Письма в ЖЭТФ, том 121, вып. 11, с. 914 – 921 © 2025 г. 10 июня

Статистика Бозе–Эйнштейна, случайные блочные шифры и одноразовый блокнот в квантовой криптографии

С. Н. Молотков[+1)], *И. С. Сущев*[*]

[+]*Институт физики твердого тела имени Ю. А. Осипьяна РАН, 142432 Черноголовка, Россия*

[*]*Центр квантовых технологий, Физический факультет, МГУ имени М. В. Ломоносова, 119991 Москва, Россия*

Поступила в редакцию 11 апреля 2025 г.
После переработки 22 апреля 2025 г.
Принята к публикации 28 апреля 2025 г.

Многие задачи статистической физики, классической и квантовой теории информации, и в частности, квантовой криптографии, имеют много общего, поскольку сводятся к обработке экспоненциально больших множеств. Показано, что имеется глубокая связь между размещением бозонов по энергетическим уровням и числом коллизий случайного блочного шифра. Получена явная аналитическая оценка числа коллизий случайного блочного шифра – число коллизий оказывается равным числу пустых уровней при размещении бозонов по уровням. Число коллизий имеет практический интерес, поскольку определяет трудоемкость поиска ключей при их продвижении по квантовой сети.

DOI: 10.31857/S0370274X25060101, EDN: KCOVMY

Введение. Квантовая криптография – квантовое распределение ключей (КРК) позволяет распределять ключи между удаленными пользователями, используя открытые и доступные для вторжения квантовый и классический аутентичный каналы связи [1, 2]. Первый запуск системы требует стартового ключа для аутентификации, после сеанса КРК часть квантового ключа используется для аутентификации в следующем сеансе, а остальная часть – для других криптографических целей. По сути системы КРК представляют собой системы расширения первичного ключа. Как было показано в [3], после первого запуска системы возможна практически сколь угодно долгая работа системы КРК до следующего перезапуска [3]. В дальнейшем квантовые ключи используются для различных криптографических целей, например, для продвижения *внешних ключей* через доверенные промежуточные узлы по квантовой сети [4–8] или шифрования сообщений. При продвижении ключей по сети или шифровании сообщений используется шифрование на квантовых ключах.

Возможны различные способы шифрования.

1) Продвигаемый ключ или сообщение шифруется одноразовым блокнотом [9–11] на квантовых ключах.

2) Продвигаемый ключ или сообщение шифруется блочным шифром с использованием квантовых ключей.

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

Перенесенный по сети ключ используется, например, для защиты трафика при передаче аудио- и видео-информации, как это происходит в квантовой университетской сети [8].

При шифровании продвигаемого по сети внешнего ключа квантовыми ключами в режиме одноразового блокнота Вернама, Котельникова, Шеннона [9–11] невозможно определить продвигаемый ключ (“взломать одноразовый блокнот”) даже теоретически. Однако на сегодняшний день по технологическим причинам чаще используется второй способ шифрования продвигаемого внешнего ключа.

По этой причине принципиально важно знать, как изменится трудоемкость по поиску ключа шифрования [12], в случае, когда шифрование осуществляется блочным шифром или одноразовым блокнотом. Какие характеристики блочного шифра нужно знать, чтобы ответить на данный вопрос?

В работе [6] была получена *точная явная формула*, показывающая, что уменьшение трудоемкости перебора выражается через число *коллизий блочного шифра.*

В чем тогда состоит проблема? Проблема в том, что ни для одного блочного шифра число коллизий неизвестно.

Число коллизий уменьшает трудоемкость перебора по поиску ключей при шифровании блочным шифром по сравнению с трудоемкостью поиска ключей при шифровании одноразовым блокнотом. В случае шифрования одноразовым блокнотом трудоемкость поиска ключей имеет *теоретический максимум.*

Почему число коллизий неизвестно? Удобно пояснить этот факт на примере. Пусть открытое сообщение фиксировано, тогда для подсчета числа коллизий блочного шифра требуется "пробежаться" по всем ключам и выяснить, на каком количестве разных ключей шифртексты совпадают. Такую процедуру нужно проделать для всех сообщений.

Для современных блочных шифров, например, для Российского стандарта "Кузнечик" [13], длина ключа 256 бит, размер множества всех ключей имеет порядок $2^{256} \approx 10^{77}$. Вычисление шифртекстов на всех ключах требует $2^{256} \approx 10^{77}$ вычислительных операций, что находится далеко за пределами всех вычислительных возможностей. Напомним, что число атомов в видимой части Вселенной оценивается как 10^{77}.

Квантовые алгоритмы поиска коллизий блочных шифров на практическом уровне не улучшают ситуацию [14]. Сложность вычислений на квантовом компьютере составляет $\sqrt{2^{256}} \approx 10^{38}$, что также находится за разумными пределами. Кроме того, квантовый вычислитель пока существует как умозрительный объект.

В связи с этим возникает вопрос о приближенной аналитической оценке числа коллизий.

Основная идея приближенной аналитической оценки числа коллизий. *Возникает вопрос: существуют ли блочные шифры, для которых возможна аналитическая оценка числа коллизий? Если такие шифры существуют, то можно оценить число коллизий для такого шифра и рассматривать данный шифр как приближение к регулярному блочному шифру. Далее, центральная идея аналитической оценки числа коллизий для блочного шифра состоит в замене регулярного блочного шифра случайным блочным шифром.*

В определенном смысле данная идея перекликается с идеей Шеннона в теории кодирования [15], когда вместо регулярного отдельного кода рассматривается ансамбль случайных кодов, в каждом из которых используется случайный выбор кодовых слов – каждому сообщению случайно, в соответствии с некоторым распределением вероятностей, сопоставляется случайное кодовое слово (см. также [16]).

Применительно к рассматриваемой ситуации, для каждого ключа и сообщения шифртекст формируется не по некоторому регулярному правилу, а случайно, т.е. каждая конкретная реализация кода сама является случайной величиной.

Такое приближение основано не на логических доводах, а скорее на большом числе "экспериментальных" фактов о поведении блочных шифров, например, свойствах псевдослучайных последовательностей, получаемых на выходе блочного шифра, которые ведут себя практически неотличимо от случайных.

Ниже будет показано, что существует глубокая связь между статистикой Бозе–Эйнштейна и шифрованием *случайным блочным шифром.*

При *аналитической оценке числа коллизий блочного шифра* используется приближение случайных блочных шифров по аналогии со случайным выбором кодовых слов в теории кодирования при вычислении пропускной способности каналов связи [16].

В рамках данного приближения будет получена *аналитическая формула, дающая оценку числа коллизий.*

Размещение бозонов по энергетическим уровням. Уточним более детально, как статистика Бозе–Эйнштейна, которой подчиняются размещения бозе частиц по уровням, связана со случайными блочными шифрами. Рассмотрим размещение бозонов по энергетическим уровням.

Нас будет интересовать среднее, по всевозможным размещениям, число незаполненных уровней. Как будет показано ниже, именно, данная величина окажется равной числу коллизий для случайных блочных шифров.

Число уровней будет равно числу ключей $|\mathcal{K}| = 2^{256} \approx 10^{77}$ – размер ключевого пространства.

Пусть имеется $|\mathcal{K}|$-кратно вырожденный уровень, т.е. имеется $|\mathcal{K}|$ состояний с одинаковой энергией, на которые требуется разместить $|\mathcal{K}|$ тождественных бозе частиц. Возможны $\frac{(|\mathcal{K}|+|\mathcal{K}|-1)!}{|\mathcal{K}|!(|\mathcal{K}|-1)!}$ вариантов размещения частиц. *Все варианты равновероятны.* На каждом уровне может находится любое число частиц от 0 до $|\mathcal{K}|$. Каждая из $|\mathcal{K}|$ частиц равновероятно размещается на один из $|\mathcal{K}|$ уровней вероятностью $\frac{1}{|\mathcal{K}|}$. Нас будет интересовать среднее число пустых уровней. Здесь удобно воспользоваться классическими результатами о размещении одинаковых $|\mathcal{K}|$ предметов по $|\mathcal{K}|$ ящикам [17, 18]. Вероятность того, что m из $|\mathcal{K}|$ ящиков останутся пустыми есть

$$\mathrm{P}(m, |\mathcal{K}|) = C_{|\mathcal{K}|}^{m} \sum_{\ell=0}^{|\mathcal{K}|-m} (-1)^{\ell} C_{|\mathcal{K}|-m}^{\ell} \left(1 - \frac{m+\ell}{|\mathcal{K}|}\right)^{m}, \tag{1}$$

где C_n^m – биномиальный коэффициент. Среднее число пустых уровней (ящиков) по всем случайным размещениям равно (см., например, [17, 18])

$$\mathbf{E}(m)=\sum_{m=0}^{|\mathcal{K}|} m\mathrm{P}(m,|\mathcal{K}|)=|\mathcal{K}|\left(1-\frac{1}{|\mathcal{K}|}\right)^{|\mathcal{K}|}. \qquad (2)$$

Используя формулу Эйлера для замечательного предела при $|\mathcal{K}|\gg 1$, получаем

$$\frac{\mathbf{E}(m)}{|\mathcal{K}|}\to e^{-1}\approx 0.367. \qquad (3)$$

Резюмируем, что было использовано при подсчете среднего числа пустых уровней. Каждое размещение $|\mathcal{K}|$ тождественных частиц – бозонов по $|\mathcal{K}|$ уровням независимо. Выбор уровня для размещения выбирается равновероятно.

Приведение к общей длине блочного шифра и одноразового блокнота. Для сравнения блочного шифра и одноразового блокнота необходимо, чтобы длина ключа, сообщения и шифртекста совпадали. Пусть имеется алгоритм блочного шифрования. Для определенности будем иметь в виду блочный шифр "Кузнечик" [13]. Длина ключа составляет 256 бит. Открытый текст шифруется блоками по 128 бит. Пусть m_1 – шифруемый текст 128 бит, k – ключ шифрования 256 бит, $C(k,m_1)$ – функция блочного шифрования – шифртекст 128 бит. При шифровании одноразовым блокнотом длина шифруемого сообщения, шифртекста должны быть одинаковы и равны длине ключа – 256 бит. Для сравнения близости блочного шифра к одноразовому блокноту необходимо конкатенировать два блока шифруемого текста по 128 бит, чтобы шифртекс был 256 бит. Иначе говоря, будем считать шифртекст $\mathcal{C}_{\mathrm{Cip}}(k,m_1||m_2)=C(k,m_1)||C(k,m_2)$, где длина $m_1||m_2$ равна 256 бит, и длина $\mathcal{C}_{\mathrm{Cip}}(k,m_1||m_2)$ также равна 256 бит. Для одноразового блокнота $\mathcal{C}_{OTP}(k,m_1||m_2)$ – длина шифртекста для одноразового блокнота также равна 256 бит. Далее $k\in\mathcal{K}=\{0,1\}^{256}$, $|\mathcal{K}|=2^{256}$, $m\in\mathcal{M}=\{0,1\}^{256}$, $|\mathcal{M}|=2^{256}$) $C\in\mathcal{C}=\{0,1\}^{256}$, $|\mathcal{C}|=2^{256}$.

Приближение блочного шифра случайными размещениями бозе частиц. Пусть случайно выбран некоторый ключ k из $|\mathcal{K}|$ ключей. Пусть заданы блоки шифруемых сообщений $\{M_1,M_2,...,M_{|\mathcal{M}|}\}$ каждый по 256 бит. Всевозможные значения зашифрованных сообщений на ключе k_1 $\{\mathcal{C}_{\mathrm{Cip}}(k_1,M_1),\mathcal{C}_{\mathrm{Cip}}(k_1,M_2),...,\mathcal{C}_{\mathrm{Cip}}(k_1,M_{|\mathcal{M}|})\}$, каждое длиной по 256 бит, заменяются *случайной подстановкой* на множестве значений $\{M_1,M_2,...,M_{|\mathcal{M}|}\}$. Естественно, что разные сообщения переходят в разные значения шифртекстов, полученных на одном ключе. *Это требуется для однозначного расшифрования шифртекстов, отвечающих разным открытым текстам, зашифрованных на одном ключе.*

В итоге получается *случайная* таблица шифртекстов для разных сообщений, зашифрованных на разных ключах. Вертикальная колонка отвечает шифртекстам одного открытого текста на разных ключах.

Отметим, что условие однозначного расшифрования разных сообщений, зашифрованных на одном и том же ключе, означает, что шифртексты для разных сообщений (для одного ключа) представляют собой подстановку на множестве $\{0,1\}^{256}$.

Поскольку в каждой строке подстановка, отвечающая зашифрованию на одном ключе разных сообщений, выбирается случайно и независимо для разных ключей – строк, то шифртексты для некоторых открытых текстов на разных ключах могут совпадать.

Пусть для каждого ключа k_i $(i=1,...,|\mathcal{K}|)$ (далее строки в таблице) и сообщения m_j $(j=1,...,|\mathcal{M}|)$ выбирается случайная подстановка. Подстановка выбирается случайно и равновероятно из всевозможных подстановок независимо для каждого ключа. *Это и есть случайный шифр. Строки в таблице выбираются равновероятно с вероятностью $\frac{1}{2^{256}}$ из множества $\{0,1\}^{256}$ бинарных строк.*

Введем обозначения, $\mathcal{C}_i(j)=\mathcal{C}(k_i,m_j)$. Далее для каждого *случайного шифра $\mathcal{C}$* имеем щифр-таблицу

$$\mathcal{C}=\begin{pmatrix} \mathcal{C}_1(1) & \mathcal{C}_1(2) & ... & \mathcal{C}_1(|\mathcal{M}|)\\ \mathcal{C}_2(1) & \mathcal{C}_2(2) & ... & \mathcal{C}_2(|\mathcal{M}|)\\ ... & ... & ... & ...\\ \mathcal{C}_{|\mathcal{K}|}(1) & \mathcal{C}_{|\mathcal{K}|}(2) & ... & \mathcal{C}_{|\mathcal{K}|}(|\mathcal{M}|) \end{pmatrix}, \qquad (4)$$

т.е. шифр сам является случайной величиной, по аналогии со случайным кодом в теории кодирования Шеннона [15, 16]. Ключи k_i, сообщения m_j – пробегают всевозможные значения из $\{0,1\}^n$ (для Кузнечика $n=256$). Шифртексты $\mathcal{C}_i(j)$ принимают значения на множестве $\{0,1\}^n$, но для блочного шифра из-за коллизий, часть значений из множества $\{0,1\}^n$ не появляется.

По построению – всевозможные случайные шифры равновероятны, их всего $\mathrm{P}(\mathcal{C})=\frac{1}{N_{\mathcal{C}}}$, где $N_{\mathcal{C}}=(|\mathcal{K}|!)^{|\mathcal{K}|}$ – число различных вариантов шифртаблицы.

Рассмотрим, например, первый столбец таблицы для конкретной реализации случайного шифра, который отвечает шифртекстам для первого сообщения. Поскольку шифртексты на разных ключах могут совпадать, то соберем одинаковые шифртектсы в отдельные ячейки. Будут ячейки, содержащие один шифртекст $N_1(\mathcal{C},m_1)$ – число ячеек, два шифртекста $N_2(\mathcal{C},m_1)$ – число ячеек, три и т.д. Полное число заполненных ячеек

$N_{\text{fill}}(\mathcal{C}, m_1) = \sum_{\ell=1}^{N_{\max}(\mathcal{C}, m_1)} N_i(\mathcal{C}, m_1)$. Число ячеек $N_{\text{Empty}}(\mathcal{C}, m_1) = N - N_{\text{fill}}(\mathcal{C}, m_1)$ останется незаполненными. Число пустых ячеек зависит от конкретной реализации случайного шифра $\mathcal{C}$ и сообщения m_i (в данном случае от m_1).

Важно, что среднее число пустых ячеек по всем ключам и по всем случайным шифрам уже не зависит от номера сообщения, такое среднее пустых ячеек одинаково по любому столбцу. Независимость среднего значения от номера столбца является следствием случайного выбора шифртекста. Именно по этой причине приходится использовать приближение блочного шифра случайным блочным шифром. Среднее равно математическому ожиданию числа пустых ящиков при случайном размещении $|\mathcal{K}|$ бозе частиц по $|\mathcal{K}|$ ящикам.

Соберем в каждый ящик для данного открытого текста все одинаковые шифртексты. Из-за совпадения – коллизий шифртекстов для отдельных сообщений, зашифрованных на разных ключах, часть ящиков окажется пустой. Число пустых ящиков зависит от конкретной реализации случайного блочного шифра и само является случайной величиной.

Как следует из выше сказанного, среднее число пустых ящиков при размещении бозонов по уровням равно среднему числу шифртекстов для случайных блочных шифров, которые не возникают ни для одного ключа и ни для одного сообщения. Ниже будет показано, что следовое расстояние между приближением блочных шифров и одноразовым блокнотом как раз равно среднему числу пустых ящиков.

Перейдем к одноразовым блокнотам. Одноразовые блокноты [15] являются идеальными (совершенными) шифрами. Любой одноразовый блокнот представляет собой латинский квадрат. Все клетки шифр-таблицы заполнены. Для каждого ключа строка представляет собой подстановку. Для разных ключей постановки таковы, что в каждой строке и столбце присутствуют все элементы таким образом, что в каждой строке и каждом столбце каждый элемент присутствует только однократно.

Для каждой реализации случайного блочного шифра существует ближайший одноразовый блокнот. Это такой блокнот, для которого суммарное отличие шифртекстов по всей таблице наименьшее.

Иллюстративный пример. Прежде чем привести вывод расстояния между случайным блочным шифром и одноразовым блокнотом в смысле следовой метрики, удобно привести простой иллюстративный пример. Из данного примера несложно можно будет увидеть, что расстояние как раз равно среднему числу пустых ящиков при размещении бозонов.

Пусть $|\mathcal{K}| = 2$. Имеется для сообщения m_1 и m_2 два ключа k_1 и k_2 и $(|\mathcal{K}|!)^{|\mathcal{K}|} = (2!)^2 = 4$ случайных шифров. Все 4 таблицы случайных шфров приведены на рис. 1. Имеются два случайных шифра, когда шифртексты на ключах k_1 и k_2 совпадают, и два варианта, когда шифртексты на разных ключах разные.

Для краткости в клетках таблицы цифры 1 и 2 отвечают шифртекстам для k_i, m_j соответственно, для случайного блочного шифра (C) и одноразового блокнота (OTP), $C_{k_i}(m_j)$ и $OTP_{k_i}(m_j)$ – элементы, стоящие на пересечении k_i строки и m_j столбца, и равные 1 или 2.

Фиделити – среднее расстояние по всем случайным блочным шифрам и соответствующим *ближайшим одноразовым блокнотам для каждой случайной реализации блочного шифра*, равна

$$\mathcal{F}(C, OTP) = \tag{5}$$
$$= \frac{1}{|\mathcal{M}|} \sum_{m_j \in \mathcal{M}} \frac{1}{|\mathcal{K}|} \sum_{k_i \in \mathcal{K}} \frac{1}{|\mathcal{C}|} \sum_{C \in \mathcal{C}} \delta_{C_{k_i}(m_j), OTP_{k_i}(m_j)}.$$

Суммирование проводится по всем клеткам 4-х таблиц для случайных блочных шифров и ближайших к ним одноразовых блокнотов.

Например, ближайшим одноразововым блокнотом к случайным блочным шифрам $C(12/12)$ является $OTP(12/21)$, для $C(21/21)$ – ближайший $OTP(21/11)$, для $C(12/21)$ – ближайший $OTP(12/21)$, для $C(21/21)$ – ближайший $OTP(21/12)$.

Подсчет ненулевых слагаемых только по тем клеткам, где значения шифртекстов совпадают. В итоге, по всем реализациям случайных блочных шифров имеется 12 совпадений, число не совпадений – число пустых клеток при размещениям бозонов рано 4.

Фиделити равна

$$\mathcal{F}(C, OTP) = \frac{N_{\text{Ful}} - N_{\text{Empty}}}{N_{\text{Ful}}} = \frac{16-4}{16} = \frac{3}{4}, \tag{6}$$

соответственно, расстояние между случайным блочным шифром и одноразовым блокнотом равно

$$1 - \mathcal{F}(C, OTP) = \frac{N_{\text{Empty}}}{N_{\text{Ful}}} = \frac{1}{4}. \tag{7}$$

Среднее число пустых ящиков есть $\frac{1}{2}\frac{1}{2}\frac{1}{4}4 = 0.25$.

Таким образом, расстояние между одноразовым блокнотом и случайным блочным шифром выражается через размер множества шифртекстов, недоступных для блочного шифра – числу пустых ящиков при размещении бозонов.

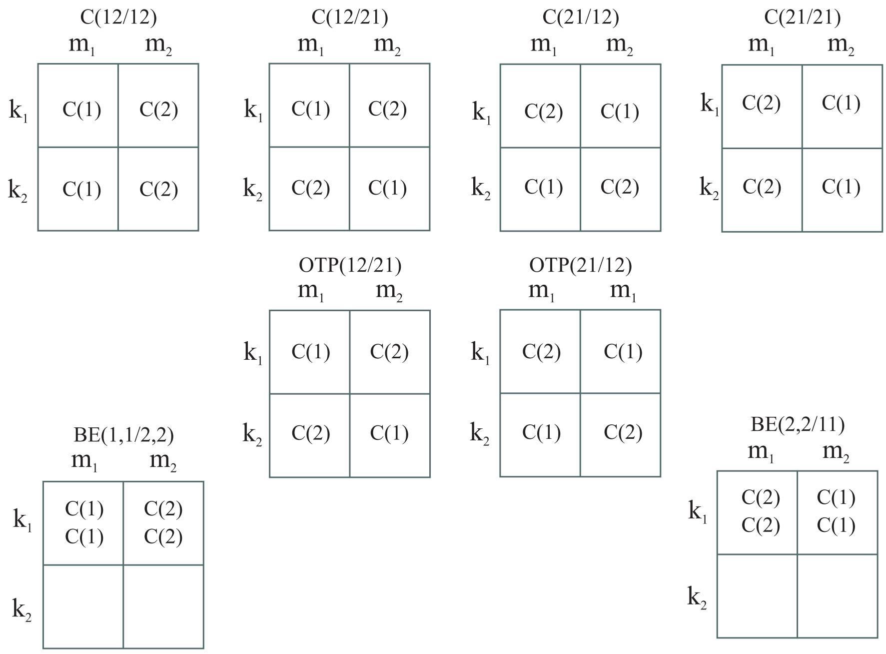

Рис. 1. (Цветной онлайн) Верхняя часть – таблицы случайных блочных шифров. Средняя часть – таблицы одноразовых блокнотов. Нижняя часть – таблицы случайного размещения бозонов

Оценка следового расстояния блочного шифра до одноразового блокнота. В квантовой криптографии секретность ключей формулируется в терминах различимости квантовых состояний – матриц плотности, отвечающим реальной и идеальной ситуациям при квантовом распределении ключей. Метрикой близости двух квантовых состояний является следовая метрика (см. ниже). В классической криптографии секретность ключей понимается в терминах сложности перебора ключей.

Идеальная ситуация – это ситуация, когда отсутствует вторжение в квантовый и классический каналы связи. В реальной ситуации имеются атаки на квантовый и классический каналы связи. Матрицы плотности до зашифрования после реального (ρ_{KE}) и идеального ($\rho_{U_K} \otimes \rho_E$) квантового распределения ключей имеют вид

$$\rho_{KE} = \sum_k P_K(k)|k\rangle_{K\,K}\langle k| \otimes \rho_E^k,$$
$$\rho_{U_K} = \frac{1}{|\mathcal{K}|}\sum_k |k\rangle_{K\,K}\langle k|, \qquad (8)$$
$$\rho_E = \mathrm{Tr}_K\{\rho_{KE}\} = \sum_k P_K(k)\rho_E^k,$$

здесь ρ_E^k – матрица плотности Евы, коррелированная с квантовым ключом k, $P_K(k)$ – функция распределения ключей после реального сеанса КРК, ρ_{U_K} – матрица плотности, отвечающая идеальным равновероятным ключам, $|k\rangle_K = |k_1\rangle|k_2\rangle...|k_n\rangle$ – ортогональные квантовые состояния, сопоставленные битовой строке ключей $k = (k_1, k_1, ..., k_n)$, $k_i = 0, 1$, $i = 1, 2, ..., n$.

В квантовой криптографии ключи называются ε_{QKD}-секретными [2, 19], если следовое расстояние между матрицами плотности (8) равно

$$\frac{1}{2}||\rho_{KE} - \rho_{U_K} \otimes \rho_E||_1 < \varepsilon_{QKD}. \qquad (9)$$

Далее, пусть ρ_{U_M}, отвечающая всевозможным сообщениям, имеет вид

$$\rho_{U_M} = \frac{1}{|\mathcal{M}|}\sum_m |m\rangle_{M\,M}\langle m|, \qquad (10)$$

где $|m\rangle_M = |m_1\rangle|m_2\rangle...|m\rangle_n$ – ортогональные квантовые состояния, отвечающая всевозможным сообщениям, $m = (m_1, m_1, ..., m_n)$, $m_i = 0, 1$, $i = 1, 2, ..., n$. Для того, чтобы не загромождать выкладки, считаем, что сообщения выбираются равновероятно. Полученные результаты будут справедливы и для неравновероятного выбора сообщений.

Зашифрование блочным шифром и одноразовым блокнотом производится действием унитарного оператора, действующего на регистры ключей, сообщений и на пустой регистр, предварительно подготовленный для записи зашифрованных состояний. Матрицы плотности для реальной и идеальной ситуаций до зашифрования, с учетом пустого регистра, куда будет записан результат зашифрования, имеют вид

$$\rho_{KMEC} = \frac{1}{|\mathcal{C}|}\sum_{C\in\mathcal{C}} \rho_{U_M}\otimes\rho_{KE}\otimes|0\rangle_{CC}\langle 0|,$$
$$\rho_{U_KU_MEC} = \frac{1}{|\mathcal{C}|}\sum_{C\in\mathcal{C}} \rho_{U_K}\otimes\rho_{U_M}\otimes\rho_E\otimes|0\rangle_{CC}\langle 0|. \tag{11}$$

Зашифрование блочным шифром и одноразовым блокнотом описывается унитарными операторами, имеем

$$\rho^{\mathrm{Cip}}_{KMEC} = U_{\mathrm{Cip}}\left(\rho_{KMEC}\right)U^{+}_{\mathrm{Cip}} = \tag{12}$$
$$= \frac{1}{|\mathcal{C}|}\sum_{C\in\mathcal{C}}\frac{1}{|\mathcal{M}|}\sum_{m\in\mathcal{M}}\sum_{k\in\mathcal{K}} P_K(k)|k\rangle_{KK}\langle k|\otimes$$
$$\otimes|m\rangle_{MM}\langle m|\otimes\rho^k_E\otimes|C_{\mathrm{Cip}}(k,m)\rangle_{CC}\langle C_{\mathrm{Cip}}(k,m)|,$$

и

$$\rho^{\mathrm{Cip}}_{U_KU_MEC} = U_{\mathrm{Cip}}\left(\rho_{U_KU_MEC}\right)U^{+}_{\mathrm{Cip}} = \tag{13}$$
$$= \Bigg(\frac{1}{|\mathcal{C}|}\sum_{C\in\mathcal{C}}\frac{1}{|\mathcal{M}|}\frac{1}{|\mathcal{K}|}\sum_{m\in\mathcal{M}}\sum_{k\in\mathcal{K}}|k\rangle_{KK}\langle k|\otimes$$
$$\otimes|m\rangle_{MM}\langle m|\otimes|C_{\mathrm{Cip}}(k,m)\rangle_{CC}\langle C_{\mathrm{Cip}}(k,m)|\Bigg)\otimes\rho_E,$$

где

$$|C_{\mathrm{Cip}}(k,m)\rangle_C = |C_{1_{\mathrm{Cip}}}(k,m)\rangle|C_{2_{\mathrm{Cip}}}(k,m)\rangle...|C_{n_{\mathrm{Cip}}}(k,m)\rangle$$

– квантовые состояния, отвечающие зашифрованным блочным шифром сообщениям,

$$C_{\mathrm{Cip}}(k,m) = (C_{1_{\mathrm{Cip}}}(k,m), C_{2_{\mathrm{Cip}}}(k,m), ..., C_{n_{\mathrm{Cip}}}(k,m)),$$
$$C_{i_{Cip}}(k,m) = 0,1, \quad i=1,2,...,n.$$

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

$$\rho^{OTP}_{U_KU_MEC} = U_{OTP}\left(\rho_{U_KU_MEC}\right)U^{+}_{OTP} = \tag{14}$$
$$= \Bigg(\frac{1}{|\mathcal{C}|}\sum_{C\in\mathcal{C}}\frac{1}{|\mathcal{M}|}\sum_{m\in\mathcal{M}}\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}|k\rangle_{KK}\langle k|\otimes$$
$$\otimes|m\rangle_{MM}\langle m|\otimes|C_{OTP}(k,m)\rangle_{CC}\langle C_{OTP}(k,m)|\Bigg)\otimes\rho_E,$$

здесь $|C_{OTP}(k,m)\rangle_C$ – квантовые состояния, которые аналогичны выше приведенным $|C_{\mathrm{Cip}}(k,m)\rangle_C$.

Далее, используя неравенство треугольника, находим

$$||\rho^{\mathrm{Cip}}_{KMEC} - \rho^{OTP}_{U_KU_MEC}||_1 \le ||\rho^{\mathrm{Cip}}_{KMEC} - \rho^{\mathrm{Cip}}_{U_KU_MEC}||_1 +$$
$$+||\rho^{\mathrm{Cip}}_{U_KU_MEC} - \rho^{OTP}_{U_KU_MEC}||_1 =$$
$$= ||U_{\mathrm{Cip}}\left(\rho_{KMEC} - \rho_{U_KU_MEC}\right)U^{+}_{\mathrm{Cip}}||_1 +$$
$$+ ||\rho^{\mathrm{Cip}}_{U_KU_MEC} - \rho^{OTP}_{U_KU_MEC}||_1 =$$
$$= ||\rho_{KE} - \rho_{U_KE}||_1 + ||\rho^{\mathrm{Cip}}_{U_KU_MEC} - \rho^{OTP}_{U_KU_MEC}||_1 \le$$
$$\le \varepsilon_{QKD} + +||\rho^{\mathrm{Cip}}_{U_KU_MEC} - \rho^{OTP}_{U_KU_MEC}||_1, \tag{15}$$

здесь $\rho^{\mathrm{Cip}}_{U_KU_MEC} = \rho^{\mathrm{Cip}}_{U_KU_MC}\otimes\rho_E$ – матрица плотности, отвечающая идеальной ситуации – идеальному КРК.

Далее, матрицы плотности для идеальной ситуации после зашифрования блочным шифром и одноразовым блокнотом, соответственно, имеют вид

$$\rho^{\mathrm{Cip}}_{U_MU_K\mathcal{C}} = U_{\mathrm{Cip}}\left(\rho_{U_KU_M\mathcal{C}}\right)U^{+}_{\mathrm{Cip}} =$$
$$= \frac{1}{|\mathcal{C}|}\frac{1}{|\mathcal{M}|}\frac{1}{|\mathcal{K}|}\sum_{C\in\mathcal{C}}\sum_{m_j\in\mathcal{M}}\sum_{k_i\in\mathcal{K}}|m_j\rangle_{MM}\langle m_j|\otimes$$
$$\otimes|k_i\rangle_{KK}\langle k_i|\otimes|C_{\mathrm{Cip}}(k_i,m_j)\rangle_{\mathcal{CC}}\langle C_{\mathrm{Cip}}(k_i,m_j)|. \tag{16}$$
$$\rho^{OTP}_{U_KU_M\mathcal{C}} = U_{OTP}\left(\rho_{U_KU_M\mathcal{C}}\right)U^{+}_{OTP} =$$
$$= \frac{1}{|\mathcal{C}|}\frac{1}{|\mathcal{M}|}\frac{1}{|\mathcal{K}|}\sum_{C\in\mathcal{C}}\sum_{m_j\in\mathcal{M}}\sum_{k_i\in\mathcal{K}}|m_j\rangle_{MM}\langle m_j|\otimes$$
$$\otimes|k_i\rangle_{KK}\langle k_i|\otimes|C_{OTP}(k_i,m_j)\rangle_{\mathcal{CC}}\langle C_{OTP}(k_i,m_j)|. \tag{17}$$

Здесь важно отметить, что суммирование идет по одноразовым блокнотам ближайшим к случайному блочному шифру.

Остается оценить последнее слагаемое в (15). Прямые вычисления дают

$$\frac{1}{2}||\rho^{\mathrm{Cip}}_{U_KU_M\mathcal{C}} - \rho^{OTP}_{U_KU_M\mathcal{C}}||_1 = \frac{1}{2}\frac{1}{|\mathcal{C}|}\frac{1}{|\mathcal{K}|}\frac{1}{|\mathcal{M}|}\times$$
$$\times\sum_{C\in\mathcal{C}}\sum_{k_i\in\mathcal{K}}\sum_{m_j\in\mathcal{M}}\mathrm{Tr}\{|\ |C_{\mathrm{Cip}}(k_i,m_j)\rangle_{\mathcal{CC}}\langle C_{\mathrm{Cip}}(k_i,m_j)| -$$
$$-|C_{OTP}(k_i,m_j)\rangle_{\mathcal{CC}}\langle C_{OTP}(k_i,m_j)|\ |\}. \tag{18}$$

Воспользуемся связью следового расстояния и фиделити [20], находим

$$\frac{1}{2}\mathrm{Tr}\{||\varphi\rangle\langle\varphi| - |\psi\rangle\langle\psi||\} =$$
$$= \sqrt{1-|\langle\varphi|\psi\rangle|^2} = \sqrt{1-\mathcal{F}(|\varphi\rangle,|\psi\rangle)}, \tag{19}$$
$$\frac{1}{2}||\rho^{\mathrm{Cip}}_{U_KU_M\mathcal{C}} - \rho^{OTP}_{U_KU_M\mathcal{C}}||_1 =$$

$$= \frac{1}{|\mathcal{M}|} \sum_{m_j \in \mathcal{M}} \frac{1}{|\mathcal{K}|} \sum_{k_i \in \mathcal{K}} \frac{1}{|\mathcal{C}|} \times$$

$$\times \sum_{C \in \mathcal{C}} \sqrt{1 - |_C\langle C_{\text{Cip}}(k_i, m_j)|C_{OTP}(k_i, m_j)\rangle_C|^2} =$$

$$= \frac{1}{|\mathcal{M}|} \sum_{m_j \in \mathcal{M}} \frac{1}{|\mathcal{K}|} \sum_{k_i \in \mathcal{K}} \frac{1}{|\mathcal{C}|} \times$$

$$= \sum_{C \in \mathcal{C}} \sqrt{1 - \delta_{C_{\text{Cip}}(k_i, m_j), C_{OTP}(k_i, m_j)}} =$$

$$= \frac{1}{|\mathcal{K}|} \sum_{i=2}^{L} (i-1)|\mathcal{K}_i| = \frac{1}{|\mathcal{K}|} |\mathcal{K}_\perp|. \quad (20)$$

Здесь использован факт, что среднее по всем случайным блочным шифрам не зависит от сообщения m – все столбцы выглядят одинаково (см. подпись к рис. 1).

Поясним вычисления, пусть шифруемый текст m и ключ шифрования k фиксированы. Напомним, что выбирается ближайший одноразовый блокнот к данной реализации случайного блочного шифра. Шифрование одноразовым блокнотом "накрывает" *все множество шифртекстов однократно.*

Обозначим множество ключей $\mathcal{K}_{1,\mathcal{C}}(m)$, для которых существует единственный шифртекст для случайного блочного шифра. Скалярное произведение в (20) на всех ключах из данного множества $|_C\langle C_{\text{Cip}}(k, m)|C_{OTP}(k, m)\rangle_C| = 1$, поэтому данное слагаемое не дает вклад в сумму по $k \in \mathcal{K}_{1,\mathcal{C}}(m)$.

Обозначим $\mathcal{K}_{2,\mathcal{C}}(m)$ множество *пар ключей.* Число ключей $2|\mathcal{K}_{2,\mathcal{C}}(m)|$, для которых существуют парные коллизии, имеется общий шифртекст при шифровании случайным блочным шифром для пары ключей. Выберем такую пару ключей. Совпадение шифртекстов случайного для блочного шифра и одноразового блокнота возможно только на одном из ключей пары. Скалярное произведение равно единице только на одном из ключей из пары, данное слагаемое не дает вклад в сумму. На втором ключе скалярное произведение равно нулю, вклад в сумму равен единице.

Из множества ключей $\mathcal{K}_{2,\mathcal{C}}(m)$ в сумму (18), (20) дает вклад $(2-1)|\mathcal{K}_{2,\mathcal{C}}(m)|$ слагаемых. Аналогичными рассуждениями подсчитывается число слагаемых в сумме (18), (20) с тройным, и т.д. числом коллизий. Вклад в сумму (18), (20) от множества ключей $\mathcal{K}_{i,\mathcal{C}}(m)$ дают $(i-1)|\mathcal{K}_{i,\mathcal{C}}(m)|$ слагаемых, где $\mathcal{K}_{i,\mathcal{C}}(m)$ – множество i *штук ключей*, на которых имеют место коллизии i-го порядка для случайного блочного шифра.

Число ненулевых слагаемых в (18), (20) совпадает с размером множества $|\mathcal{K}_{\perp,\mathcal{C}}(m)|$, это та часть множества, в которую не попадают шифртексты случайного блочного шифра. Размер данного множества зависит от *случайного блочного шифра и сообщения* m. Из рассуждений выше также следует, что (см. подпись к рис. 2)

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

здесь $|\mathcal{K}_{i,\mathcal{C}}(m)|$ размер множества i-х коллизий при данном сообщении m.

Размер данного множества равен числу незаполненных ящиков для конкретного случайного размещения бозонов. Среднее по всевозможным случайным размещениям – случайным блочным шифрам уже не зависит от сообщения m,

$$|\mathcal{K}_\perp| = \frac{1}{|\mathcal{C}|} \sum_{C \in \mathcal{C}} |\mathcal{K}_{\perp,\mathcal{C}}(m)| =$$

$$= \sum_{i=2}^{L} (i-1) \frac{1}{|\mathcal{C}|} \sum_{C \in \mathcal{C}} |\mathcal{K}_{i,\mathcal{C}}(m)| = \sum_{i=2}^{L} (i-1)|\mathcal{K}_i|, \quad (21)$$

где

$$|\mathcal{K}_i| = \frac{1}{|\mathcal{C}|} \sum_{C \in \mathcal{C}} |\mathcal{K}_{i,\mathcal{C}}(m)|$$

равно среднему числу пустых ящиков по всевозможным размещениям бозонов (1)–(3)

$$|\mathcal{K}_\perp| = |\mathcal{K}| \left(1 - \frac{1}{|\mathcal{K}|}\right)^{|\mathcal{K}|}. \quad (22)$$

В итоге, учитывая (22), и что $|\mathcal{K}| = 2^{256} \to \infty$, получаем оценку для расстояния между случайными блочными шифрами и соответствующими одноразовыми блокнотами,

$$\frac{1}{2} ||\rho^{\text{Cip}}_{KMEC} - \rho^{OTP}_{U_K U_M EC}||_1 \le \varepsilon_{QKD} + e^{-1} \approx 0.367, \quad (23)$$

поскольку типичные значения ε_{QKD} в системах КРК составляют $\varepsilon_{QKD} \approx 10^{-7} \div 10^{-9}$. Как было показано ранее [6], величина следового расстояния между блочным шифром и одноразовым блокнотом определяет уменьшении трудоемкости при переборе ключей, в итоге трудоемкость полного перебора 2^{256} снижается до $\approx 2^{256}(1 - \frac{1}{e})$.

Заключение. Уточним еще раз используемые приближения. *Сам случайный шифр является случайной величиной.* Расстояние между отдельным случайным шифром и одноразовым блокнотом оказывается равным числу пустых уровней при конкретной реализации случайного размещения бозонов по

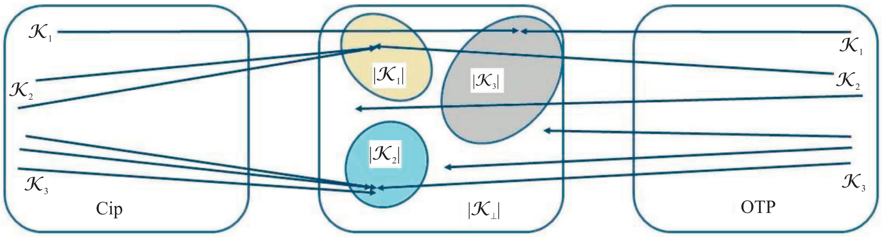

Рис. 2. (Цветной онлайн) Схематическое изображение множества ключей (слева) при шифровании блочным шифром, одноразовым блокнотом (справа), в центре – множество шифр текстов. Различным цветом показаны множества шифртекстов, на которых имеются коллизии (показаны только двойные и тройные коллизии). Белым цветом показана область шифртекстов, которые не появляются при шифровании блочным шифром

этим уровням. Таким образом, число пустых уровней для каждого размещения само является случайной величиной. Среднее расстояние – математическое ожидание числа пустых уровней по всем случайным размещениям бозонов – случайным шифрам принимает универсальное значение $\frac{1}{e}$. Невозможность аналитического и численного вычисления числа коллизий для регулярного блочного шифра фактически связана с "обработкой" экспоненциально большого множества, поэтому при получении аналитических оценок неизбежно приходится прибегать к приближениям типа ансамбля случайных блочных кодов.

Выражаем благодарность И. М. Арбекову, В. А. Кирюхину, С. П. Кулику, коллегам по Инфотекс и СФБ Лаборатории за интересные обсуждения и замечания.

Финансирование работы. Работа выполнена в рамках бюджетного финансирования организаций авторов.

Конфликт интресов. Авторы данной работы заявляют, что у них нет конфликта интересов.

---

1. C. H. Bennett and G. Brassard, *Quantum cryptography: public key distribution and coin tossing*, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (1984), p. 175.
2. Ch. Portmann and R. Renner, Rev. Mod. Phys. **94**, 025008 (2022).
3. S. N. Molotkov, Laser Phys. **34**, 045202 (2024).
4. И. М. Арбеков, С. Н. Молотков, Математические вопросы криптографии **14**(3), 9 (2023).
5. S. N. Molotkov, Laser Phys. Lett. **19**, 045201 (2022).
6. С. Н. Молотков, Письма в ЖЭТФ **117**, 470 (2023).
7. Д. Д. Сукачев, Успехи физических наук **191**(10), 1077 (1921).
8. https://www.youtube.com/watch?v=0WAuDcYhKbo.
9. G. S.Vernam, Bell Telephone Laboratories Reprint B-198, June (1926).
10. В. А. Котельников, Отчет, 19 июня (1941). Ю. В. Гуляев, Н. В. Котельникова, В. А. Котельников, Н. А. Арманд, В. Н. Сачков, С. Н. Молотков, Б. Е. Черток, *Научная сессия Отделения физических наук Российской академии наук, посвященная памяти академика Владимира Александровича Котельникова (22 февраля 2006 г.)* Успехи физических наук, **176**, 751 (2006).
11. C. E. Shannon, *A Mathematical Theory of Cryptography*, dated Sept. 1 (1945), p. 86, part III of original document; https://www.iacr.org/museum/shannon/shannon45.pdf.
12. И. М. Арбеков, С. Н. Молотков, ЖЭТФ **151**(6), 1 (2017).
13. ГОСТ Р 34.12-2015 – "'Кузнечик".
14. С. Н. Молотков, Письма в ЖЭТФ **117**, 80 (2023).
15. C. E. Shannon, 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).
16. T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley, N.Y. (1991).
17. В. Феллер, *Введение в теорию вероятностей и ее приложения*, Мир, М., (1964), т. 1, 511 с.
18. В. Ф. Колчин, Б. А. Севастьянов, В. П. Чистяков, *Случайные размещения*, Наука, М. (1976), 226 с.
19. R. Renner, arXiv:quant-ph/0512258v2 (2006).
20. M. M.Wilde, arXiv:1106.1445v6 [quant-ph] 2 Dec 2015.