– среднюю вероятность оказаться истинному ключу шифрования k_1 на m-м месте.

Неформально среднее по распределению вероятностей можно понимать как среднее по серии экспериментов, в каждом из которых случайная величина (или величины), по которой происходит усреднение, принимает одно значение в каждом акте

с некоторой вероятностью. Если ключ после M опробований не найден, то Ева переходит к следующему эксперименту по поиску ключа после нового сеанса КРК, в котором возникает новый ключ k_1. При этом у Евы, в результате измерения своей квантовой системы $\rho_E^{k_1}$, привязанной к новому ключу k_1 после КРК, возникнет новая случайная пара (y, c_1). Уже для данной новой пары (y, c_1) Ева опять упорядочивает условные вероятности (3) (так как (y, c_1) имеют новые значения) и начинает опробование ключей. Для вероятности нахождения ключа на m-м месте необходимо усреднить по всем значениям случайной величины – случайной пары (формула (4)).

Для усеченного алгоритма U вычисляются следующие характеристики:

∘ *средняя вероятность успеха (нахождения ключа шифрования) – вероятность попасть случайному ключу k_1 в переборное множество – множество наиболее вероятных ключей, которые опробуются,*

$$\pi_U(M) = \sum_{m=1}^{M} p_m = \\ = \sum_{m=1}^{M} \sum_{y,c_1} P^{\text{cip}}_{(K_1K)|YC_1}(k_m|y,c_1))\, P^{\text{cip}}_{YC_1}(y,c_1), \quad (5)$$

∘ *средняя сложность (в опробованиях) – среднее число актов – шагов опробования внутри переборного множества опробования*

$$S_U(M) = (1-\pi_U(M))\, M + \pi_U(M) \sum_{m=1}^{M} m \frac{p_m}{\pi_U(M)}, \quad (6)$$

∘ *средняя трудоемкость нахождения ключа шифрования – среднее число шагов (актов) опробования внутри переборного множества, нормированное на вероятность успеха – вероятность ключу попасть в переборное множество*

$$Q_U(M) = \frac{S_U(M)}{\pi_U(M)} = \frac{\left(1 - \sum_{m=1}^{M} p_m\right) M + \sum_{m=1}^{M} m p_m}{\sum_{m=1}^{M} p_m}. \quad (7)$$

Определяется Q_{U,π_0} – минимальная средняя сложность для усеченных алгоритмов, приводящих к нахождению ключа с вероятностью успеха, не меньшей π_0:

$$Q_{U,\pi_0} = \min_{\left\{M:\sum_{m=1}^{M} p_m \geq \pi_0\right\}} Q_U = \quad (8)$$

$$= \min_{\left\{M:\sum_{m=1}^{M} p_m \geq \pi_0\right\}} \frac{\left(1 - \sum_{m=1}^{M} p_m\right) M + \sum_{m=1}^{M} m p_m}{\sum_{m=1}^{M} p_m}.$$

В работах [5, 6] было показано, что средняя сложность Q_{U,π_0} удовлетворяет неравенству

$$Q_{U,\pi_0} \geq \left(1 - \frac{2\delta_1}{\pi_0}\right)\left(\frac{|\mathcal{K}|(1-8\delta_1)+1}{2}\right), \quad (9)$$

где

$$\delta_1 = \frac{1}{2}\sum_{m=1}^{|\mathcal{K}|}\left|p_m - \frac{1}{|\mathcal{K}|}\right|. \quad (10)$$

Далее, поскольку

$$\sum_{c_1\in\{0,1\}^n}\sum_{y\in\{0,1\}^n} \frac{1}{|\mathcal{K}|^2} P_Y(y) = \frac{1}{|\mathcal{K}|}, \quad (11)$$

то, с учетом (3), (4), и перестановочности $\{k_1, k_2, ..., k_K\}$, получаем

$$\delta_1 = \frac{1}{2}\sum_{m=1}^{|\mathcal{K}|}\left|p_m - \frac{1}{|\mathcal{K}|}\right| = \quad (12)$$

$$= \frac{1}{2}\sum_{m=1}^{|\mathcal{K}|}\left|\sum_{c_1\in\{0,1\}^n}\sum_{y\in\{0,1\}^n}\left(P^{\text{cip}}_{YC_1}(y,c_1)P^{\text{cip}}_{(K_1K)|YC_1}(k_m|y,c_1) - \frac{1}{|\mathcal{K}|^2}P^{OTP}_Y(y)\right)\right| =$$

$$\leq \frac{1}{2}\sum_{m=1}^{|\mathcal{K}|}\sum_{c_1\in\{0,1\}^n}\sum_{y\in\{0,1\}^n}\left|P^{\text{cip}}_{(KK_1)YC_1}(k_m,y,c_1) - \frac{1}{|\mathcal{K}|^2}P^{OTP}_Y(y)\right| =$$

$$= \frac{1}{2}\sum_{k_1\in\{0,1\}^n}\sum_{y\in\{0,1\}^n}\sum_{c_1\in\{0,1\}^n}\left|P^{\text{cip}}_{K_1KYC_1}(k_1,d(k_1,c_1),y,c_1) - P^{OTP}_{U_KU_1YC_1}(k_1,d_{OTP}(k_1,c_{OTP}),y,c_1)\right| \leq$$

$$\leq \frac{1}{2}||\rho^{\text{cip}}_{K_1KEC_1} - \rho^{OTP}_{U_{K_1}U_KEC_1}||_1, \quad (13)$$

где в (13) следовое расстояние $||\rho||_1 = \text{Tr}\{|\rho|\}$.

Индекс U_K в (13) символизирует равновероятное распределение идеальных продвигаемых ключей k (аббревиатура от Uniform). Аналогично индекс U_{K_1} отвечает равновероятному распределению квантовых ключей k_1.

Для связи матриц плотности $\rho^{\text{cip}}_{K_1KEC_1}$ и $\rho^{OTP}_{U_{K_1}U_KEC_1}$ и распределениями вероятностей в (1)–(5), (12) воспользуемся результатами работы [6]. Следовое расстояние между распределениями вероятностей (13) мажорируется следовым расстоянием между соответствующими матрицами плотности (см. подробности вывода в [6]).

Далее $\rho^{\text{cip}}_{K_1KEC_1}$ – матрица плотности после реального квантового распределения ключей с наличием Евы (E), и продвижением ε_K-секретного внешнего ключа k, который зашифровывается блочным шифром $c_(k_1,k)$ на реальном ε_{K_1}-секретном ключе после реального квантового распределения ключей.

$\rho^{OTP}_{U_{K_1}U_KEC_1} = \rho^{OTP}_{U_{K_1}U_KC_1} \otimes \rho_E$ – матрица плотности после идеального квантового распределения ключей без Евы (E) при проталкивании идеального внешнего ключа $k \in U_K$, который зашифровывается идеальным шифром (одноразовым блокнотом – OTP) $c_{OTP}(k,k_1)$ на идеальном ключе $k_1 \in U_{K_1}$ после идеального квантового распределения ключей без Евы. Матрица плотности Евы ρ_E определим чуть ниже.

Остается мажорировать операторное следовое расстояние в (13).

Последовательно, используя неравенство треугольника, получаем

$$||\rho^{\text{cip}}_{K_1KEC_1} - \rho^{OTP}_{U_{K_1}U_KEC_1}||_1 \le$$
$$\le ||\rho^{\text{cip}}_{K_1KEC_1} - \rho^{\text{cip}}_{U_{K_1}U_KEC_1}||_1 +$$
$$+ ||\rho^{cip}_{U_{K_1}U_KEC_1} - \rho^{OTP}_{U_{K_1}U_KEC_1}||_1, \qquad (14)$$

здесь матрицы плотности $\rho^{\text{cip}}_{U_{K_1}U_KEC_1} = \rho^{\text{cip}}_{U_{K_1}U_KC_1} \otimes$ $\otimes\, \rho_E$ – матрица плотности после идеального квантового распределения ключей без Евы (E), далее проталкивания реального идеального внешнего ключа $k \in U_K$, который зашифровывается блочным шифром $c(k_1,k)$ на идеальном $k_1 \in U_{K_1}$ ключе после идеального квантового распределения ключей без Евы. Матрица плотности Евы ρ_E определим чуть ниже.

2.1. Определение матриц плотности до и после зашифрования. Определим матрицы плотности, фигурирующие в предыдущих разделах.

Матрица плотности, отвечающая реальным ρ_K и идеальным ρ_{U_K} внешним проталкиваемым ключам, имеет вид

$$\rho_{U_K} = \sum_k P_K(k)|k\rangle_{KK}\langle k|, \qquad (15)$$

$$\rho_K = \sum_k P_{U_K}(k)|k\rangle_{KK}\langle k|, \quad P_{U_K(k)} = \frac{1}{2^n} = \frac{1}{|\mathcal{K}|}. \qquad (16)$$

Следовое расстояние между реальными и идеальными внешними ключами есть

$$\frac{1}{2}||\rho_K - \rho_{U_K}||_1 = \frac{1}{2}\sum_k |P_K(k) - P_{U_K}(k)| < \varepsilon_K, \qquad (17)$$

Внешний продвигаемый по сети ключ является ε_K-секретным [2, 3].

Матрицы плотности до зашифрования после реального (ρ_{K_1E}) и идеального ($\rho_{U_{K_1}} \otimes \rho_E$) квантового распределения ключей имеют вид

$$\rho_{K_1E} = \sum_{k_1} P_{K_1}(k_1)|k_1\rangle_{K_1K_1}\langle k_1| \otimes \rho_E^{k_1}, \qquad (18)$$

$$\rho_{U_{K_1}} = \sum_{k_1} P_{U_{K_1}}(k_1)|k_1\rangle_{K_1K_1}\langle k_1|,$$
$$P_{U_{K_1}}(k_1) = \frac{1}{2^n} = \frac{1}{|\mathcal{K}|}. \qquad (19)$$

$$\rho_E = \text{Tr}_{K_1}\{\rho_{K_1E}\} = \sum_{k_1} P_{K_1}(k)\rho_E^{k_1}. \qquad (20)$$

Следовое расстояние между матрицами плотности (18) и (19) имеет вид

$$\frac{1}{2}||\rho_{K_1E} - \rho_{U_{K_1}} \otimes \rho_E||_1 < \varepsilon_{K_1}, \qquad (21)$$

т.е. ключи после квантового распределения ключей на сегменте являются ε_{K_1}-секретными.

Матрицы плотности до зашифрования, с учетом пустого регистра C_1, куда будет записан результат зашифрования, принимают вид:

$$\rho_{K_1KEC_1} = \rho_K \otimes \rho_{K_1E} \otimes |0\rangle_{C_1C_1}\langle 0|,$$
$$\rho_{U_KU_{K_1}EC_1} = \rho_{U_K} \otimes \rho_{U_{K_1}} \otimes \rho_E \otimes |0\rangle_{C_1C_1}\langle 0|. \qquad (22)$$

Зашифрование блочным шифром и одноразовым блокнотом описывается унитарными операторами, имеем

$$\rho^{\text{cip}}_{K_1KEC_1} = U_{\text{cip}}\left(\rho_{K_1KEC_1}\right)U^+_{\text{cip}} = \qquad (23)$$
$$= \sum_k \sum_{k_1} P_K(k)P_{K_1}(k_1)|k\rangle_{KK}\langle k| \otimes |k_1\rangle_{K_1K_1}\langle k_1| \otimes \rho_E^{k_1} \otimes |c_1(k_1,k)\rangle_{C_1C_1}\langle c_1(k_1,k)|,$$

и

$$\rho^{\rm cip}_{U_{K_1}U_KEC_1} = U_{\rm cip}\left(\rho_{U_{K_1}U_KEC_1}\right)U^+_{\rm cip} = \tag{24}$$

$$= \left(\frac{1}{|\mathcal{K}|}\frac{1}{|\mathcal{K}|}\sum_k\sum_{k_1}|k\rangle_{KK}\langle k|\otimes|k_1\rangle_{K_1K_1}\langle k_1|\otimes|c_1(k_1,k)\rangle_{C_1C_1}\langle c_1(k_1,k)|\right)\otimes\rho_E.$$

Напомним, что при реализации унитарного (обратимого) вычисления – зашифрования используются вспомогательные (мусорные) регистры, которые по окончании вычисления, переводятся обратно в исходное нулевое состояние и которые для экономии обозначений опускаем.

Матрица плотности после зашифрования одноразовым блокнотом имеет вид

$$\rho^{OTP}_{U_{K_1}U_KEC_1} = U_{OTP}\left(\rho_{U_{K_1}U_KEC_1}\right)U^+_{OTP} = \tag{25}$$

$$= \left(\frac{1}{|\mathcal{K}|}\frac{1}{|\mathcal{K}|}\sum_k\sum_{k_1}|k\rangle_{KK}\langle k|\otimes|k_1\rangle_{K_1K_1}\langle k_1|\otimes|c_{OTP}(k_1,k)\rangle_{C_1C_1}\langle c_{OTP}(k_1,k)|\right)\otimes\rho_E.$$

Далее, используя несколько раз неравенство треугольника для следового расстояния, получаем

$$\frac{1}{2}||\rho^{\rm cip}_{K_1KEC_1} - \rho^{OTP}_{U_{K_1}U_KEC_1}||_1 \le \tag{26}$$

$$\le \frac{1}{2}||\rho^{\rm cip}_{K_1KEC_1} - \rho^{\rm cip}_{U_{K_1}U_KEC_1}||_1 + \frac{1}{2}||\rho^{\rm cip}_{U_{K_1}U_KEC_1} - \rho^{OTP}_{U_{K_1}U_KEC_1}||_1 =$$

$$= \frac{1}{2}||U_{\rm cip}\left(\rho_{K_1KEC_1} - \rho_{U_{K_1}U_KEC_1}\right)U^+_{\rm cip}||_1 + \frac{1}{2}||\left(\rho^{\rm cip}_{U_{K_1}U_KC_1} - \rho^{OTP}_{U_{K_1}U_KC_1}\right)\otimes\rho_E||_1 =$$

$$= \frac{1}{2}||\rho_K\rho_{K_1E} - \rho_{U_K}\otimes\rho_{U_{K_1}}\otimes\rho_E||_1 + \frac{1}{2}||\left(\rho^{\rm cip}_{U_{K_1}U_KC_1} - \rho^{OTP}_{U_{K_1}U_KC_1}\right)\otimes\rho_E||_1 \le$$

$$\le \frac{1}{2}||\rho_K - \rho_{U_K}||_1 + \frac{1}{2}||\rho_{K_1E} - \rho_{U_{K_1}}\otimes\rho_E||_1 + \frac{1}{2}||\rho^{\rm cip}_{U_{K_1}U_KC_1} - \rho^{OTP}_{U_{K_1}U_KC_1}||_1 \le$$

$$\le (\varepsilon_K + \varepsilon_{K_1}) + \frac{1}{2}||\rho^{\rm cip}_{U_{K_1}U_KC_1} - \rho^{OTP}_{U_{K_1}U_KC_1}||_1.$$

2.2. Оценка следового расстояния блочного шифра до одноразового блокнота. Остается оценить последнее слагаемое в (26). Прямые вычисления дают

$$\frac{1}{2}||\rho^{\rm cip}_{U_{K_1}U_KC_1} - \rho^{OTP}_{U_{K_1}U_KC_1}||_1 = \tag{27}$$

$$= \frac{1}{2}\frac{1}{|\mathcal{K}|}\frac{1}{|\mathcal{K}|}\sum_k\sum_{k_1}{\rm Tr}_{C_1}\{|\ |c_1(k_1,k)\rangle_{C_1C_1}\langle c_1(k_1,k)| - |c_{OTP}(k_1,k)\rangle_{C_1C_1}\langle c_{OTP}(k_1,k)|\ |\} =$$

$$= \frac{1}{|\mathcal{K}|}\frac{1}{|\mathcal{K}|}\sum_k\sum_{k_1}\sqrt{1 - |_{C_1}\langle c_1(k_1,k)|c_{OTP}(k_1,k)\rangle_{C_1}|^2}.$$

При каждом k определим множества:

$\mathcal{K}_\perp(k)$ – множество значений шифр-текстов при данном сообщении k, которые отсутствуют – не достигаются ни при одном ключе k_1.

$\mathcal{K}_1(k)$ – множество значений шифр-текстов при данном сообщении k, которые имеют место только при одном ключе k_1.

$\mathcal{K}_2(k)$ – множество значений шифр-текстов при данном сообщении k, которые имеют место при двух ключах k_{1_1} и k_{1_2}.

...

$\mathcal{K}_L(k)$ – множество значений шифр-текстов при данном сообщении k, которые имеют место при L ключах k_{1_1}, k_{1_2}, ..., k_{1_L}, $L \le |\mathcal{K}|$.

При шифровании одноразовым блокнотом для каждого открытого текста (k) и каждого ключа ключа (k_1) имеется только одно значение шифр-текста – все множество шифр-текстов накрывается однократно (рис. 1). На рисунке 1 для иллюстрации показаны множества без коллизий и только множества парных и тройных коллизий.

Множество $\mathcal{K}_\perp$, это множество шифр-текстов, которые отсутствуют при шифровании блочным шифром.

Важно отметить, что выбирается реализация одноразового блокнота ближайшая, в смысле следового расстояния, к блочному шифру. Иначе говоря, такая реализация, при которой при каждом открытом тексте значения шифр-текстов для одноразового блокнота и блочного шифра совпадают на максимально возможном множестве значений ключей (рис. 1). Для остальных значений ключей шифр-тексты для блочного шифра недоступны – пространство $\mathcal{K}_\perp$.

Используя связь следового расстояния и фиделити [7], получаем

$$\frac{1}{2}\frac{1}{|\mathcal{K}|}\sum_{k_1}\mathrm{Tr}_{C_1}\{|\ |c_1(k_1,k)\rangle_{C_1C_1}\langle c_1(k_1,k)| -$$

$$-\ |c_{OTP}(k_1,k)\rangle_{C_1C_1}\langle c_{OTP}(k_1,k)|\ |\} =$$

$$=\frac{1}{|\mathcal{K}|}\sum_{k_1}\sqrt{1-|_{C_1}\langle c_1(k_1,k)|c_{OTP}(k_1,k)\rangle_{C_1}|^2}.$$

$$=\frac{1}{|\mathcal{K}|}|\mathcal{K}_\perp(k)|=\frac{1}{|\mathcal{K}|}\sum_{i=2}^{L}(i-1)|\mathcal{K}_i(k)|=\frac{|\mathcal{K}_{\mathrm{coll}}(k)|}{|\mathcal{K}|}= \tag{28}$$

Поясним вычисления по формуле (28). Пусть шифруемый текст k фиксирован, и ключ шифрования есть k_1.

Пусть множество ключей $\mathcal{K}_1$, для которых существует единственный шифр-текст, то скалярное произведение в (28) на всех ключах из данного множества $|_{C_1}\langle c_1(k_1,k)|c_{OTP}(k_1,k)\rangle_{C_1}|=1$ равно единице, поэтому данное слагаемое не дает вклад в сумму по k_1.

Пусть множество пар ключей $\mathcal{K}_2$, для каждой пары которых существует общий шифр-текст при шифровании блочным шифром. Выберем такую пару ключей $k_{1,1}$ и $k_{1,2}$. На одном из ключей, например, $k_{1,1}$ шифр-тексты для блочного шифра и одноразового блокнота совпадают, скалярное произведение в (28) $|_{C_1}\langle c_1(k_{1,1},k)|c_{OTP}(k_{1,1},k)\rangle_{C_1}|=1$ равно единице, данное слагаемое не дает вклад в сумму по k_1.

Однако для второго ключа $k_{1,2}$ шифр-тексты для блочного шифра и одноразового блокнота не совпадают, скалярное произведение в (28) $|_{C_1}\langle c_1(k_{1,2},k)|c_{OTP}(k_{1,2},k)\rangle_{C_1}|=0$ равно нулю, данное слагаемое дает вклад единица в сумму по k_1.

В итоге из множества ключей $\mathcal{K}_2$ в сумму (28) дает вклад $(2-1)|\mathcal{K}_2|$ слагаемых.

Аналогичными рассуждениями подсчитывается число слагаемых в сумме (28). Вклад в сумму (28) от множества ключей из $\mathcal{K}_i$ дают $(i-1)|\mathcal{K}_i|$ слагаемых.

Из рассуждений выше следует, что число ненулевых слагаемых в (28) совпадает с размером множества $|\mathcal{K}_\perp(k)|$, это та часть множества шифр-текстов, которые отсутствуют при шифровании блочным шифром. Из рассуждений выше также следует, что (см. для пояснения рис. 1)

$$|\mathcal{K}_\perp(k)|=\sum_{i=2}^{L}(i-1)|\mathcal{K}_i(k)|,$$

здесь $|\mathcal{K}_i(k)|$ – размер множества i-ых коллизий при данном сообщении k.

При вычислении следового расстояния в (27) удобно сначала вычислять сначала сумму по k_1 при фиксированном k. Это связано с тем, что для разных сообщений k и одном и том же ключе шифрования k_1 шифр-тексты будут разными, что следует из условия однозначного расшифрования разных сообщений, зашифрованных на одном ключей. По этой причине подсчет ненулевых слагаемых в сумме (27) был бы не столь прозрачным.

Естественно оба способа подсчета приводят к одинаковому результату.

Далее, имеем

$$\frac{1}{2}||\rho^{\mathrm{cip}}_{U_KU_{K_1}C_1}-\rho^{OTP}_{U_KU_{K_1}C_1}||_1=$$
$$=\frac{1}{|\mathcal{K}|}\sum_{k}\frac{|\mathcal{K}_{\mathrm{coll}}(k)|}{|\mathcal{K}|}=\overline{|\mathcal{K}_{\mathrm{coll}}|}. \tag{29}$$

В итоге для средней сложности Q_{U,π_0} поиска ключа с учетом (9) находим

$$Q_{U,\pi_0}\geq\left(1-\frac{2\delta_1}{\pi_0}\right)\left(\frac{|\mathcal{K}|(1-8\delta_1)+1}{2}\right), \tag{30}$$

где (см. (12), (13))

$$\delta_1\leq\varepsilon_K+\varepsilon_{K_1}+\overline{|\mathcal{K}_{\mathrm{coll}}|}. \tag{31}$$

3. Заключение и обсуждение результатов. Таким образом показано, что трудоемкость (сложность перебора) по поиску продвигаемого по сети ключа зависит от величины δ_1, которая мажорируется величиной $\overline{|\mathcal{K}_\perp|}$, а также величинами $\varepsilon_K,\varepsilon_{K_1}$, которые определяют неидеальность внешнего ключа и квантовых ключей. По смыслу величина $\overline{|\mathcal{K}_\perp|}$ совпадает со средней вероятностью коллизий блочного шифра $\overline{|\mathcal{K}_{\mathrm{coll}}|}$. Чем больше коллизий имеет шифр, соответственно, накрывает меньшее множество шифр-текстов, тем меньшее число шагов перебора требуется для нахождения ключа.

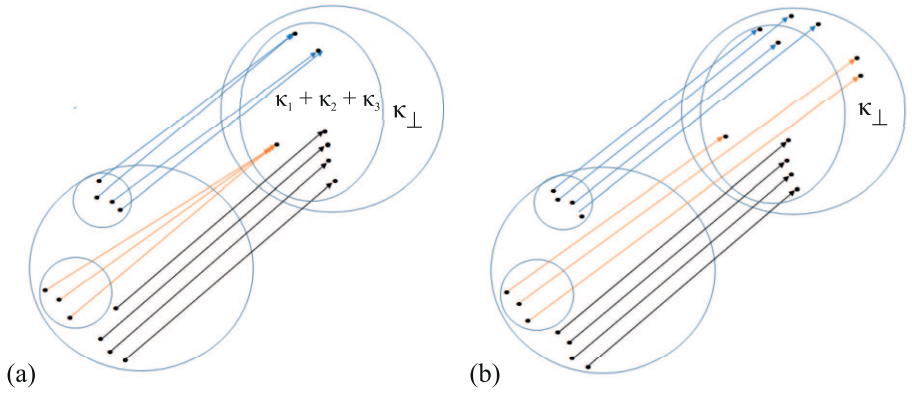

Рис. 1. (Цветной онлайн) (a) – Схематическое изображение множества ключей и шифр-текстов для блочного шифра; (b) – схематическое изображение множества ключей и шифр-текстов для одноразового блокнота

Даже в случае идеального внешнего ключа и идеальных квантовых ключей ($\varepsilon_K = 0$, $\varepsilon_{K_1} = 0$), при шифровании внешнего ключа блочным шифром, перенесенный ключ уклоняется, в смысле следового расстояния, от идеального ключа на вероятность коллизий блочного шифра. Трудоемкость по поиску ключа уменьшается по сравнению с полным перебором на число коллизий блочного шифра. Как предельный (патологический пример) плохого шифра, когда число коллизий стремится к размеру полного множества шифров $|\mathcal{K}|$ – почти все шифр-тексты на разных ключах слипаются, трудоемкость, согласно (30), (31), формально стремится к нулю – ключ определяется за один шаг перебора.

В то же время, при проталкивании идеального внешнего ключа при шифровании одноразовым блокнотом на идеальных квантовых ключах ($\varepsilon_K = 0$, $\varepsilon_{K_1} = 0$), перенесенный ключ остается идеальным ($\delta_1 = 0$) – все позиции ключа независимы и равновероятны.

На сегодняшний день, неизвестно эффективных алгоритмов для вычисления коллизий ни для одного блочного шифра. Подсчет коллизий на классическом вычислителе требует полного перебора по всему ключевому пространству $|\mathcal{K}| = 2^{256}$ (при длине ключа $n = 256$ бит), что практически невозможно.

Длина ключа в российском алгоритме блочного шифрования “Кузнечик” составляет 256 бит. Квантовый алгоритм [8] остается экспоненциально сложным и требует $\sqrt{|\mathcal{K}|} = 2^{128}$ шагов вычислений. Выше был рассмотрен случай переноса ключей через один сегмент квантовой сети. Перенос ключей через N сегментов рассматривается аналогично. При этом $\delta_N = \sum_{\ell=1}^{N} \delta_1$-секретность ключей падает линейно с ростом числа сегментов, что позволяет оценить критическое число сегментов сети, на которых сохраняется требуемая стойкость (ε-секретность) финального перенесенного ключа.

Таким образом, шифрование продвигаемого ключа одноразовым блокнотом на ключах на отдельных сегментах сохраняет так называемую составную секретность (*composable security*) общего ключа. Однако, использованием одноразового блокнота, в отличии от блочного шифра не обеспечивает аутентичность общего ключа. Кроме секретности ключа, необходимо обеспечить теоретико-информационную аутентичность общего ключа, которая достигается хешированием (см., например, [9]).

Отметим, что обычно используемый перенос ключа с помощью операции XOR (см., например, [10]), без дальнейших исследований “качества” перенесенного ключа – близости распределения ключей к идеальному равновероятному, недостаточен, для того, чтобы знать криптографические свойства финального ключа (в том числе и сложность, трудоемкость поиска ключа при его дальнейшем использовании для шифрования сообщений). Кроме того, полученные выше оценки позволяют оценить насколько безопасно можно использовать данный ключ в последующих сеансах – какое число переносов по сети можно сделать, до тех пор пока уклонение (фактически δ_1 в (31)) распределения вероятностей перенесенного ключа от равновероятного не превысит критической величины.

Как было показано ранее [6], величина δ_1, от которой зависит трудоемкость перебора, имеет следующий операциональный смысл. Пусть размер полного ключевого пространства $|\mathcal{K}| = 2^{256} \approx 1.5 \cdot 10^{77}$ (напомним, что число атомов в видимой части Вселенной оценивается как 10^{77}). Пусть опробовается M первых ключей. Число шагов перебора даже при $M = 2^{128} \approx 10^{38}$ является запредельным. Величи-

на δ_1 (31), которую можно реально достичь в системах квантовой криптографии на сегодня, имеет порядок $\delta_1 = 2^{-32} \approx 2.5 \cdot 10^{-10}$. Поэтому $|\mathcal{K}|\delta_1 \gg M$, в этом случае среднее число шагов опробования ключей до первого определения ключа – до первого сообщения, которое, возможно, будет дешифровано, есть $\approx \frac{1}{\delta_1} \approx 10^{10}$, т.е. из 10^{10} сообщений в среднем, возможно, будет прочитано одно сообщение. После переноса через N сегментов (или шифровании на ключе N раз) среднее число сообщений до первого прочитанного будет $\approx \frac{1}{N\delta_1}$.

Выражаю благодарность И. М. Арбекову, В. А. Кирюхину, С. П. Кулику, А. В. Уривскому, а также коллегам по Академии криптографии Российской Федерации и Инфотекс за многочисленные интересные обсуждения и замечания.

1. https://www.youtube.com/watch?v=0WAuDcYhKbo.
2. R. Renner, arXiv:quant-ph/0512258v2 11 Jan 2006.
3. Ch. Portmann and R. Renner, arXiv:1409.3525v1 [quant-ph] 11 Sep 2014.
4. C. E. Shannon, *A Mathematical Theory of Communication*, Bell System Technical Journal, July, 379 (1948); Oct., 623 (1948); *The material in this paper appeared originally in a confidential report A Mathematical Theory of Cryptography*, dated Sept. 1, (1945).
5. I. M. Arbekov, Математические вопросы криптографии **78**(2), 27 (2017).
6. И. М. Арбеков, С. Н. Молотков, ЖЭТФ **151**(6), 1 (2017).
7. M. M. Wilde, arXiv:1106.1445v6 [quant-ph] 2 Dec 2015.
8. С. Н. Молотков, Письма в ЖЭТФ **117**, 80 (2023).
9. S. N. Molotkov, Laser Phys. Lett. **19**, 075203 (2022).
10. Д. Д. Сукачев, Успехи физических наук **191**(10), 1077 (2021), раздел 6.2 “Доверенные узлы”.