Письма в ЖЭТФ, том 117, вып. 1, с. 80 – 88

Квантовый алгоритм инвариантной оценки близости классических шифров к одноразовому блокноту

С. Н. Молотков[1)]

Академия криптографии Российской Федерации, 121552 Москва, Россия

Институт физики твердого тела РАН, 42432 Черноголовка, Россия

Поступила в редакцию 5 октября 2022 г.
После переработки 10 ноября 2022 г.
Принята к публикации 17 ноября 2022 г.

Предложена инвариантная мера близости блочного шифра к совершенному (идеальному) шифру – одноразовому блокноту. Мера близости является инвариантной, не зависит от конкретной реализации одноразового блокнота – является одинаковой для любой реализации. Предложен квантовый алгоритм оценки близости блочного шифра к идеальному, в смысле предложенной меры. Квантовый алгоритм, основанный на определении собственного значения (фазы) квантового состояния, с высокой вероятностью и точностью позволяет оценить меру близости шифра к идеальному.

DOI: 10.31857/S1234567823010123, EDN: nvycqs

1. Введение. На сегодняшний день известно достаточно большое число квантовых алгоритмов для решения различных вычислительных задач и задач в криптографии [1–32]. Наиболее известными являются алгоритм Шора [2] – алгоритм разложения на простые сомножители составного числа и алгоритм Гровера [3] – алгоритм поиска в неструктурированной базе данных. Алгоритм Шора решает задачу вскрытия шифров в асимметричной криптографии.

Алгоритмы Шора и Гровера являются базовыми. Существует большое число новых задач [5–36], в которых, так или иначе используются данные базовые алгоритмы и их вариации, приспособленные для решения конкретной задачи.

Несмотря на большое разнообразие приложений квантовых алгоритмов существует базовый элемент квантовых алгоритмов, который делает их эффективными по сравнению с классическими алгоритмами.

Одним из таких общих элементов бóльшего числа квантовых алгоритмов является квантовое преобразование Фурье, которое эффективно реализуется квантовыми схемами по сравнению с классическим случаем. В классической области преобразование Фурье используется при решении огромного количества задач в различных областях.

Говоря формально, любое вычисление, классическое или квантовое, сводится вычислению некоторой содержательной булевой функции, содержательность которой определяется решаемой задачей. В квантовой области задача сводится к обратимому вычислению некоторой булевой функции. Методы вычисления могут быть общими. Если удается свести вычисление булевой функции к задаче определения периода, то задача может быть ускорена на квантовом вычислителе с использованием квантового преобразования Фурье.

Задача разложения числа на простые множители была сведена Шором к задаче нахождения периода, что позволило эффективно ее решать с помощью преобразования Фурье. Задача нахождения скрытой подгруппы [32] также может быть сведена к нахождению периода, что приводит к ее ускорению с использованием квантового преобразования Фурье. Подсчет числа элементов в некотором множестве [27, 37] также может быть сведено к нахождению периода функции, который определяется размером множества.

Нас будет интересовать задача о близости блочного шифра к совершенному шифру – одноразовому блокноту.

Близость блочного шифра к совершенному определяет стойкость ключей при их “проталкивании” по квантовым сетям [38], стойкость теоретико-информационной аутентификации ключей в квантовой криптографии [39], сложность поиска (трудоемкость поиска) ключей [40, 41], полученных в квантовой криптографии.

Близость блочного шифра к совершенному подразумевает использование некоторой меры (метри-

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

ки) близости, которая не зависит от конкретной реализации одноразового блокнота – совершенного шифра.

В работе предлагается инвариантная метрика близости, не зависящая от конкретной реализации одноразового блокнота.

Будет показано, что вычисление данных инвариантов может быть сведено к нахождению периода некоторой булевой функции, период которой определяется инвариантами шифра, что позволяет использовать квантовое преобразование Фурье, которое эффективно реализуется квантовой схемой и используется, как упоминалось выше, в различных задачах (например, [3, 5, 27, 36, 37]).

2. Определение инвариантов. Пусть задана функция двух аргументов $c(k, m)$ – алгоритм шифрования. Пусть имеется множество открытых текстов $\mathcal{M} = \{0,1\}^M$, множество ключей $\mathcal{K} = \{0,1\}^n$ и множество шифр-текстов $\mathcal{C} = \{0,1\}^M$. Алгоритм шифрования – блочный шифр $c(k, m)$ ($k \in \mathcal{K}$, $m \in \mathcal{M}$, $c \in \mathcal{C}$), реализующий отображение $\mathcal{K} \times \mathcal{M} \to \mathcal{C}$: $\{0,1\}^n \times \{0,1\}^M \to \{0,1\}^M$.

Ниже нас будет интересовать случай, когда длина сообщения равна длине ключа, такая ситуация возникает при проталкивании внешнего ключа посредством его шифрования на "квантовых ключах" в квантовых сетях.

Эталоном шифрования – идеальным шифром является шифрование в режиме одноразового блокнота. В этом случае, *для любого сообщения m при пробегании ключом шифрования k_i всего множества ключей $\mathcal{K}$, шифр-текст $c(k_i, m)$ пробегает однократно все множество шифр-текстов $\mathcal{C}$.*

Шифрование в режиме одноразового блокнота было независимо открыто Вернамом [34], Котельниковым [35] и Шенноном [36]. При таком шифровании ключ, случайная битовая строка, известная только легитимным пользователям, используется однократно и его длина в битах не менее длины открытого текста. В этом случае шифр-текст, доступный подслушивателю, который не знает ключа, является статистически независимым от открытого сообщения.

Аналогично, *для любого ключа k при пробегании сообщением m_i всего множества открытых текстов $\mathcal{M}$, шифр-текст $c(k, m_i)$ пробегает однократно все множество шифр-текстов $\mathcal{C}$.*

Для блочных шифров, функция шифрования $c(k, m)$ всегда выбирается таким образом, чтобы она не имела никакой скрытой внутренней структуры.

Одним из свойств, определяющих стойкость классических блочных шифров, является число коллизий. Под коллизией ниже понимаем следующее. Коллизия на заданном открытом тексте m, это совпадение шифр-текстов, полученных при шифровании одного и того же открытого текста на разных ключах: $c(k_1, m) = c(k_2, m)$.

Ни для одного серьезного блочного шифра число коллизий неизвестно.

Почему важно уметь оценивать число коллизий?

Отметим, сразу, что инвариант, связанный с коллизиями лишь один из восьми возможных. Именно на нем сосредоточимся, остальные вычисляются аналогично.

Пусть открытый текст задан. Коллизии в блочных шифрах неизбежно возникают из-за того, что при одном и том же открытом тексте, зашифрованным на разных ключах, шифр-текст отображается не на все множество $\mathcal{C}$, а лишь на некоторое подмножество. Сказанное поясняется рис. 1a, b.

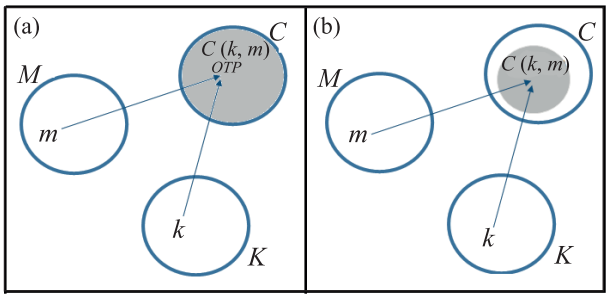

Рис. 1. (Цветной онлайн) Схематическое изображение множеств (инвариантов) шифр текстов для: (a) – любой реализации шифрования одноразовым блокнотом $C_{OTP}(k, m)$ (OTP сокращение от One Time Pad); (b) – блочным шифром $c(k, m)$

Чем больше коллизий, тем шифр является менее стойким, поскольку, например, при известной атаке известный открытый текст и шифр-текст $(m, c(k, m))$ достаточно найти не единственный ключ, а любой ключ из множества ключей, которые удовлетворяют условию $c = c(k, m)$, что уменьшает число опробований ключей.

Возможны различные меры близости блочного шифра к идеальному. Ниже за меру близости блочного шифра к идеальному выберем близость размера определенных множеств к размеру соответствующих множеств для совершенного шифра (см. детали ниже). Как известно, что одноразовый блокнот может быть реализован множеством способов, например, при помощи латинских квадратов.

При таком выборе меры близости, размеры множеств для совершенного шифра **не зависят от конкретной реализации одноразового блокнота** *– являются инвариантами. Далее для кратко-*

сти такие множества будем называть инвариантами. При таком выборе меры близости – вычислении размера множеств (инвариантов) блочного шифра не требуется аппеляция к конкретной реализации одноразового блокнота.

Все реализации одноразового блокнота являются структурно одинаковыми, поэтому размеры данных множеств являются инвариантными – не зависят от конкретной реализации одноразового блокнота.

Размеры данных множеств для одноразового блокнота являются эталонными. Для блочного шифра, чем размеры множеств ближе к соответствующим размерам множеств для одноразового блокнота, тем шифр ближе к идеальному. Далее для краткости будем называть размеры множеств инвариантами. Забегая вперед, отметим, что при вычислении квантовым алгоритмом размеров множеств для блочного шифра не требуется апелляция к одноразовому блокноту. Размеры множеств вычисляются исходя только из функции шифрования блочного шифра $c(k,m)$, а затем сравниваются размеры множеств с соответствующими эталонными инвариантами для одноразового блокнота.

Более формально, задача сводится к оценке размера следующих множеств:

$$|0,0,0| = \tag{1}$$
$$= \sum_{k_1\in\mathcal{K}}\sum_{k_2\in\mathcal{K}}\sum_{m_1\in\mathcal{M}}\sum_{m_2\in\mathcal{M}} \delta_{k_1,k_2}\delta_{m_1,m_2}\delta_{c(k_1,m_1),c(k_2,m_2)},$$

$$|0,\neq 0,0| =$$
$$= \sum_{k_1\in\mathcal{K}}\sum_{k_2\in\mathcal{K}}\sum_{m_1\in\mathcal{M}}\sum_{m_2\in\mathcal{M}} \delta_{k_1,k_2}(1-\delta_{m_1,m_2})\times$$
$$\times\,\delta_{c(k_1,m_1),c(k_2,m_2)},$$

$$|0,\neq 0,\neq 0| =$$
$$= \sum_{k_1\in\mathcal{K}}\sum_{k_2\in\mathcal{K}}\sum_{m_1\in\mathcal{M}}\sum_{m_2\in\mathcal{M}} \delta_{k_1,k_2}(1-\delta_{m_1,m_2})\times$$
$$\times\,(1-\delta_{c(k_1,m_1),c(k_2,m_2)}),$$

$$|\neq 0,0,0| =$$
$$= \sum_{k_1\in\mathcal{K}}\sum_{k_2\in\mathcal{K}}\sum_{m_1\in\mathcal{M}}\sum_{m_2\in\mathcal{M}} (1-\delta_{k_1,k_2})\times$$
$$\times\,\delta_{m_1,m_2}\delta_{c(k_1,m_1),c(k_2,m_2)},$$

$$|\neq 0,0,\neq 0| =$$
$$= \sum_{k_1\in\mathcal{K}}\sum_{k_2\in\mathcal{K}}\sum_{m_1\in\mathcal{M}}\sum_{m_2\in\mathcal{M}} (1-\delta_{k_1,k_2})\times$$
$$\times\,\delta_{m_1,m_2}(1-\delta_{c(k_1,m_1),c(k_2,m_2)}),$$

$$|\neq 0,\neq 0,0| =$$
$$= \sum_{k_1\in\mathcal{K}}\sum_{k_2\in\mathcal{K}}\sum_{m_1\in\mathcal{M}}\sum_{m_2\in\mathcal{M}} (1-\delta_{k_1,k_2})\times$$
$$\times\,(1-\delta_{m_1,m_2})\delta_{c(k_1,m_1),c(k_2,m_2)},$$

$$|\neq 0,\neq 0,\neq 0| =$$
$$= \sum_{k_1\in\mathcal{K}}\sum_{k_2\in\mathcal{K}}\sum_{m_1\in\mathcal{M}}\sum_{m_2\in\mathcal{M}} (1-\delta_{k_1,k_2})(1-\delta_{m_1,m_2})\times$$
$$\times\,(1-\delta_{c(k_1,m_1),c(k_2,m_2)}),$$

$$|0,0,\neq 0| =$$
$$= \sum_{k_1\in\mathcal{K}}\sum_{k_2\in\mathcal{K}}\sum_{m_1\in\mathcal{M}}\sum_{m_2\in\mathcal{M}} \delta_{k_1,k_2}\delta_{m_1,m_2}\times$$
$$\times\,(1-\delta_{c(k_1,m_1),c(k_2,m_2)}).$$

Здесь введены обозначения, $|i,j,k|$ – размер множества $(i,j,k = 0,\neq 0)$, индексы $i = 0/\neq 0$ означают, что ключи шифрования равны/не равны $(k_1 = k_2/k_1 \neq k_2)$, $j = 0/\neq 0$ – открытые тексты $(m_1 = m_2/m_1 \neq m_2)$ совпадают/не совпадают, индекс $k = 0/\neq 0$ – шифр-тексты $c_1 = c(k_1,m_1) = c_2(k_2,m_2)/c_1 = c(k_1,m_1) \neq c_2 = c(k_2,m_2)$ совпадают/не совпадают.

Для шифров размеры некоторых множеств тождественно равны нулю: $|0,\neq 0,0| \equiv 0$, так как открытые тексты зашифрованные на одном и том же ключе имеют разные шифр-тексты – условие однозначного расшифрования; $|0,0,\neq 0| \equiv 0$, так как одинаковые открытые тексты, зашифрованные на одном и том же ключе не могут иметь разные шифр-тексты.

3. Постановка задачи. Любой квантовый алгоритм состоит из трех стадий: приготовление входного состояния, специально подобранная унитарная эволюция (собственно "вычисление"), получение результата вычисления – измерение квантового состояния. Измерение результата носит вероятностный характер.

Для вычисления каждого инварианта используется свой алгоритм. Все алгоритмы однотипны. каждый алгоритм дает оценку следующих вероятностей,

$$\begin{gathered}\Pr\{0,0,0\},\quad \Pr\{0,\neq 0,0\},\\ \Pr\{0,\neq 0,\neq 0\},\quad \Pr\{\neq 0,0,0\},\\ \Pr\{\neq 0,\neq 0,0\},\quad \Pr\{\neq 0,\neq 0,0\},\\ \Pr\{\neq 0,\neq 0,\neq 0\},\quad \Pr\{0,0,\neq 0\},\end{gathered} \tag{2}$$

которые с точностью до множителя $|\mathcal{K}||\mathcal{M}|$ равны размерам множеств (1).

Поскольку алгоритмы однотипны, то проведем рассмотрение оценки размера множества, например,

$|\neq 000|$. Для одноразового блокнота данный инвариант равен 0, поскольку одно и то же сообщение m, зашифрованное на разных ключах, не может иметь совпадающих шифр-текстов. Для блочных шифров возможны коллизии, т.е. размер $|\neq 000|$ не будет равен 0. Чем больше уклонение от 0, тем блочный шифр будет хуже – дальше от одноразового блокнота.

Прямое вычисление инвариантов (1) на классическом вычислителе представляет собой переборную задачу.

Квантовый алгоритм оценивает инварианты не напрямую, а через оценку фазы квантового состояния.

Алгоритм состоит из следующих шагов.

1) Приготовление входного состояния, представляющего собой две копии суперпозиций всех состояний ключей и открытых сообщений.

2) Вычисление двух независимых копий функций шифрования для суперпозиции состояний ключей и сообщений.

3) Выделение унитарным преобразованием внутри суперпозиции компонент, отвечающих вычисляемому инварианту.

4) Фазовое унитарное преобразование состояния.

5) Вычисление квантового преобразования Фурье от состояния.

6) Измерение состояния – получение оценки инварианта.

7) Оценка точности вычисляемого инварианта.

4. Описание алгоритма.

1) Приготовление входного состояния. Входным состоянием являются две независимые копии состояний, являющиеся произведением двух состояний – первое состояние суперпозиция всех ключей, второе – суперпозиция всех открытых сообщений,

$$(k_1,k_2,...,k_n)\to\frac{1}{\sqrt{|\mathcal{K}|}}\sum_{k\in\mathcal{K}}|\overline{k}\rangle=$$
$$=\sum_{k\in\mathcal{K}}|k_1\rangle\otimes|k_2\rangle\otimes...\otimes|k_n\rangle,$$
$$k_i=0,1,\quad i=1,...,n,\quad |\mathcal{K}|=2^n, \tag{3}$$

$$(m_1,m_2,...,m_M)\to\frac{1}{\sqrt{|\mathcal{M}|}}\sum_{m\in\mathcal{M}}|\overline{m}\rangle=$$
$$=\sum_{m\in\mathcal{M}}|m_1\rangle\otimes|m_2\rangle\otimes...\otimes|m_n\rangle,$$
$$m_i=0,1,\quad i=1,...,M,\quad |\mathcal{M}|=2^M. \tag{4}$$

Для блочного шифра длина сообщения может отличаться от длины ключа и обычно больше. В квантовых сетях при продвижении внешнего ключа через сегменты сети с квантовым распределением ключей возникает необходимость шифрования внешнего ключа на "квантовых" ключах на отдельных сегментах сети [37]. В этом случае длина сообщения – внешнего ключа равна длине ключа шифрования. При шифровании одноразовым блокнотом сохраняется так называемая "составная секретность" продвигаемого ключа [37].

Имея ввиду упомянутую задачу, ниже считаем, что длина открытого текста совпадает с длиной ключа, соответственно, $|\mathcal{M}|=|\mathcal{K}|$ $(M=n)$. Общий случай требует несколько большего места и будет рассмотрен отдельно.

Состояния приготавливаются посредством поворота Адамара H регистра состояний из n кубитов, находящихся изначально в состоянии 0,

$$|0\rangle_K^{\otimes n}\to H^{\otimes}|0\rangle_K^{\otimes n}=\left(\frac{|0\rangle_K+|1\rangle_K}{\sqrt{2}}\right)^{\otimes n},$$

$$|0\rangle_M^{\otimes M}\to H^{\otimes}|0\rangle_M^{\otimes M}=\left(\frac{|0\rangle_M+|1\rangle_M}{\sqrt{2}}\right)^{\otimes M}. \tag{5}$$

Далее приготавливается еще одна копия состояний (3), (4). Окончательно входное состояние для алгоритма принимает вид

$$|\Psi_1\rangle=\frac{1}{\sqrt{|\mathcal{N}|}}\sum_{k_1,k_2\in\mathcal{K}}\sum_{m_1,m_2\in\mathcal{M}}|\overline{k}_1,\overline{k}_2\,\overline{m}_1,\overline{m}_2\rangle, \tag{6}$$

$$|\overline{k}_1,\overline{k}_2\,\overline{m}_1,\overline{m}_2\rangle=|\overline{k}_1\rangle\otimes|\overline{k}_2\rangle\otimes|\overline{m}_1\rangle\otimes|\overline{m}_2\rangle,$$
$$\sqrt{|\mathcal{N}|}=|\mathcal{K}||\mathcal{M}|$$

2) Вычисление функции шифрования для блочного шифра. Зашифрование реализуется при помощи операторов U_{C_1} и U_{C_2}[2)], которые реализуются квантовой схемой. Схемы получают входные квантовые состояния ключей и открытых текстов, на выходе

[2)] Для унитарной реализации функции шифрования требуются дополнительные "мусорные" кубиты, которые изначально находятся в состоянии 0, *после вычисления функции опять возвращаются в исходное нулевое состояние* (см. детали общего метода очистки мусорных кубитов в [32]). По этой причине данные вспомогательные кубиты из экономии места далее опускаем. Число вспомогательных кубитов зависит от используемой функции шифрования. Оценки для ряда шифров различаются, разные оценки показывают, что число вспомогательных кубитов при одном обращении к квантовой схеме, реализующей шифрование, полиномиально по длине ключа n [12]. При длине сообщения больше длины ключа, сообщения шифруются блоками. Пусть число блоков N_c, при этом число обращений к квантовой схеме также будет N_c, т.е. линейно по числу блоков, при этом число вспомогательных кубитов не растет с числом блоков – длины сообщения, поскольку вспомогательные кубиты после каждого обращения "обнуляются" и используются повторно.

возникает зашифрованное сообщение, которое записывается в два дополнительных регистра $|0\rangle_{C_1}^{\otimes M}$ и $|0\rangle_{C_2}^{\otimes M}$ из M кубитов, находящихся изначально в нулевом состоянии. В итоге возникает новое квантовое состояние

$$|\Psi_2\rangle = (U_{C_1}\otimes U_{C_2})(|\Psi_1\rangle\otimes|0\rangle_{C_1}\otimes|0\rangle_{C_1}) = \\ = \frac{1}{\sqrt{|\mathcal{N}|}}\sum_{k_1,k_2\in\mathcal{K}}\sum_{m_1,m_2\in\mathcal{M}}|\overline{k}_1,\overline{k}_2\,\overline{m}_1,\overline{m}_2,\overline{c}_1,\overline{c}_2\rangle, \quad (7)$$

$$|\overline{k}_1,\overline{k}_2\,\overline{m}_1,\overline{m}_2,\overline{c}_1,\overline{c}_2\rangle = |\overline{k}_1,\overline{k}_2\,\overline{m}_1,\overline{m}_2\rangle\otimes|\overline{c}_1,\overline{c}_2\rangle,$$

$$|\overline{c}_1,\overline{c}_2\rangle = (|c(k_{1_1},m_{1_1})\rangle\otimes\ldots\otimes|c(k_{1_n},m_{1_M})\rangle)\otimes \\ \otimes(|c(k_{2_1},m_{2_1})\rangle\otimes\ldots\otimes|c(k_{2_n},m_{2_M})\rangle).$$

3) Выделение унитарным преобразованием внутри суперпозиции компонент, отвечающих вычисляемому инварианту. Для определенности вычисления проводятся для инварианта $|\neq 000|$. Вычисления для остальных проводятся аналогично. Для вычисления требуется выделить в суперпозиции состояний в (7) две компоненты. Первая компонента содержит состояния с неравными ключами $k_1\neq k_2$, равными сообщениями $m_1=m_2$ и равными шифр-текстами $c(k_1,m_1)=c(k_2,m_2)$. Вторая компонента в суперпозиции содержит все остальные компоненты.

Такое выделение должно быть сделано при помощи унитарного преобразования, при таком выделении никакой информации получить нельзя – состояние не "портится".

Идея выделения состоит в использовании булевой функции

$$\mathcal{F}(\overline{k}_1,\overline{k}_2,\overline{m}_1,\overline{m}_2,\overline{c}_1,\overline{c}_2) = \\ = \begin{cases} 1, & \overline{k}_1\neq\overline{k}_2, \quad \overline{m}_1=\overline{m}_2, \quad \overline{c}_1=\overline{c}_2, \\ 0, & \text{для других значений аргументов.}\end{cases} \quad (8)$$

В зависимости от того, какой инвариант нужно вычислить, выбирается соответствующая булева функция – функция, которая имеет значение 1 на выбранном множестве аргументов, отвечающих инварианту, и равная 0 при остальных значениях аргументов.

Вычислимая булевая функция может быть реализована обратимым образом – унитарным преобразованием с использованием вспомогательных "мусорных" состояний, которые изначально находятся в нулевом состоянии $|0\rangle_G$, и после преобразования возвращаются в исходное состояние (см. детали обратимой реализации булевых функций в [36]). Значение булевой функции записывается в регистр $|0\rangle_{\mathcal{F}}$ Унитарный оператор обозначим $U_{\mathcal{F}}$.

$$|\Psi_3\rangle = U_{\mathcal{F}}(|\Psi_2\rangle\otimes|0\rangle_{\mathcal{F}}\otimes|0\rangle_G) = \quad (9)$$

$$= \frac{1}{\sqrt{|\mathcal{N}|}}\left(\sum_{k_1,k_2\in\mathcal{K}}\sum_{m_1,m_2\in\mathcal{M}}(1-\delta_{\overline{k}_1,\overline{k}_2})\delta_{\overline{m}_1,\overline{m}_2}\delta_{\overline{c}_1,\overline{c}_1}|\overline{k}_1,\overline{k}_2,\overline{m}_1,\overline{m}_2,\overline{c}_1,\overline{c}_2\rangle\right)\otimes|1\rangle_{\mathcal{F}}\otimes|0\rangle_G + \\ + \frac{1}{\sqrt{|\mathcal{N}|}}\left(\sum_{k_1,k_2\in\mathcal{K}}\sum_{m_1,m_2\in\mathcal{M}}[1-(1-\delta_{\overline{k}_1,\overline{k}_2})\delta_{\overline{m}_1,\overline{m}_2}\delta_{\overline{c}_1,\overline{c}_1}]|\overline{k}_1,\overline{k}_2,\overline{m}_1,\overline{m}_2,\overline{c}_1,\overline{c}_2\rangle\right)\otimes|0\rangle_{\mathcal{F}}\otimes|0\rangle_G.$$

В первом слагаемом в сумме фигурируют значения аргументов $(\overline{k}_1,\overline{k}_2,\overline{m}_1,\overline{m}_2,\overline{c}_1,\overline{c}_2)$ такие, что $\mathcal{F}(\overline{k}_1,\overline{k}_2,\overline{m}_1,\overline{m}_2,\overline{c}_1,\overline{c}_2)=1$. Во втором слагаемом в сумме фигурируют значения аргументов такие, что $\mathcal{F}(\overline{k}_1,\overline{k}_2,\overline{m}_1,\overline{m}_2,\overline{c}_1,\overline{c}_2)=0$.

Заметим, что квадрат модуля амплитуды первого слагаемого как раз равен $\Pr\{\neq 000\}$ (см. (2)).

Для дальнейшего удобно записать состояние (9) в более кратком и удобном виде, вводя нормированные состояния,

$$|\Psi_3\rangle = \sin(\theta)|OK,1\rangle + \cos(\theta)|\neq OK,0\rangle, \quad (10)$$

$$|OK,1\rangle = \frac{1}{\sqrt{\Pr\{\neq 000\}}}\left(\sum_{k_1,k_2\in\mathcal{K}}\sum_{m_1,m_2\in\mathcal{M}}(1-\delta_{\overline{k}_1,\overline{k}_2})\delta_{\overline{m}_1,\overline{m}_2}\delta_{\overline{c}_1,\overline{c}_1}|\overline{k}_1,\overline{k}_2,\overline{m}_1,\overline{m}_2,\overline{c}_1,\overline{c}_2\rangle\right)\otimes|1\rangle_{\mathcal{F}}\otimes|0\rangle_G, \quad (11)$$

$$|\neq OK,0\rangle = \frac{1}{\sqrt{1-\Pr\{\neq 000\}}}\left(\sum_{k_1,k_2\in\mathcal{K}}\sum_{m_1,m_2\in\mathcal{M}}[1-(1-\delta_{\overline{k}_1,\overline{k}_2})\delta_{\overline{m}_1,\overline{m}_2}\delta_{\overline{c}_1,\overline{c}_1}]|\overline{k}_1,\overline{k}_2,\overline{m}_1,\overline{m}_2,\overline{c}_1,\overline{c}_2\rangle\right)\otimes|0\rangle_{\mathcal{F}}\otimes|0\rangle_G, \quad (12)$$

$$\sin^2(\theta) = \Pr\{\neq 000\} = \frac{|\neq 000|}{|\mathcal{N}|}.$$

Квадрат амплитуды, интересующего нас состояния, $\sin^2(\theta)$ напрямую связан с инвариантом. Сама фаза θ неизвестна. Дальнейшая задача будет состоять в оценке фазы θ.

4) Фазовое унитарное преобразование состояния – оценка фазы состояния. Первое преобразование состоит в изменении знака в состоянии (10) перед компонентой $|OK,1\rangle$. Изменение фазы производится унитарным оператором $U_\pi = \sigma_Z$ – оператором Паули, который действует только на состояния $|1\rangle_{\mathcal{F}}, |0\rangle_{\mathcal{F}}$, на остальные – действие тождественное, имеем

$$|\Psi_4\rangle = U_\pi|\Psi_3\rangle = -\sin(\theta)|OK,1\rangle + \cos(\theta)|\neq OK,0\rangle. \tag{13}$$

Все преобразования происходят в пространстве, натянутом на ортогональные базисные векторы $\{|OK,1\rangle, |\neq OK,0\rangle\}$. Далее удобно ввести другие ортогональные базисные векторы $\{|\Psi\rangle, |\Psi^\perp\rangle\}$ ($|\Psi\rangle$ – исходное состояние), которые связаны с предыдущими векторами соотношением

$$\begin{aligned} |\Psi\rangle &= \sin(\theta)|OK,1\rangle + \cos(\theta)|\neq OK,0\rangle, \\ |\Psi^\perp\rangle &= \cos(\theta)|OK,1\rangle - \sin(\theta)|\neq OK,0\rangle. \end{aligned} \tag{14}$$

С учетом (10), (14) состояние $|\Psi_4\rangle$ в (13) после изменения знака фазы представляется как

$$|\Psi_4\rangle = \cos(2\theta)|\Psi\rangle - \sin(2\theta)|\Psi^\perp\rangle. \tag{15}$$

Следующее преобразование – отражение состояния $|\psi_4\rangle$ относительно среднего, как в алгоритме Гровера. Преобразование реализуется унитарным оператором $U_\perp = (2|\Psi\rangle\langle\Psi| - I)$ (I – единичный оператор в пространстве, натянутом на базисные векторы $\{|\Psi\rangle, |\Psi^\perp\rangle\}$), получаем

$$\begin{aligned} U_\perp|\Psi_4\rangle &= (2|\Psi\rangle\langle\Psi| - I)(\cos(2\theta)|\Psi\rangle - \sin(2\theta)|\Psi^\perp\rangle) = \\ &= \cos(2\theta)|\Psi\rangle - \sin(2\theta)|\Psi^\perp\rangle = \\ &= \sin(3\theta)|OK,1\rangle + \cos(3\theta)|\neq OK,0\rangle. \end{aligned} \tag{16}$$

Отметим, что значение фазы θ неизвестно при всех преобразованиях выше – квантовое состояние не "портится".

Введем обозначение $Q = U_\perp U_\pi$. Далее, с учетом (13)–(16), находим

$$\begin{aligned} Q^k(\sin(\theta)|OK,1\rangle + \cos(\theta)|\neq OK,0\rangle) = \\ = \sin[(2k+1)\theta]|OK,1\rangle + \cos([(2k+1)\theta]\theta)|\neq OK,0\rangle. \end{aligned} \tag{17}$$

Исходное состояние (10) ($|\Psi\rangle = \sin(\theta)|OK,1\rangle + \cos(\theta)|\neq OK,0\rangle$) до фазовых преобразований удобно записать через собственные состояния $|\Psi_\pm\rangle$ оператора Q с собственными числами $e^{\pm i2\theta}$,

$$\begin{aligned} |\Psi_-\rangle &= \frac{1}{\sqrt{2}}\left(|OK,1\rangle + i|OK,0\rangle\right), \\ |\Psi_+\rangle &= \frac{1}{\sqrt{2}}\left(|OK,1\rangle - i|OK,0\rangle\right), \end{aligned} \tag{18}$$

с учетом (10)–(16) находим

$$|\Psi\rangle = \frac{e^{i\theta}}{\sqrt{2}}|\Psi_+\rangle + \frac{e^{-i\theta}}{\sqrt{2}}|\Psi_-\rangle, \tag{19}$$

$$Q|\Psi_\pm\rangle = e^{\pm i2\theta}|\Psi_\pm\rangle. \tag{20}$$

5) Вычисление квантового преобразования Фурье от состояния. Следующий шаг квантового алгоритма состоит в реализации квантового преобразования Фурье от состояния (17). Для этого вводится дополнительный вспомогательный регистр из L кубитов, находящихся в однородной суперпозиции всех состояний, аналогичный суперпозиции (3), (4),

$$|\overline{\ell}\rangle = \frac{1}{\sqrt{|\mathcal{L}|}}\sum_{\ell\in\mathcal{L}}|\ell\rangle, \quad \ell = (\ell_1,\ell_2,...,\ell_L),$$

$$\ell_i = 0,1, \quad i = 1,...,L, \quad |\mathcal{L}| = 2^L.$$

Длина регистра L будет определять точность оценки инварианта.

Введем, следуя [27] (см. также [32]), унитарный оператор $\Lambda(Q)$, действие которого на вспомогательный регистр и наше состояние (19), определим как

$$\Lambda(Q)(|\ell\rangle\otimes|\Psi\rangle) = |\ell\rangle\otimes Q^\ell|\Psi\rangle. \tag{21}$$

Для собственных функций (18) действие оператора сводится к

$$\Lambda(Q)(|\ell\rangle\otimes|\Psi_\pm\rangle) = e^{\pm i2\theta\ell}(|\ell\rangle\otimes|\Psi_\pm\rangle), \tag{22}$$

в формуле (22) в показателе экспоненты l равно целому числу, отвечающему бинарному представлению строки $\ell = (\ell_1,...,\ell_L)$.

С учетом (18)–(22) находим

$$\begin{aligned} \Lambda(Q)(|\overline{\ell}\rangle\otimes|\Psi\rangle) = \\ = \frac{1}{\sqrt{|\mathcal{L}|}}\sum_{\ell\in\mathcal{L}}|\ell\rangle\left(e^{i2\theta\ell}\frac{e^{i\theta}}{\sqrt{2}}|\Psi_+\rangle + e^{-i2\theta\ell}\frac{e^{-i\theta}}{\sqrt{2}}|\Psi_-\rangle\right). \end{aligned} \tag{23}$$

Здесь, как и выше, ℓ в экспоненте – целое число, угол θ – вещественное число.

Как видно из (23), оператор $\Lambda(Q)$ выполняет условное (управляемое) квантовое преобразование Фурье, которое реализуется полиномиальными ресурсами (см. детали, например, в [32]).

Состояния $|\Psi_{\pm}\rangle$ "отвязаны" от регистра ℓ.

Далее выполняется обратное квантовое преобразованием Фурье (QFT^{-1}) над вспомогательным регистром. Имеем

$$\frac{1}{\sqrt{|\mathcal{L}|}}\sum_{n\in\mathcal{L}}\varphi_n^{\pm}|n\rangle = QFT^{-1}\left(\frac{1}{\sqrt{|\mathcal{L}|}}\sum_{\ell\in\mathcal{L}}\varphi_\ell^{\pm}|\ell\rangle\right) = \\ = QFT^{-1}\left(\frac{1}{\sqrt{|\mathcal{L}|}}\sum_{\ell\in\mathcal{L}}e^{\pm i2\theta\ell}|\ell\rangle\right), \qquad (24)$$

где $\varphi_\ell^{\pm} = e^{\pm i2\theta\ell}$ и $\varphi_n^{\pm}$ – амплитуды состояний в базисе $\{|\ell\rangle\}$ и базисе $\{|n\rangle\}$ после преобразования Фурье, $n = (n_1, ..., n_L)$. Амплитуды $\varphi_n^{\pm}$ состояния в базисе $\{n\rangle\}$ после фурье-преобразования имеют вид

$$\varphi_n^{\pm} = \frac{1}{\sqrt{|\mathcal{L}|}}\sum_{\ell\in\mathcal{L}}\varphi_\ell^{\pm}\exp\left(i\frac{2\pi\ell n}{|\mathcal{L}|}\right) = \\ = \frac{1}{\sqrt{|\mathcal{L}|}}\sum_{\ell\in\mathcal{L}}\exp\left(i\left(\frac{2\pi n}{|\mathcal{L}|}\pm 2\theta\right)\ell\right), \qquad (25)$$

здесь так же, как и в (22) n, ℓ в показателе экспоненты – целые числа, отвечающие бинарному представлению состояния $|n\rangle$, $|\ell\rangle$.

Отметим, что все предыдущие преобразования являются унитарными – не "портят" состояния и не требуют знания угла θ (соответственно, инварианта, см. формулы (1), (2)).

6) Измерение состояния – получение оценки инварианта. На заключительном этапе работы алгоритма производятся измерения в базисе $\{|n\rangle\}$. Вероятность результата измерения равна квадрату модуля амплитуды $|\varphi_n^{\pm}|^2$ в (25).

Результатом измерения в базисе $\{|n\rangle\}$ является бинарное представление целого числа n. Данное число входит в оценку угла θ.

На уровне физической интуиции ясно, что максимальная вероятность результата измерения возникает для тех фурье-компонент, у которых показатель экспоненты близок к нулю, при этом квадрат модуля амплитуды и вероятность соответствующего исхода n, близки к единице. Таким образом, для оценки фазы получаем

$$\frac{2\pi n}{|\mathcal{L}|}\approx 2\theta, \quad \theta\approx\frac{\pi n}{|\mathcal{L}|}. \qquad (26)$$

Оценка угла дает оценку инварианта, с учетом (12), находим

$$|\neq 000|\approx\sin^2\left(\frac{\pi n}{|\mathcal{L}|}\right)|\mathcal{N}|. \qquad (27)$$

7) Оценка точности инварианта. Фаза θ является вещественным числом, которое аппроксимируется конечным набором значений n $0\le\frac{\pi n}{|\mathcal{L}|}\le 1$. Имеются две неточности в определении инварианта. Первая, связана с конечной разрядной сеткой n. Вторая неточность связана с тем, что результат измерения n является случайной величиной, распределенной в окрестности значения $\frac{\theta|\mathcal{L}|}{\pi}$. Иначе говоря, в каждом прогоне алгоритма возникает оценка θ, диктуемая распределением n – квадратом модуля фурье-компонент в (25).

Определение точности – близости оценки параметра к истинному значению является задачей математической статистики. Здесь можно воспользоваться оценками точности, приведенными в работе [27].

Средняя ошибка зависит от числа прогонов (испытаний) алгоритма. При каждом прогоне используется два обращения к квантовой схеме, реализующей шифрование и одно обращение к квантовой схеме для булевой функции.

Применительно к нашему случаю, согласно [27] для точности определения параметра θ при числе испытаний (прогонов) $O(\sqrt{|\mathcal{N}|})$ (соответственно, $O(\sqrt{|\mathcal{N}|})$ обращений к функции шифрования и булевой функции), длине разрядной сетки $L = \log(|\mathcal{L}|) = \log(|\mathcal{N}|)$ вероятность получить оценку значения $\overline{|\neq 000|}$, которая находится в пределах нескольких квадратичных уклонений от точного значения $|\neq 000|$, не менее

$$\Pr\{||\neq 000| - \overline{|\neq 000|}| < 2\pi\sqrt{|\neq 000|}\} > \frac{8}{\pi^2}. \qquad (28)$$

5. Заключение. Предложен новый подход к определению близости блочного шифра к совершенному шифру – одноразовому блокноту. Предложенная мера близости является инвариантной – не зависит от конкретной реализации одноразового блокнота.

Квантовый алгоритм, основанный на определении собственного значения (фазы) квантового состояния, с высокой вероятностью и точностью позволяет оценить инварианты за $O(\sqrt{|\mathcal{N}|})$ прогонов алгоритма. Отметим, что эталонные инварианты для одноразового блокнота, с которыми производится сравнение инвариантов для блочного шифра, также могут быть вычислены квантовым алгоритмом.

В классическом случае определение близости является переборной задачей, но имеет существенные отличия от задачи поиска определенного значения, например, ключа.

Необходимые вычислительные ресурсы для вычисления инвариантов зависят от наличия большой памяти.

Если большая память масштаба $O(|\mathcal{N}|)$ отсутствует, а имеется только небольшая память для записи текущего результата – текущего значения ключа, сообщения и шифр-текста, то для сравнения

шифр-текстов требуется $O(|\mathcal{N}|^2)$ обращений к функции шифрования и сравнений. Действительно, всего пар $c(k,m)$ имеется $|\mathcal{N}|$. Берется первая пара из $|\mathcal{N}|$, вычисляется $c(k,m)$. Затем вычисляется значение $c(k,m)$ для одной из оставшихся из $|\mathcal{N}|-1$ пар и значения сравниваются. Далее, поскольку большая память отсутствует, вычисляется $c(k,m)$ для следующей пары из $|\mathcal{N}|-2$ оставшихся, значения сравниваются, т.д. Данная процедура, вычисления "на ходу" значений $c(k,m)$ и сравнения, требует $|\mathcal{N}|-1+|\mathcal{N}|-2+|\mathcal{N}|-3+...+|\mathcal{N}|-(|\mathcal{N}|-1) \approx O(|\mathcal{N}|^2)$ вызовов функции шифрования и вызовов функции сравнения (булевой функции), т.е. сложность $O(|\mathcal{N}|)^2$.

Если имеется память размера $O(|\mathcal{N}|)$ то, можно за $O(|\mathcal{N}|)$ обращений к функции шифрования вычислить все значения $c(k,m)$ и записать их в таблицу для дальнейшего просмотра и сравнения шифр-текстов при разных (k,m). В наихудшем варианте требуется $O(|\mathcal{N}|)^2$ сравнений в таблице. При этом число обращений к функции шифрования будет $O(|\mathcal{N}|)$, но при этом требуется большая память размера $O(|\mathcal{N}|)$.

Таким образом, сложность сильно зависит от наличия памяти, и имеет разную структуру вычислительных ресурсов: "нулевая память" (небольшая рабочая память, большая память (память достаточная для записи всех значений $c(k,m)$). При любой промежуточной памяти ответ не известен.

В квантовом случае требуется $O(\sqrt{|\mathcal{N}|})$ прогонов алгоритма – обращений к функции шифрования и сравнения для вычисления инварианта с достаточной точностью и высокой вероятностью (см. формулу (28)).

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

1. D. Deutsch and R.Jozsa, Proceedings of the Royal Society of London, Series A: Mathematical and Physical Sciences **439**(1907), 553 (1992).
2. P. W. Shor, SIAM J. Comput. **26**(5), 1484 (1997).
3. L. K.Grover, *A fast quantum mechanical algorithm for database search*, Proceedings of the twenty-eighth annual ACM symposium on Theory of computing – STOC '96. ACM Press, N. Y., USA (1996), p. 212.
4. D. R. Simon, SIAM J. Comput. **26**(5), 1474 (1997).
5. M. Kaplan, G. Leurent, A. Leverrier, and M. Naya–Plasencia, arXiv:1602.05973 [quan-ph], (2016).
6. A. Ambainis, *Quantum Walk Algorithm for Element Distinctness*, 45th Annual IEEE Symposium on Foundations of Computer Science. IEEE (2014), p. 22; https://ieeexplore.ieee.org/document/1366221.
7. A. W. Harrow, A. Hassidim, and S. Lloyd, Phys. Rev. Lett. **103**(15), 150502 (2009).
8. D. Dervovic, M. Herbster, P. Mountney, S. Severini, N. Usher1, and L. Wossnig, arXiv:0311001 [quant-ph], (2014).
9. M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwand, arXiv:1512.04965 [quant-ph] (2015).
10. M. Almazrooie, A. Samsudin, R. Abdullah, and K. N. Mutter, SpringerPlus **5**(1), 1494 (2016).
11. M. Almazrooie, A. Samsudin, R. Abdullah, and K. N. Mutter, *Quantum Grover Attack on the Simplified-AES*, Proceedings of the 2018 7th International Conference on Software and Computer Applications, ACM, N.Y., NY, USA (2018), p. 204.
12. Д. В. Денисенко, Г. Б. Маршалко, М. В. Никитенкова, В. И. Рудской, В. А. Шишкин, ЖЭТФ **155**, 645 (2019).
13. V. Gheorghiu and M.Mosca, *A resource estimation framework for quantum attacks against cryptographic functions – recent developments*, (2021); https://globalriskinstitute.org.
14. M. Piani and M. Mosca, *Quantum threat timeline report*, (2020); https://globalriskinstitute.org.
15. M.Piani, M.Mosca, *Quantum threat timeline report* (2019); https://globalriskinstitute.org.
16. V. Gheorghiu and M.Mosca, *A resource estimation framework for quantum attacks against cryptographic functions*, Global Risk Institute quantum risk assessment report (2020); https://globalriskinstitute.org.
17. V. Gheorghiu and M. Mosca, *A resource estimation framework for quantum attacks against cryptographic functions*, part 4, Global Risk Institute quantum risk assessment report (2018); https://globalriskinstitute.org.
18. V. Gheorghiu and M. Mosca, *A resource estimation framework for quantum attacks against cryptographic functions*, part 3, Global Risk Institute quantum risk assessment report (2018); https://globalriskinstitute.org.
19. V. Gheorghiu and M.Mosca, *A resource estimation framework for quantum attacks against cryptographic functions*, part 2, Global Risk Institute quantum risk assessment report (2018); https://globalriskinstitute.org.
20. V. Gheorghiu and M.Mosca, *A resource estimation framework for quantum attacks against cryptographic functions*, part 1, Global Risk Institute quantum risk assessment report (2017); https://globalriskinstitute.org.
21. Y.-A. Chen and X.-S. Gao, arXiv:1712.06239 [quant-ph] (2018).
22. A. Ambainis, arXiv:1010.4458 [quant-ph] (2010).

23. A. M. Childs, R. Kothari, and R. D. Somma, SIAM Journal on Computing. **46**(6), 1920 (2017).
24. L. Wossnig, Z. Zhao, and A. Prakash, Phys. Rev. Lett. **120**(5), 050502 (2018).
25. G. Brassard, P. Hoyer, and A. Tapp, ACM SIGACT News **28**(2), 14 (1997).
26. A. Chailloux, M. Naya-Plasencia, and A. Schrottenloher, *An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography*, preprint (2017); https://eprint.iacr.org/2017/847.
27. G. Brassard, P. Hoyer, and A. Tapp, arXiv:0005055 [quant-ph] (2000).
28. T. Häner and M. Soeken, arXiv:2006.03845 [quant-ph] (2020).
29. M. Roetteler and R. Steinwandt, Inf. Process. Lett. **115**(1), 40 (2015).
30. A. Hosoyamada and E. Aoki, *On Quantum Related-Key Attacks on Iterated Even-Mansour Ciphers*, ed. by S. Obana and K. Chida, Springer International Publishing AG, WSEC 2017, LNCS 10418, Springer Nature Switzerland AG, Geneva (2017)p. 3; https://link.springer.com/chapter/10.1007/978-3-319-64200-0_1.
31. X.Bonnetain, M. Naya-Plasencia, and A. Schrottenloher, *On Quantum Slide Attacks*, preprint (2018); https://eprint.iacr.org/2018/1067.pdf.
32. А. Китаев, А. Шень, М. Вялый, *Классические и квантовые вычисления*, МЦНМО-ЧеРо, М. (1999), 192 с.
33. G. Leander and A.May, *Grover Meets Simon – Quantumly Attacking the FX-construction*, Advances in Cryptology ? ASIACRYPT 2017 23rd International Conference on the Theory and Applications of Cryptology and Information Security Hong Kong, China, December 3–7, 2017 Proceedings, Part II, Springer (2017).
34. G. S. Vernam, Journal of the IEEE **55**, 109 (1926).
35. В. А. Котельников, Отчет (19 Июня, 1941); https://cryptography-museum.ru.
36. 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); https://www.iacr.org > shannon > shannon45.
37. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th Anniversary Edition, Cambridge University Press, Cambridge, N.Y., Melbourne, Madrid, Cape Town, Singapore, Sao Paulo, Delhi, Dubai, Tokyo, Mexico City (2010).
38. S. N. Molotkov, Laser Phys. Lett. **19**, 045201 (2022).
39. S. N. Molotkov, Laser Phys. Lett. **19**, 075203 (2022).
40. И. М. Арбеков, С. Н. Молотков, ЖЭТФ **152**, 62 (2017).
41. С. Н. Молотков, Письма в ЖЭТФ **103**, 389 (2016).