Квантовый алгоритм Саймона и его применение в задачах криптоанализа

Денисенко Д.В.

25 марта 2021

Структура доклада

1. Квантовый алгоритм Саймона.
2. Применение квантового алгоритма Саймона к схеме Эвена-Мансура.
3. О применении алгоритма Саймона к другим криптосхемам.

Модели Q1 и Q2 квантовых вычислений [1, 2, 3, 21]

Q1

Standard security: a block cipher is standard secure against quantum adversaries if no efficient quantum algorithm can distinguish the block cipher from PRP (or a PRF) by making only classical queries.

Quantum circuit for classical values.
Example: breaking RSA with Shor's algorithm.

Q2

Quantum security: a block cipher is quantum secure against quantum adversaries if noefficient quantum algorithm can distinguish the block cipher from PRP (or a PRF) even by making quantum queries.

Superposition queries access quantum circuit implementing the primitive with a secret key.
Example: breaking 3-round Feistel cipher, quantum-type Even-Mansour cipher, CBC-MAC with Simon's algorithm.

Алгоритм Саймона, см. [4]

- Частный случай задачи нахождения скрытой подгруппы.
- Пусть $f : V_k \to V_{k'}, k \leq k'$ и выполнено одно из условий:
  - Отображение f инъективно.
  - Существует вектор $\vec{s} \in V_k \setminus (0, 0, \ldots, 0)$ такой, что для любых различных $x_1, x_2 \in V_k$ выполняется $f(x_1) = f(x_2) \Leftrightarrow x_1 = x_2 \oplus s$.
- Необходимо проверить, какое из указанных условий выполнено, и во втором случае определить $\vec{s} \in V_k \setminus (0, 0, \ldots, 0)$.
- Трудоемкость: $O(n)$, с учетом решения СЛУ $O(n^3)$, vs $O(\sqrt{2^n})$ в классическом случае.

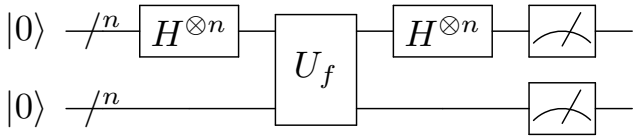

Рис. 1: Квантовая схема алгоритма Саймона.

Квантовый алгоритм Саймона. Слайд 2/4

1. Начальное состояние $|\psi_0\rangle = |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n}$, после $H^{\otimes n}$ получим
$$|\psi_1\rangle = \sum_{x \in V_n} \frac{|x\rangle}{\sqrt{2^n}} |0\rangle^{\otimes n}.$$
2. Применим U_f к $|\psi_1\rangle$, получим $|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in V_n} |x\rangle\,|f(x)\rangle$.
3. Измерение нижних n кубитов, получим случайное значение $f(r) \in V_n,\ r \in V_n$. Верхние n кубит перейдут в $\frac{1}{\sqrt{2}}|r\rangle + \frac{1}{\sqrt{2}}|r \oplus s\rangle$, состояние всей системы
$$|\psi_3\rangle = \left(\frac{1}{\sqrt{2}}|r\rangle + \frac{1}{\sqrt{2}}|r \oplus s\rangle\right) \otimes |f(r) \equiv f(r \oplus s)\rangle.$$
4. Выполнить $H^{\otimes n}$ для первых n кубит $|\psi_3\rangle$, получим $|\psi_4\rangle = \sum_{y \in V_n} \beta_y |y\rangle$, где
$$\beta_y = \frac{1}{\sqrt{2^{(n+1)}}}(-1)^{(r,y)} + \frac{1}{\sqrt{2^{(n+1)}}}(-1)^{((r\oplus s),y)} = \frac{(-1)^{(r,y)}}{\sqrt{2^{(n+1)}}}\left[1 + (-1)^{(s,y)}\right].$$
5. Измерение верхних n кубитов. Возможны два случая:
$$\begin{cases} (s,y) \equiv 1 (mod 2), \Rightarrow \beta_y = 0; \\ (s,y) \equiv 0 (mod 2), \Rightarrow \beta_y = 2 \cdot \frac{(-1)^{(r,y)}}{\sqrt{2^{(n+1)}}} = \frac{(-1)^{(r,y)}}{\sqrt{2^{(n-1)}}}; \end{cases}$$
Таким образом, в результате измерения верхних n кубитов, с вероятностью $|\beta_y|^2 = \frac{1}{2^{n-1}}$ получим какое-то значение y, для которого выполняется свойство $(s,y) \equiv 0 (mod 2)$.
6. Повторить 1-5 несколько раз, получим $n-1$ линейно независимых $y_1, \ldots y_{n-1}$.

Квантовый алгоритм Саймона. Слайд 3/4

Получили СЛУ над GF(2):

$$\begin{cases} s_1 \cdot y_{1,1} + s_2 \cdot y_{1,2} + \ldots + s_n \cdot y_{1,n} = 0 \\ s_1 \cdot y_{2,1} + s_2 \cdot y_{2,2} + \ldots + s_n \cdot y_{2,n} = 0 \\ \vdots \\ s_1 \cdot y_{n-1,1} + s_2 \cdot y_{n-1,2} + \ldots + s_n \cdot y_{n-1,n} = 0 \end{cases}$$

найдем такое $s \in V_n$, что $f(x) = f(x \oplus s)$.
Если $s \neq 0$, вероятность того, что удастся получить $n-1$ линейно независимых вариантов $y_1, \ldots y_{n-1}$ можно оценить с помощью таблицы 1:

Номер запуска процедуры 1-5	Неудачный результат на шаге 5	Вероятность неудачи на соответствующем шаге	Вероятность получить совместную СЛУ
1	$\vec{0} \in V_n$	$\frac{1}{2^{n-1}}$	$1 - \frac{1}{2^{n-1}}$
2	$\{\vec{0}, y_1\}$	$\frac{2}{2^{n-1}}$	$1 - \frac{2}{2^{n-2}}$
3	$\{\vec{0}, y_1, y_2, y_1 \oplus y_2\}$	$\frac{4}{2^{n-1}}$	$1 - \frac{4}{2^{n-3}}$
...	...	...	...
n-1	$\{\vec{0}, y_1, y_2, \ldots\}$	$\frac{2^{n-2}}{2^{n-1}} = \frac{1}{2}$	$1 - \frac{1}{2} = \frac{1}{2}$

Таблица 1: Вероятность успеха алгоритма Саймона для $f : V_n \to V_n$ за n итераций можно вычислить перемножив вероятности успеха из 4 столбца.

Квантовый алгоритм Саймона. Слайд 4/4

1. Вероятность получить $n-2$ линейно независимых уравнения оценивается по формуле $S_n \to \frac{b_1}{1-q}$ при $n \to \infty$ как

$$1 - \frac{1}{4}\left(1 + 1/2 + 1/4 + \ldots\right) > \frac{1}{2};$$

2. Вероятность успеха на последнем шаге равна $1/2$;
3. Вероятность получить $n-1$ линейно независимое уравнение оценивается снизу $1/2 \times 1/2$, т.е. вероятность успеха алгоритма Саймона $> 1/4$:

$$P_{Simon}(success) > \prod_{k=1}^{\infty}\left(1 - \frac{1}{2^k}\right) > \frac{1}{4}.$$

Квантовый алгоритм Саймона. Пример. Слайд 1/3

Рассмотрим $f : V_3 \to V_3$, заданное в таблице:

$x_1x_2x_3$	$f_1\ f_2\ f_3$
000	1 0 1
001	0 1 0
010	0 0 0
011	1 1 0
100	0 0 0
101	1 1 0
110	1 0 1
111	0 1 0

Таблица 2: Период $s = 110$, т.е. $\forall\, x \in V_3 :\ f(x) = f(x \oplus s)$, координатные функции:
$f_1(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3 \oplus 1$, $f_2(x_1, x_2, x_3) = x_3$, $f_3(x_1, x_2, x_3) = x_1x_3 \oplus x_2x_3 \oplus x_1 \oplus x_2 \oplus x_3 \oplus 1$.
В данном примере у каждого образа ровно два прообраза.

Квантовый алгоритм Саймона. Пример. Слайд 2/3

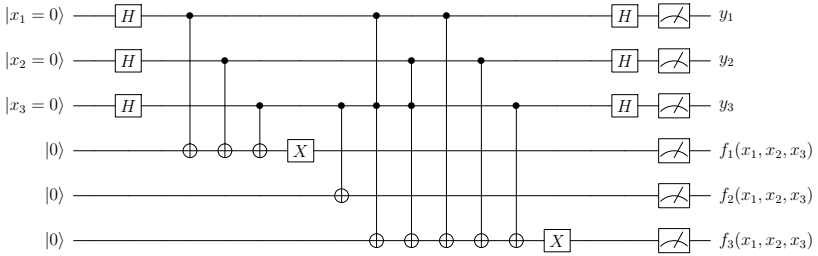

Рис. 2: Квантовая схема, реализующая алгоритм Саймона для $f : V_3 \to V_3$.

$y \in V_3$	Вероятность получить y
111	0.25
001	0.25
110	0.25
000	0.25

Таблица 3: Распределение вероятностей возможных результатов измерений первых трех кубитов (проверено в квантовом симуляторе Quipper).

Квантовый алгоритм Саймона. Пример. Слайд 3/3

Допустим, что в результате нескольких запусков получены $y_1 = 111$ и $y_2 = 001$, по которым составлена система линейных уравнений

$$\begin{cases} s_1 \cdot 1 + s_2 \cdot 1 + s_3 \cdot 1 = 0 \\ s_1 \cdot 0 + s_2 \cdot 0 + s_3 \cdot 1 = 0 \end{cases}.$$

Решения этой СЛУ над $\mathrm{GF}(2)$ – это $s = 000$ и период $s = 110$.

Алгоритм Саймона vs схема Эвена-Мансура

- В 1997 году, в работе [5], предложена схема $E : V_n \times V_n \times V_n \to V_n$;
- $E_{k_1,k_2}(m) = c$;
- k_1, k_2 – неизвестные ключи;
- P – известная подстановка;

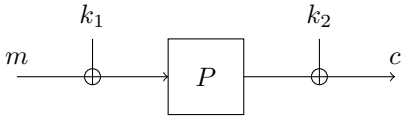

Рис. 3: Схема Эвена-Мансура.

Рассматривается отображение $f(x) = P(x \oplus k_1) \oplus k_2 \oplus P(x)$, для всех $x \in V_n$ выполняется $f(x) = f(x \oplus k_1)$, т.е. для поиска k_1 применим квантовый алгоритм Саймона. После определения k_1 по известным парам (о.т., ш.т.) легко восстанавливается k_2, см. [6], [7], [8], [10].

Цитаты из публикаций. 1/4

В [10], section 3: *Previous works* ***have used Simon's algorithm to break the security of classical constructions*** *in symmetric cryptography: the* ***Even-Mansour*** *construction and the* ***3-round Feistel*** *scheme....* При этом, помимо результатов [6] и [7], рассматривается применение алгоритма Саймона к режимам CBC-MAC, PMAC, GMAC, GCM, OCB, алгоритмам CLOC, AEZ, COPA, OTR, POET, OMD, Minalpher – продемонстрирована возможность навязывания ложных сообщений, квантовая «слайд-атака» на ключ с полиномиальной трудоемкостью (только в модели Q2!!!).

В [11] (Grover Meets Simon, FX-конструкции): *However, as we show in this work,* ***using whitening keys does not increase the security in the quantum-CPA setting*** *significantly. For this we present a quantum algorithm that breaks the construction with whitening keys in essentially* ***the same time complexity as Grover's original algorithm*** *breaks the underlying block cipher. Technically this result is based on the combination of the quantum algorithms of Grover and Simon...*

Так же в [11]: *Kaplan et al. further showed how slide attacks can profit from using a quantum computer.*

Цитаты из публикаций. 2/4

В [12]: *At Crypto 2016, Kaplan et al. proposed the first quantum exponential acceleration of a classical symmetric cryptanalysis technique: they showed that, in the superposition query model,* ***Simon's algorithm could be applied to accelerate the slide attack on the alternate-key cipher. This allows to recover an n-bit key with*** $O(n)$ ***quantum time and queries.*** (хотя на самом деле в [10] n - это длина блока б.ш., а не длина ключа)

В [13]:*...the security significantly changes when we consider attacks in the quantum settings,* ***where the adversary can make superposition queries****... we continue the investigation of the security of Feistel ciphers in the* ***quantum setting****. We show a quantum CCA (chosen-ciphertext attacks) distinguisher against 4-round Feistel cipher.*

В [14]: *For d-branch Type-1 GFS, we introduce (2d-1)-round quantum distinguishers ... For 2d-branch Type-2 GFS, we give (2d+1)-round quantum distinguishers with polynomial time. Classically, Moriai and Vaudenay proved that a 7-round 4-branch Type-1 GFS and 5-round 4-branch Type-2 GFS are secure pseudo-random permutations. Obviously,* ***they are no longer secure in quantum setting. Using the above quantum distinguishers, we introduce generic quantum key-recovery attacks by applying the combination of Simon's and Grover's algorithms*** *recently proposed* in [11].

Цитаты из публикаций. 3/4

В [15] (а так же в [16], улучшение результатов [14]): *...we give more improved polynomial-time quantum distinguishers for Type-1 GFS in quantum chosen-plaintext attack (qCPA) setting and quantum chosen-ciphertext attack (qCCA) setting. ... we give some quantum attacks on CAST-256 block cipher. We find 12-round and 13-round polynomial-time quantum distinguishers in qCPA and qCCA settings, respectively, while the best previouse is only 7 rounds.* ***Hence, we could derive quantum key-recovery attack on 19-round CAST-256****. While the best previous quantum key-recovery attack is on 16 rounds. When comparing our quantum attacks with classical attacks, our result also reaches 16 round on CAST-256 with 128-bit key under a competitive complexity.*

В [17] рассмотрена возможность применения алгоритма Саймона к нескольким итерациям схемы Эвена-Мансура:

$$E_P(x; k_1, k_2, \ldots, k_t) = (P_{k_t} \circ \cdots \circ P_{k_1})(x) \oplus k_{t+1}.$$

Представлен подход для поиска итерационных ключей, являющийся обобщением квантовой слайд-атаки из [10].

Цитаты из публикаций. 4/4

В [18]: ... ***We focus on the study of the symmetric ciphers against Q2 adversary***. *Combining with Simon's algorithm, we convert the classical advanced slide attacks to a quantum one, that gains an exponential speed-up of the time complexity. Thus, we could break 2K-/4K-Feistel block ciphers and 2K-/4K-DES block ciphers in polynomial time.*
Concretely, we turn the classical attacks on 2K-/4K-Feistel block ciphers with $2^{0.25n}$ *encryptions into quantum attacks with about* $n + 2 + 2\sqrt{n/2 + 1}$ *quantum queries of the encryption process using about* $n + 1$ *qubits.*

We turn the classical attacks on 2K-/4K-DES block ciphers with 233 encryptions into quantum attacks with 155 or 233 quantum queries of the encryption process with 65 qubits.

В [18] есть раздел про ГОСТ 28147-89, основанный на использовании комбинации свойств алгоритма шифрования и квантового алгоритма Гровера: .....*we give a new quantum key-recovery attack, that breaks GOST in* $2^{114.8}$ *quantum queries of the encryption process, which is faster than the quantum brute force search attack by a factor of* $2^{13.2}$. *The attack needs (не менее) 224 qubits.*

Ещё несколько работ про использование квантового алгоритма Саймона: [19], [20], [21], [22] и др.

Алгоритм Саймона vs схема Эвена-Мансура, пример 1.

Выберем $P = (12, 8, 2, 1, 13, 4, 15, 6, 7, 0, 10, 5, 3, 14, 9, 11)$, в схеме Эвена-Мансура зафиксируем $k_1 = 5, k_2 = 14$ (см. рис. 3), получим $E : V_4 \to V_4$, где $E(x) = P(x \oplus k_1) \oplus k_2$.

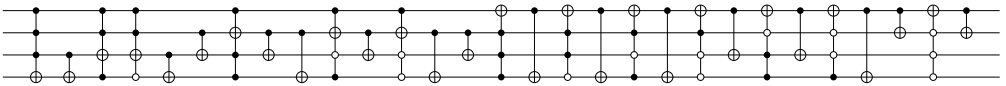

Рис. 4: Квантовая схема, реализующая подстановку P.

Все возможные пары блоков о.т. и ш.т.: (0,10), (1,3), (2,8), (3,1), (4,6), (5,2), (6,15), (7,12), (8,0), (9,13), (10,5), (11,7), (12,14), (13,9), (14,11), (15,4).

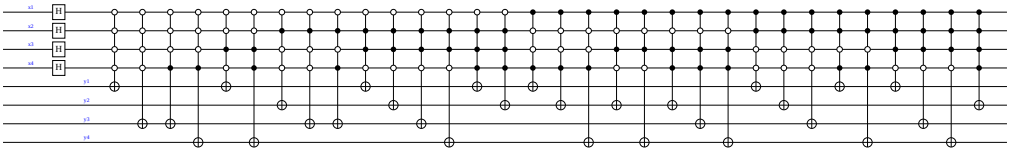

Рис. 5: Квантовая схема для подготовки $\frac{1}{\sqrt{2^4}} \sum_{x=0}^{15} |x\rangle |E_{k_1=5,k_2=14}(x)\rangle$ (задана по таблице, можно было реализовать ANF каждой координаты).

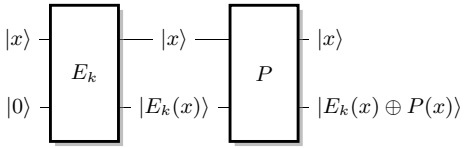

Рис. 6: Квантовая схема для поиска ключа k_1 в схеме Эвена-Мансура из [10].

Посмотрим распределение вероятностей результатов измерений после выполнения алгоритма Саймона:

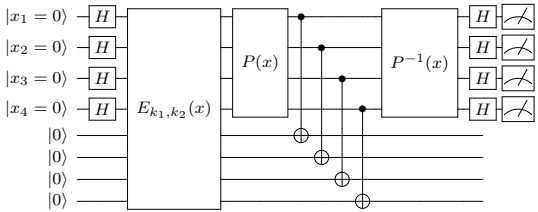

Рис. 7: Квантовая схема для поиска ключа k_1. Обратите внимание, тут нет регистра для записи ключа.

$y \in V_4$	$P(y)$
1000	0.125
0000	0.125
0010	0.125
0101	0.125
0111	0.125
1010	0.125
1101	0.125
1111	0.125

Таблица 4: Уравнения для СЛУ над GF(2): $< k_1, y >= 0$.

Допустим, что в квантовой схеме на рис. 5 (подготовка $\frac{1}{\sqrt{2^4}} \sum_{x=0}^{15} |x\rangle |E_{k_1,k_2}(x)\rangle$) самый правый квантовый гейт не применяется, т.е. таблица переходов блоков о.т. и ш.т. будет нарушена, вместо (15,4) получим (15,0), при этом все остальные переходы выполняются правильно (при $k_1 = 5, k_2 = 14$).

Распределение вероятностей результатов измерений после выполнения алгоритма Саймона, когда имеются не все блоки о.т. и ш.т.:

$y \in V_4$	$P(y)$
0000	0.1328125
0001	0.0078125
0010	0.1015625
0011	0.0078125
0100	0.0078125
0101	0.1015625
0110	0.0078125
0111	0.1328125
1000	0.1015625
1001	0.0078125
1010	0.1328125
1011	0.0078125
1100	0.0078125
1101	0.1328125
1110	0.0078125
1111	0.1015625

Таблица 5: Уравнения для СЛУ над GF(2): должны быть $< k_1, y >= 0$.
Выбрали $k_1 = 5$, т.е. $k_1 = 0101$, по таблице видно, что $P(< k_1, y >= 1) = 0.0625$.
Тем не менее, когда блоков о.т. и ш.т. недостаточно, *необходимо учитывать* $P(< k_1, y >= 1)$.

Распределение вероятностей результатов измерений после выполнения алгоритма Саймона, когда имеются не все блоки о.т. и ш.т.:

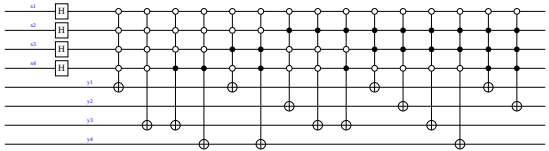

Рис. 8: Допустим, что при $k_1 = 5, k_2 = 14$ вместо квантовой схемы на рис. 5 задана только часть таблицы переходов.

$y \in V_4$	$P(y)$ без 1 перехода	$P(y)$ стало
0000	0.1328125	0.140625
0001	0.0078125	0.03125
0010	0.1015625	0.078125
0011	0.0078125	0.03125
0100	0.0078125	0.03125
0101	0.1015625	0.109375
0110	0.0078125	0.03125
0111	0.1328125	0.109375
1000	0.1015625	0.046875
1001	0.0078125	0.03125
1010	0.1328125	0.109375
1011	0.0078125	0.03125
1100	0.0078125	0.03125
1101	0.1328125	0.078125
1110	0.0078125	0.03125
1111	0.1015625	0.078125

Таблица 6: Уравнения для СЛУ над GF(2): должны быть $< k_1, y >= 0$.
Так как $k_1 = 5$, т.е. $k_1 = 0101$, то по таблице видно, что $P(< k_1, y >= 1) = 0.25$.

Алгоритм Саймона vs схема Эвена-Мансура, пример 2.

Выберем $k_1 = 2, k_2 = 14$ (см. рис. 3), все возможные пары блоков о.т. и ш.т.: (0,12), (1,15), (2,2), (3,6), (4,1), (5,8), (6,3), (7,10), (8,4), (9,11), (10,9), (11,14), (12,7), (13,5), (14,13), (15,0).

$y \in V_4$	$P(y)$
0000	0.1875
0001	0.125
0100	0.125
0101	0.0625
1000	0.1875
1001	0.125
1100	0.125
1101	0.0625

Таблица 7: Распределение вероятностей результатов измерений после выполнения алгоритма Саймона.

Неравномерность распределения в таблице 7 появляется из-за «нежелательных коллизий».

Существуют такие $x_1 \neq x_2 \neq x_3 \neq x_4$, что

$$P(x_1 \oplus k_1) \oplus P(x_1) \equiv P(x_2 \oplus k_1) \oplus P(x_2),$$

$$P(x_3 \oplus k_1) \oplus P(x_3) \equiv P(x_4 \oplus k_1) \oplus P(x_4),$$

причем $P(x_1 \oplus k_1) \oplus P(x_1) \equiv P(x_3 \oplus k_1) \oplus P(x_3)$.

Например, для выбранной $P = (12, 8, 2, 1, 13, 4, 15, 6, 7, 0, 10, 5, 3, 14, 9, 11)$ и $k_1 = 2$

$$x_1 = 4,\ x_2 = 6,$$

$$x_3 = 5,\ x_4 = 7,$$

или

$$x_1 = 9,\ x_2 = 11,$$

$$x_3 = 13,\ x_4 = 15.$$

Распределение вероятностей результатов измерений после выполнения алгоритма Саймона, когда имеются не все блоки о.т. и ш.т.:

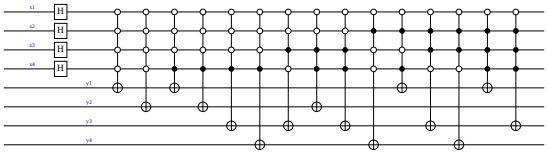

Рис. 9: Допустим, что при $k_1 = 2, k_2 = 14$ вместо квантовой схемы на рис. 5 задана только часть таблицы переходов.

$y \in V_4$	$P(y)$
0000	0.15625
0001	0.03125
0010	0.03125
0011	0.03125
0100	0.15625
0101	0.03125
0110	0.03125
0111	0.03125
1000	0.09375
1001	0.09375
1010	0.03125
1011	0.03125
1100	0.09375
1101	0.09375
1110	0.03125
1111	0.03125

Таблица 8: Уравнения для СЛУ над GF(2): должны быть $< k_1, y >= 0$.
Так как $k_1 = 2$, т.е. $k_1 = 0010$, то по таблице видно, что $P(< k_1, y >= 1) = 0.25$ (совпала с $P(< k_1, y >= 1)$ в таблице 6).

В работе [10] представлены теоремы, определяющие соотношение между количеством итераций алгоритма Саймона и вероятностью успешного определения периода отображения f:

Для $f : \{0,1\}^n \to \{0,1\}^n$, у которого на всех x выполняется $f(x \oplus s) = f(x)$, вводится

$$\varepsilon(f,s) = \max_{t \in \{0,1\}^n \setminus \{0,s\}} \Pr_x[f(x) = f(x \oplus t)].$$

Для случайного отображения f $\varepsilon(f,s) = \Theta(n2^{-n})$ (точечная оценка), если отображение $f = const$, то $\varepsilon(f,s) = 1$, тогда однозначно вычислить период s невозможно.

Theorem 1 (С ограничением $\varepsilon(f,s)$)

Если $\varepsilon(f,s) \le p_0 < 1$, то для определения периода s с вероятностью не менее $1 - \left(2\left(\frac{1+p_0}{2}\right)^c\right)^n$ требуется cn запусков алгоритма Саймона.

Theorem 2 (Без ограничений $\varepsilon(f,s)$)

Если после cn запусков алгоритма Саймона найден вектор t, ортогональный всем полученным в результате измерений u_i, то $\Pr_x[f(x \oplus t) = f(t)] \ge p_0$ с вероятностью не менее $1 - \left(2\left(\frac{1+p_0}{2}\right)^c\right)^n$.

В рассмотренных примерах с неполными таблицами переходов блоков о.т. и ш.т., в обоих случаях (несмотря на наличие «нежелательных коллизий»)

$$P(< k_1, y >= 1) = 0.25.$$

Для поиска k_1 теперь требуется «угадать» значение уравнения $< k_1, y >$.

Из работы [10]:

1. Для применения квантового алгоритма Саймона необходимо обосновывать $\varepsilon(f, s) < 1$.
2. В теореме 1, при $c \geq 3/(1 - p_0)$ вероятность ошибки убывает по экспоненциальному закону, в зависимости от n.
3. В теореме 2, при $c \geq 3/(1 - p_0)$ вероятность $1 - \left(2\left(\frac{1+p_0}{2}\right)^c\right)^n$ стремится к 1 по экспоненциальному закону в зависимости от n.

О применении к другим криптосхемам.

Применение квантового алгоритма Саймона может быть эффективно в случаях:

1. Модель Q1: получили все возможные(большую часть) пары блоков о.т. и ш.т. на одном неизвестном ключе, приготовили соотв. состояние, как на рис. 5, т.е. перешли к Q2 (требуется порядка 2^n обобщенных CNOT, т.е. трудоемкость не $poly(n)$).
2. Модель Q2: анализируем квантовый white-box, т.е. можем работать с суперпозицией пар о.т. и ш.т., полученных на одном неизвестном ключе (ключ – встроенный параметр, некоторой «квантовый гейт»); возможно актуально для протоколов Quantum Secure Direct Communication (QSDC).
3. Модель Q2: У «Алисы» есть квантовый компьютер и она хочет обмануть «Боба» – см. атаки на MAC и AEAD режимы в работах [9, 10].

Если указанные условия не выполнены, то применение квантового алгоритма Саймона для поиска ключей в схеме Эвена-Мансура (а так же и для других схем, для которых построены «различители», см. [6] - [22]), может быть неэффективно, т.к. появляется дополнительная неопределенность при составлении СЛУ над GF(2).

Спасибо за внимание.

Бонус

В работе [23] представлена реализация сумматора по модулю 2^n. Если в реализации ADD_5 из работы [23] опустить дополнительный рабочий кубит $|z\rangle$, то получится реализация операции сложения по модулю 2^n без дополнительных кубитов, т.е. для реализации $|a\rangle\,|b\rangle \to |a\rangle\,|b + a \mod 2^n\rangle$ требуется ровно $2n$ кубитов (проверено в квантовом симуляторе Quipper при $n = 4$ и $n = 5$).

Если в схеме Эвена-Мансура заменить операцию побитового XOR с ключом k_1 на операцию сложения по модулю 2^n, то представленное отображение $f(x)$ перестанет быть периодическим, при применении квантового алгоритма Саймона, так же как и в табл. 6 и табл. 8, появляются $P(< k_1, y >= 1) > 0$. Примеров периодических отображений, к которым применялся бы квантовый алгоритм Саймона для поиска периода при модульном сложении, автору неизвестно.

Судя по доказательствам теорем из работы [10], они применимы в случае когда $P(< k_1, y >= 1) = 0$. Если же $P(< k_1, y >= 1) > 0$ то трудоемкость определения истинного значения периода можно оценить сверху $O(2^{n-1} \cdot n^3)$ квантовых и классических операций (перебор всех возможных значений уравнений в СЛУ, решение каждой СЛУ методом Гаусса).

[1] Kaplan M., Leurent G., Leverrier A., Naya-Plasencia M. Quantum Differential and Linear Cryptanalysis. IACR Transactions on Symmetric Cryptology, 2016, 71-94. https://doi.org/10.13154/tosc.v2016.i1.71-94; FSE 2017. http://www.iacr.org/workshops/fse2017/slides/10-03.pdf

[2] Huiqin Xie, Li Yang *Quantum impossible differential and truncated differential cryptanalysis*, arXiv:1712.06997v2 [quant-ph], 2018.

[3] Akinori Hosoyamada and Yu Sasaki. Cryptanalysis against Symmetric-Key Schemes with Online Classical Queries and Offline Quantum Computations. https://eprint.iacr.org/2017/977.pdf.

[4] Simon D. R. On the power of quantum computation. Proceedings 35th Annual Symposium on Foundations of Computer Science.1994 p. 116-123. doi: 10.1109/SFCS.1994.365701.

[5] Even S., Mansour Y. A construction of a cipher from a single pseudorandom permutation. Cryptology.1997. vol. 10(3) p. 151-162.

[6] Kuwakado H., Morii M. Quantum distinguisher between the 3-round Feistel cipher and the random permutation. Information Theory Proceedings (ISIT) 2010 IEEE International Symposium. 2010 p. 2682-2685.

[7] Kuwakado H., Morii M. Security on the quantum-type Even-Mansour cipher. Information Theory and its Applications (ISITA). p. 312-316. 2012.

[8] Gorjan Alagic and Alexander Russell. Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts. https://eprint.iacr.org/2016/960.pdf, 2016.

[9] Anand, M.V., Targhi, E.E., Tabia, G.N., Unruh, D.: Post-quantum security of the CBC, CFB, OFB, CTR, and XTS modes of operation. In: Takagi, T. (ed.) Post-Quantum Cryptography - 7th International Workshop,

PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings. Lecture Notes in Computer Science, vol. 9606, pp. 44–63. Springer (2016).

[10] Kaplan M., Leurent G., Leverrier A., Naya-Plasencia M. Breaking Symmetric Cryptosystems Using Quantum Period Finding. Robshaw M., Katz J. (eds) Advances in Cryptology – CRYPTO 2016. CRYPTO 2016. Lecture Notes in Computer Science. 2016. vol. 9815. https://doi.org/10.1007/978-3-662-53008-5_8.

[11] Leander G., May A. Grover Meets Simon – Quantumly Attacking the FX-construction. Takagi T., Peyrin T. (eds) Advances in Cryptology – ASIACRYPT 2017. vol. 10625. https://doi.org/10.1007/978-3-319-70697-9_6.

[12] Xavier Bonnetain, María Naya-Plasencia, André Schrottenloher. On Quantum Slide Attacks. https://eprint.iacr.org/2018/1067.pdf, 2018.

[13] Ito G, Hosoyamada A., Matsumoto R., Sasaki Y, Iwata T. Quantum Chosen-Ciphertext Attacks against Feistel Ciphers. https://eprint.iacr.org/2018/1193.pdf, 2018.

[14] Dong X, Li Z., Wang X. Quantum cryptanalysis on some generalized Feistel schemes. Sci China Inf SCi, 2019, 62(2): 022501: https://doi.org/10.1007/s11432-017-9436-7.

[15] Ni B., Dong X. Improved quantum attacks on Type-1 Generalized Feistel Schemes and Its application to CAST-256. https://eprint.iacr.org/2019/318.pdf, 2019.

[16] Ito G., Iwata T. Quantum Distinguishing Attacks against Type-1 Generalized Feistel Ciphers. https://eprint.iacr.org/2019/327.pdf, 2019.

[17] Hosoyamada A., Aoki K. On Quantum Related-Key Attacks on Iterated Even-Mansour Ciphers. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences. 2019. vol. E102.A(1) p. 27-34. 10.1587/transfun.E102.A.27.

[18] Xiaoyang Dong, Bingyou Dong, Xiaoyun Wang. Quantum attacks on some feistel block ciphers. Designs, Codes and Cryptography. https://doi.org/10.1007/s10623-020-00741-y. 2020.

[19] Hodzic S., Knudsen L.R. A quantum distinguisher for 7/8-round SMS4 block cipher. Quantum Information Processing (2020) 19: 441. https://doi.org/10.1007/s11128-020-02920-6. 2020.

[20] Carlos Cid and Akinori Hosoyamada and Yunwen Liu and Siang Meng Sim, Quantum Cryptanalysis on Contracting Feistel Structures and Observation on Related-key Settings, Cryptology ePrint Archive, Report 2020/959, 2020, https://eprint.iacr.org/2020/959.

[21] Xavier Bonnetain, Akinori Hosoyamada, Maria Naya-Plasencia, Yu Sasaki and Andre Schrottenloher. Quantum Attacks without Superposition Queries: the Offline Simon's Algorithm. https://eprint.iacr.org/2019/614.pdf

[22] Bonnetain X., Jaques S. Quantum Period Finding against Symmetric Primitives in Practice, Cryptology ePrint Archive, Report 2020/1418, 2020, https://eprint.iacr.org/2020/1418.

[23] Yasuhiro Takahashi, Seiichiro Tani, and Noboru Kunihiro. Quantum addition circuits and unbounded fan-out. Quantum Information & Computation, 10(9&10):872–890, 2010. https://arxiv.org/pdf/0910.2530.pdf