Влияние теории квантовых вычислений на развитие современной криптографии

Денисенко Д.В., Никитенкова М.В., Поляков М.В., Рудской В.И.

21 марта 2019 г.

Структура доклада

1. Гейтовая модель квантовых вычислений. Квантовые схемы. Квантовые алгоритмы.
2. Обзор применения квантовых алгоритмов Гровера, Саймона, комбинации Гровера и Саймона, HHL.
3. Оценки необходимого количества логических кубитов и квантовых вентилей для реализации алгоритмов блочного шифрования в виде квантовых схем на примере Simplified-DES, ГОСТ Р 34.12-2015 (результаты работ [1], [2], [3]).
4. Обзор современных достижений в области создания квантовых компьютеров. Основные выводы из отчета Quantum Computing: Progress and Prospects [4].

Процесс квантовых вычислений

1. Вычислительная система = составная система кубитов;
2. Задается начальное состояние (одно из базисных);
3. Применяется последовательность унитарных преобразований состояния;
4. Проводится измерение и интерпретируется результат.

Бит $\Leftrightarrow$ Квантовый бит

- Сопоставим значению бита 0 состояние кубита $|e_0\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$,

  сопоставим значению бита 1 состояние кубита $|e_1\rangle = |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.
- Битовому вектору $(b_1, b_2, \ldots, b_n) \in V_n$ сопоставим

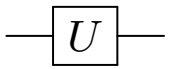
$$|b_1\rangle \otimes |b_2\rangle \otimes \ldots \otimes |b_n\rangle = |b_1 b_2 \ldots b_n\rangle$$

- Начальное состояние системы, например $|0\rangle^{\otimes n} = |0 \ldots 0\rangle$

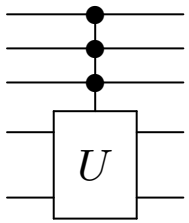
Квантовые схемы

- Способ визуализации преобразований для лучшего восприятия;
- Горизонтальные полосы – кубиты и их состояния;
- Прямоугольники – некоторые квантовые операторы;
- Вертикальные полосы – управление (см. оператор CNOT);

- Однокубитовые операторы:



- Управляемые операторы ($C^{(3)}U^{(2)}$):



Квантовая схема, реализующая булеву функцию $f(x_1, \ldots, x_n)$

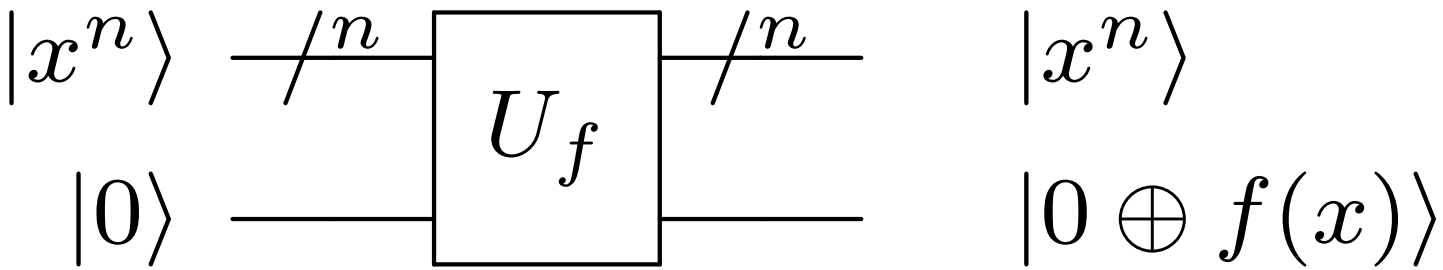


Рис. 1: Общий вид квантовой схемы, реализующей некоторую булеву функцию $f(x)$.

Пример: $f(x_1, x_2, x_3, x_4) = x_1x_2 \oplus x_2x_4 \oplus x_1x_2x_3 \oplus x_1x_2x_3x_4$

$f(x) = 1$ при $x \in \{0101, 0111, 1100\}$ и $f(x) = 0$ на всех остальных x.

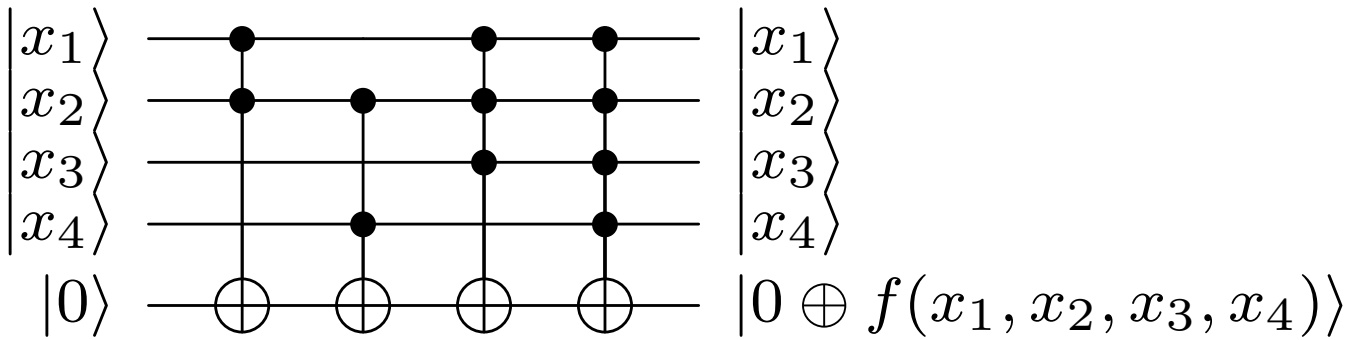


Рис. 2: Квантовая схема, задающая $f(x_1, x_2, x_3, x_4)$. Реализация с помощью обобщенных CNOT.

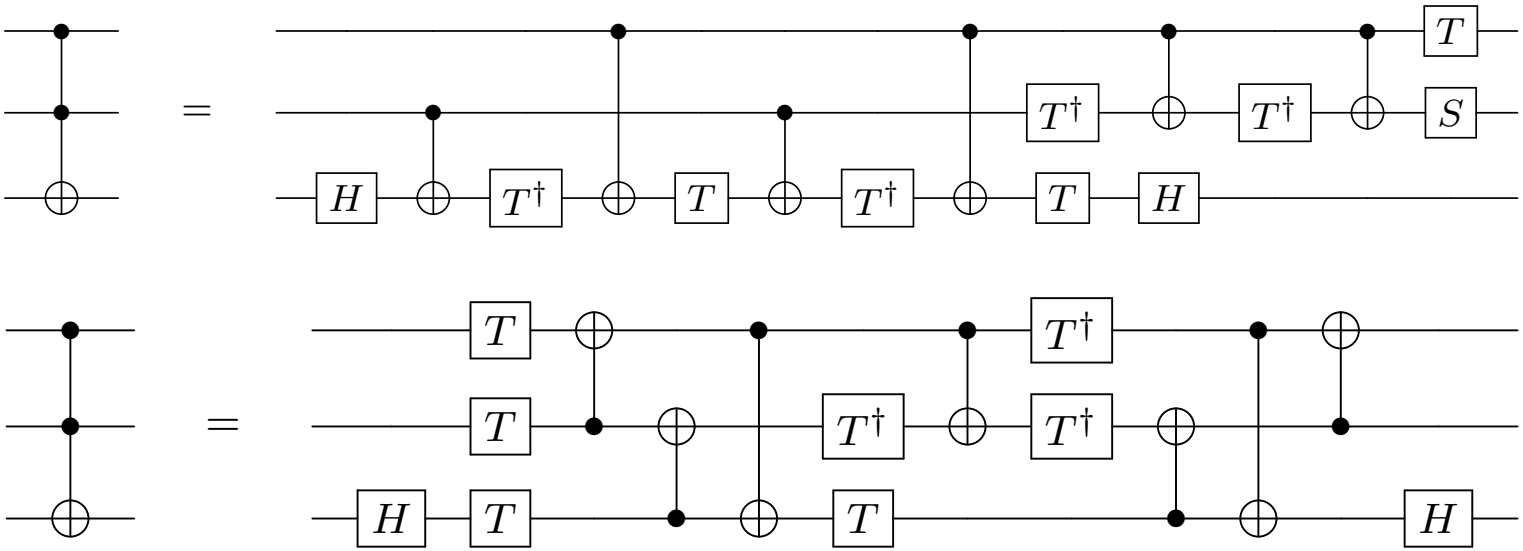


Рис. 3: См. https://www.mscs.dal.ca/ selinger/quipper/doc/QuipperLib-GateDecompositions.html

- Декомпозиция обобщенных CNOT в однокубитовые вентили и двухкубитовый CNOT без использования дополнительных кубитов существует.
- Декомпозиция обобщенных CNOT в однокубитовые вентили и двухкубитовый CNOT без использования дополнительных кубитов неоднозначна.

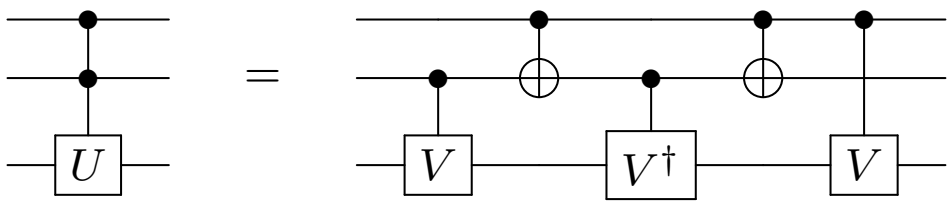


Рис. 4: Декомпозиция при $V^2 = U$. Если $V \equiv (1-i)(I+iX)/2$, то получится элемент Тоффоли.

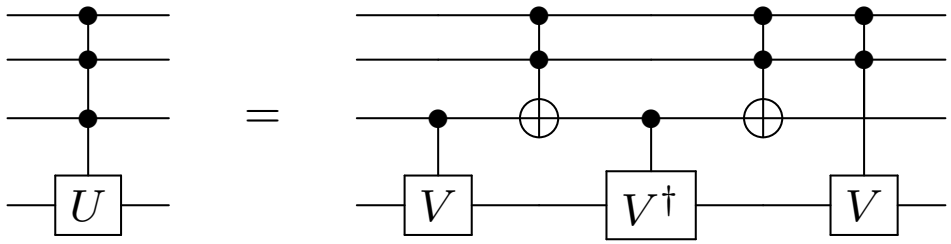


Рис. 5: Декомпозиция при $V^2 = U$, см. [50].

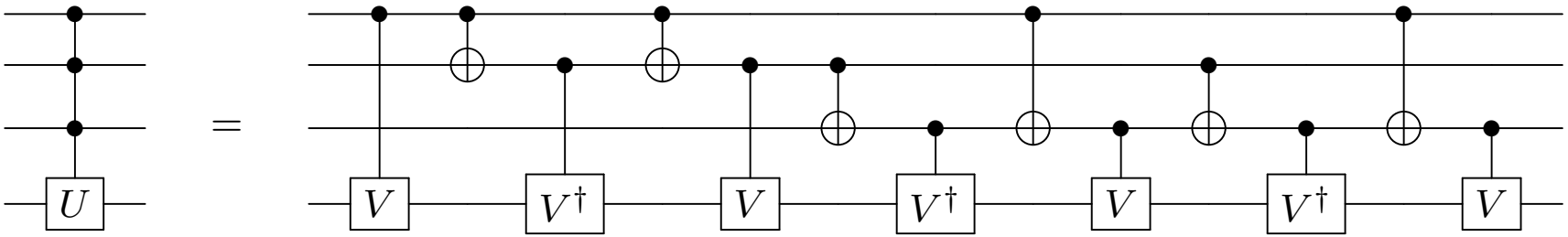


Рис. 6: Декомпозиция при $V^4 = U$, см. [50].

Алгоритм Бернштейна-Вазирани

- $f_{\vec{s}}(x_1, x_2, ..., x_n) = s_1 x_1 \oplus s_2 x_2 \oplus ... \oplus s_n x_n$;
- вектор $\vec{s} \in V_n$ – неизвестен, необходимо найти $\vec{s}$.
- квантовый алгоритм Б.В.(1993) решает указанную задачу за одно вычисление f;
- в классическом случае требуется n вычислений f.

Алгоритм Саймона

- 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.

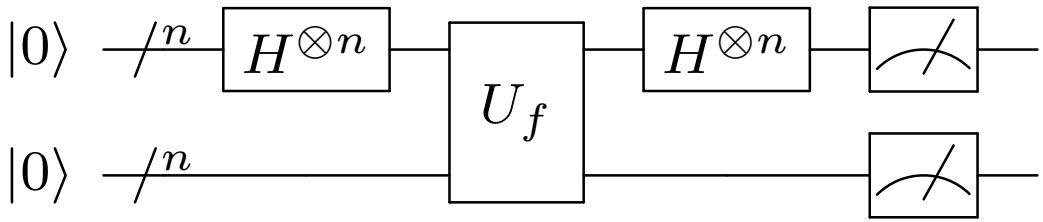
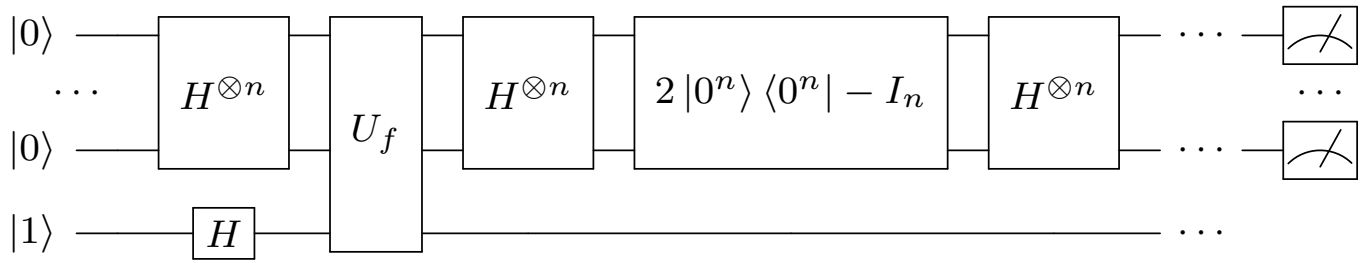


Рис. 7: Квантовая схема алгоритма Саймона.

Пусть $N = 2^n$, требуется «найти» какое-либо из M, $M < N/2$ возможных решений.

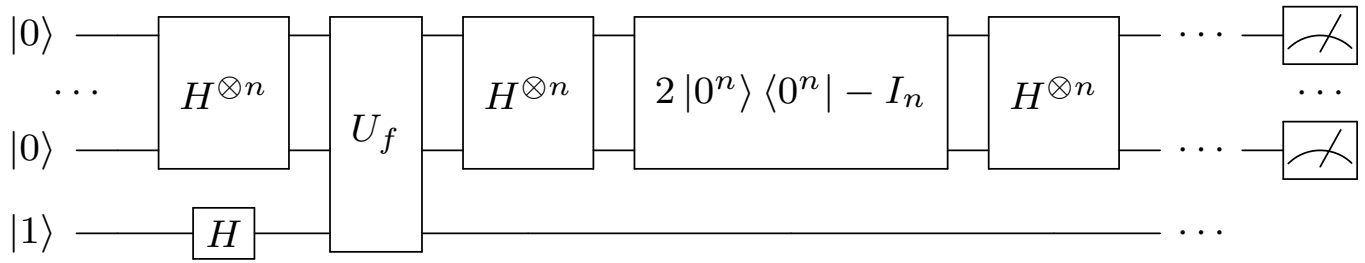


- Инициализация состояния равновероятной суперпозиции (применили $H^{\otimes n+1}$).
- Пусть $|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x'' |x\rangle$, $|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_x' |x\rangle$, тогда $|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$.
- Обозначим $cos(\frac{\theta}{2}) = \sqrt{\frac{N-M}{N}}$, тогда $|\psi\rangle = cos(\frac{\theta}{2}) |\alpha\rangle + sin(\frac{\theta}{2}) |\beta\rangle$, вероятность получить в результате измерения кубитов какое-либо из M возможных решений равна $sin^2(\frac{\theta}{2})$.
- После k итераций Гровера получим состояние

$$G^k |\psi\rangle = cos\left(\frac{2k+1}{2}\theta\right) |\alpha\rangle + sin\left(\frac{2k+1}{2}\theta\right) |\beta\rangle .$$

- После $k = \left[\frac{\pi}{4}\sqrt{\frac{N}{M}}\right]$ итераций Гровера и измерения кубитов с высокой вероятностью получим какое-то из M решений.

Пусть $N = 2^n$, требуется «найти» какое-либо из M, $M < N/2$ возможных решений.

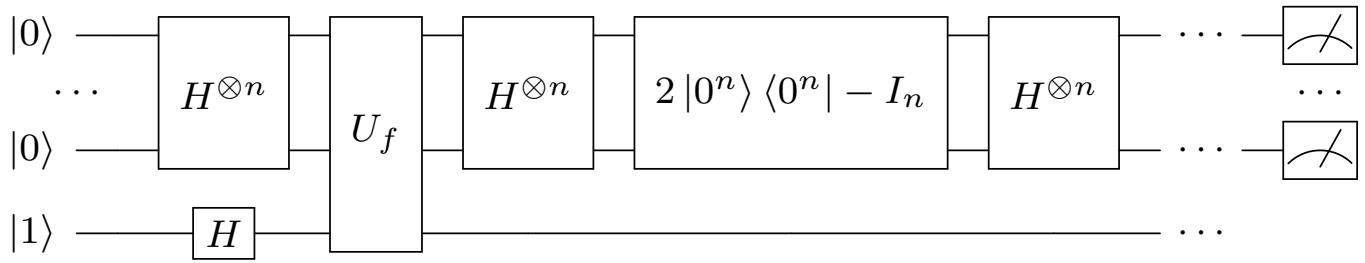


- Инициализация состояния равновероятной суперпозиции (применили $H^{\otimes n+1}$).
- Пусть $|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x'' |x\rangle$, $|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_x' |x\rangle$, тогда $|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$.
- Обозначим $cos(\frac{\theta}{2}) = \sqrt{\frac{N-M}{N}}$, тогда $|\psi\rangle = cos(\frac{\theta}{2}) |\alpha\rangle + sin(\frac{\theta}{2}) |\beta\rangle$, вероятность получить в результате измерения кубитов какое-либо из M возможных решений равна $sin^2(\frac{\theta}{2})$.
- После k итераций Гровера получим состояние

$$G^k |\psi\rangle = cos\left(\frac{2k+1}{2}\theta\right) |\alpha\rangle + sin\left(\frac{2k+1}{2}\theta\right) |\beta\rangle .$$

- После $k = \left[\frac{\pi}{4}\sqrt{\frac{N}{M}}\right]$ итераций Гровера и измерения кубитов с высокой вероятностью получим какое-то из M решений.

Пусть $N = 2^n$, требуется «найти» какое-либо из M, $M < N/2$ возможных решений.

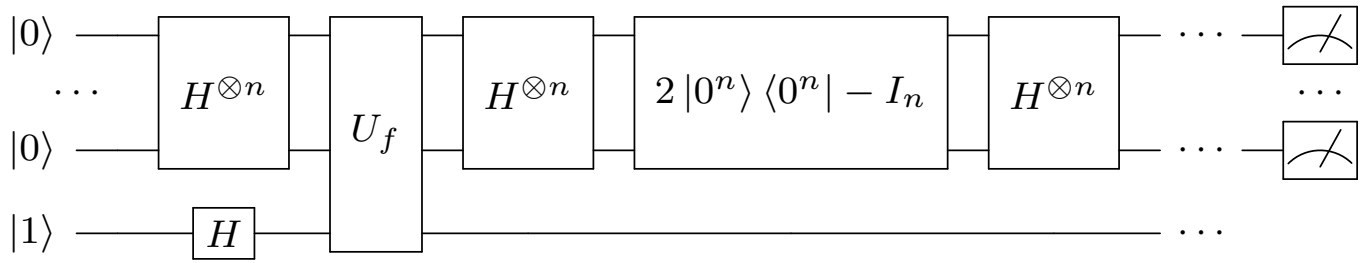


- Инициализация состояния равновероятной суперпозиции (применили $H^{\otimes n+1}$).
- Пусть $|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x'' |x\rangle$, $|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_x' |x\rangle$, тогда $|\psi\rangle = \sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle$.
- Обозначим $cos(\frac{\theta}{2}) = \sqrt{\frac{N-M}{N}}$, тогда $|\psi\rangle = cos(\frac{\theta}{2})\,|\alpha\rangle + sin(\frac{\theta}{2})\,|\beta\rangle$, вероятность получить в результате измерения кубитов какое-либо из M возможных решений равна $sin^2(\frac{\theta}{2})$.
- После k итераций Гровера получим состояние

$$G^k\,|\psi\rangle = cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle\,.$$

- После $k = \left[\frac{\pi}{4}\sqrt{\frac{N}{M}}\right]$ итераций Гровера и измерения кубитов с высокой вероятностью получим какое-то из M решений.

Пусть $N = 2^n$, требуется «найти» какое-либо из M, $M < N/2$ возможных решений.

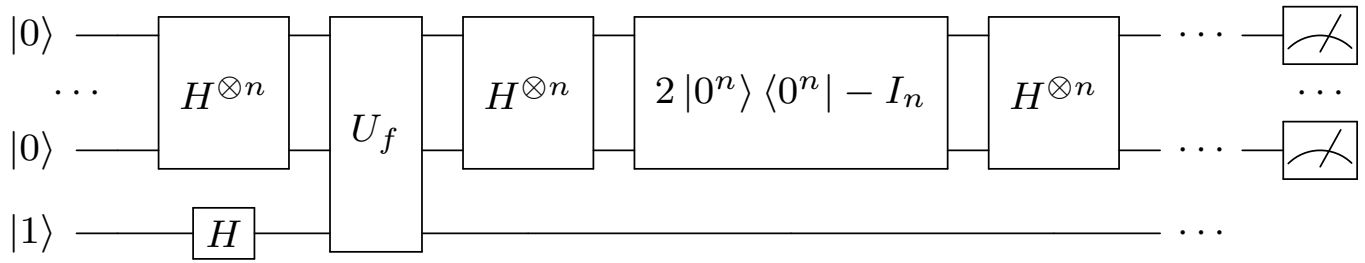


- Инициализация состояния равновероятной суперпозиции (применили $H^{\otimes n+1}$).
- Пусть $|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x'' |x\rangle$, $|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_x' |x\rangle$, тогда $|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$.
- Обозначим $cos(\frac{\theta}{2}) = \sqrt{\frac{N-M}{N}}$, тогда $|\psi\rangle = cos(\frac{\theta}{2}) |\alpha\rangle + sin(\frac{\theta}{2}) |\beta\rangle$, вероятность получить в результате измерения кубитов какое-либо из M возможных решений равна $sin^2(\frac{\theta}{2})$.
- После k итераций Гровера получим состояние

$$G^k |\psi\rangle = cos\left(\frac{2k+1}{2}\theta\right) |\alpha\rangle + sin\left(\frac{2k+1}{2}\theta\right) |\beta\rangle .$$

- После $k = \left[\frac{\pi}{4}\sqrt{\frac{N}{M}}\right]$ итераций Гровера и измерения кубитов с высокой вероятностью получим какое-то из M решений.

Пусть $N = 2^n$, требуется «найти» какое-либо из M, $M < N/2$ возможных решений.

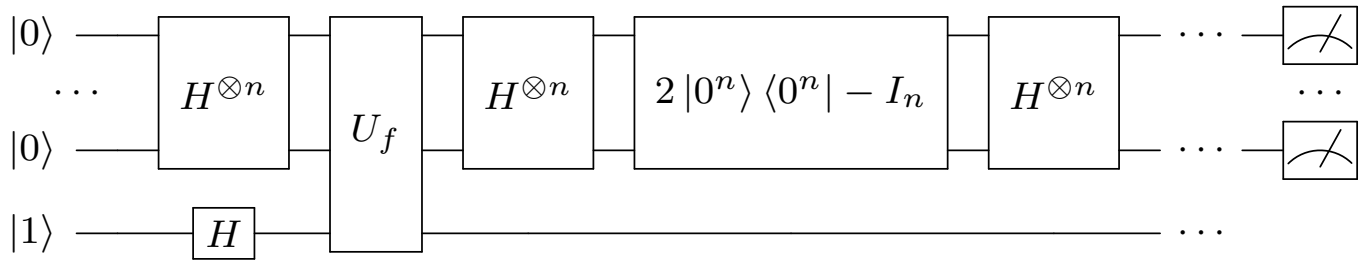


- Инициализация состояния равновероятной суперпозиции (применили $H^{\otimes n+1}$).
- Пусть $|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x'' |x\rangle$, $|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_x' |x\rangle$, тогда $|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$.
- Обозначим $cos(\frac{\theta}{2}) = \sqrt{\frac{N-M}{N}}$, тогда $|\psi\rangle = cos(\frac{\theta}{2}) |\alpha\rangle + sin(\frac{\theta}{2}) |\beta\rangle$, вероятность получить в результате измерения кубитов какое-либо из M возможных решений равна $sin^2(\frac{\theta}{2})$.
- После k итераций Гровера получим состояние

$$G^k |\psi\rangle = cos\left(\frac{2k+1}{2}\theta\right) |\alpha\rangle + sin\left(\frac{2k+1}{2}\theta\right) |\beta\rangle .$$

- После $k = \left[\frac{\pi}{4}\sqrt{\frac{N}{M}}\right]$ итераций Гровера и измерения кубитов с высокой вероятностью получим какое-то из M решений.

Пусть $N = 2^n$, требуется «найти» какое-либо из M, $M < N/2$ возможных решений.



- Инициализация состояния равновероятной суперпозиции (применили $H^{\otimes n+1}$).
- Пусть $|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x'' |x\rangle$, $|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum_x' |x\rangle$, тогда $|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$.
- Обозначим $cos(\frac{\theta}{2}) = \sqrt{\frac{N-M}{N}}$, тогда $|\psi\rangle = cos(\frac{\theta}{2}) |\alpha\rangle + sin(\frac{\theta}{2}) |\beta\rangle$, вероятность получить в результате измерения кубитов какое-либо из M возможных решений равна $sin^2(\frac{\theta}{2})$.
- После k итераций Гровера получим состояние

$$G^k |\psi\rangle = cos\left(\frac{2k+1}{2}\theta\right) |\alpha\rangle + sin\left(\frac{2k+1}{2}\theta\right) |\beta\rangle .$$

- После $k = \left[\frac{\pi}{4}\sqrt{\frac{N}{M}}\right]$ итераций Гровера и измерения кубитов с высокой вероятностью получим какое-то из M решений.

Квантовые алгоритмы в криптографических задачах

1. поиск ключа по парам блоков открытого и шифрованного текста;
2. квантовый метод согласования;
3. квантовый метод связанных ключей;
4. поиск ключей FX-конструкций, сетей Фейстеля;
5. квантовый линейный и разностный методы: поиск соотношений, восстановление ключа;
6. поиск коллизий и второго прообраза криптографических хэш-функций;
7. квантовая слайд-атака; применение квантового алгоритма Саймона для схем аутентификации (CBC-MAC, PMAC, GMAC, GCM и OCB);
8. решение СЛУ, алгебраическая атака на AES, Trivium, SHA-3, MPKC (HHL).

Квантовые алгоритмы в криптографических задачах

1. поиск ключа по парам блоков открытого и шифрованного текста;
2. квантовый метод согласования;
3. квантовый метод связанных ключей;
4. поиск ключей FX-конструкций, сетей Фейстеля;
5. квантовый линейный и разностный методы: поиск соотношений, восстановление ключа;
6. поиск коллизий и второго прообраза криптографических хэш-функций;
7. квантовая слайд-атака; применение квантового алгоритма Саймона для схем аутентификации (CBC-MAC, PMAC, GMAC, GCM и OCB);
8. решение СЛУ, алгебраическая атака на AES, Trivium, SHA-3, MPKC (HHL).

Квантовые алгоритмы в криптографических задачах

1. поиск ключа по парам блоков открытого и шифрованного текста;
2. квантовый метод согласования;
3. квантовый метод связанных ключей;
4. поиск ключей FX-конструкций, сетей Фейстеля;
5. квантовый линейный и разностный методы: поиск соотношений, восстановление ключа;
6. поиск коллизий и второго прообраза криптографических хэш-функций;
7. квантовая слайд-атака; применение квантового алгоритма Саймона для схем аутентификации (CBC-MAC, PMAC, GMAC, GCM и OCB);
8. решение СЛУ, алгебраическая атака на AES, Trivium, SHA-3, MPKC (HHL).

Квантовые алгоритмы в криптографических задачах

1. поиск ключа по парам блоков открытого и шифрованного текста;
2. квантовый метод согласования;
3. квантовый метод связанных ключей;
4. поиск ключей FX-конструкций, сетей Фейстеля;
5. квантовый линейный и разностный методы: поиск соотношений, восстановление ключа;
6. поиск коллизий и второго прообраза криптографических хэш-функций;
7. квантовая слайд-атака; применение квантового алгоритма Саймона для схем аутентификации (CBC-MAC, PMAC, GMAC, GCM и OCB);
8. решение СЛУ, алгебраическая атака на AES, Trivium, SHA-3, MPKC (HHL).

Квантовые алгоритмы в криптографических задачах

1. поиск ключа по парам блоков открытого и шифрованного текста;
2. квантовый метод согласования;
3. квантовый метод связанных ключей;
4. поиск ключей FX-конструкций, сетей Фейстеля;
5. квантовый линейный и разностный методы: поиск соотношений, восстановление ключа;
6. поиск коллизий и второго прообраза криптографических хэш-функций;
7. квантовая слайд-атака; применение квантового алгоритма Саймона для схем аутентификации (CBC-MAC, PMAC, GMAC, GCM и OCB);
8. решение СЛУ, алгебраическая атака на AES, Trivium, SHA-3, MPKC (HHL).

Квантовые алгоритмы в криптографических задачах

1. поиск ключа по парам блоков открытого и шифрованного текста;
2. квантовый метод согласования;
3. квантовый метод связанных ключей;
4. поиск ключей FX-конструкций, сетей Фейстеля;
5. квантовый линейный и разностный методы: поиск соотношений, восстановление ключа;
6. поиск коллизий и второго прообраза криптографических хэш-функций;
7. квантовая слайд-атака; применение квантового алгоритма Саймона для схем аутентификации (CBC-MAC, PMAC, GMAC, GCM и OCB);
8. решение СЛУ, алгебраическая атака на AES, Trivium, SHA-3, MPKC (HHL).

Квантовые алгоритмы в криптографических задачах

1. поиск ключа по парам блоков открытого и шифрованного текста;
2. квантовый метод согласования;
3. квантовый метод связанных ключей;
4. поиск ключей FX-конструкций, сетей Фейстеля;
5. квантовый линейный и разностный методы: поиск соотношений, восстановление ключа;
6. поиск коллизий и второго прообраза криптографических хэш-функций;
7. квантовая слайд-атака; применение квантового алгоритма Саймона для схем аутентификации (CBC-MAC, PMAC, GMAC, GCM и OCB);
8. решение СЛУ, алгебраическая атака на AES, Trivium, SHA-3, MPKC (HHL).

Квантовые алгоритмы в криптографических задачах

1. поиск ключа по парам блоков открытого и шифрованного текста;
2. квантовый метод согласования;
3. квантовый метод связанных ключей;
4. поиск ключей FX-конструкций, сетей Фейстеля;
5. квантовый линейный и разностный методы: поиск соотношений, восстановление ключа;
6. поиск коллизий и второго прообраза криптографических хэш-функций;
7. квантовая слайд-атака; применение квантового алгоритма Саймона для схем аутентификации (CBC-MAC, PMAC, GMAC, GCM и OCB);
8. решение СЛУ, алгебраическая атака на AES, Trivium, SHA-3, MPKC (HHL).

Квантовые алгоритмы в криптографических задачах

Полный перебор ключей алгоритмов шифрования	Алгоритм Гровера	[5], [6], [7], [8], [9], [10]
Слайд-атака, метод различения для режимов CBC-MAC, PMAC, GMAC, GCM, OCB, сетей Фейстеля; связанные ключи	Алгоритм Саймона	[11], [12], [13], [14], [15], [16]
Определение ключа схемы Эвана-Мансура, FX-конструкции, обобщенных сетей Фейстеля	Комбинация алгоритма Гровера и Саймона	[17], [18], [19], [20]
Метод согласования, Meet-in-the-Middle Attack	Случайные блуждания, комбинация алгоритма Гровера и Саймона	[21], [22], [23]
Факторизация и дискретное логарифмирование	Алгоритм Шора, алгоритм Экера (Martin Ekera)	[24], [25]
Поиск линейных и разностных соотношений, восстановление ключа по разностному соотношению	Алгоритм Бернштейна-Вазирани, Саймона, Гровера	[26], [27], [28], [29], [30]
Специальные методы	Алгоритм Гровера	[31], [32]
Поиск коллизий, мультиколлизий	Случайные блуждания, Гровер и др.	[33], [34], [37], [38], [39], [40], [41], [42]
Решение СЛУ, алгебраическая атака AES, Trivium, SHA-3, MPKC	Harrow, Hassidim, Lloyd	[43], [44] ,[45]

1.Квантовый метод «полного перебора»

Для поиска ключа $k \in V_n$ симметричного алгоритма шифрования с длиной блока m бит $E : V_n \times V_m \to V_m$ по известным парам блоков о.т. и ш.т. требуется $O(\sqrt{2^n})$ итераций алгоритма Гровера.

В каком-то смысле длина ключа сокращается в два раза!

Поиск 256-битового ключа осуществляется за $O(2^{128})$ итераций Гровера.

2.Квантовый метод согласования. Попытка увеличить длину ключа №1.

При использовании композиции блочных шифров с независимыми ключами трудоемкость восстановления ключа увеличивается, но не так сильно, как ожидается (см. [21]).

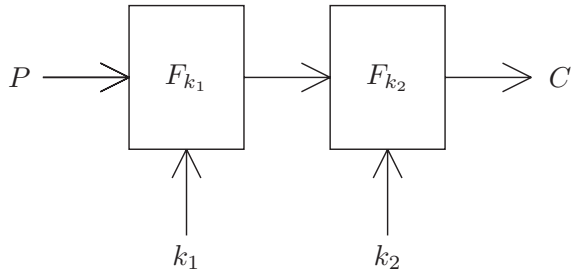


Рис. 8: Трудоемкость восстановления $(K_1, K_2) \in V_{2n}$ квантовым методом согласования составляет $O(2^{2n/3})$, меньше, чем $O(2^n)$, однако требуется память (кубиты) порядка $O(2^{2n/3})$.

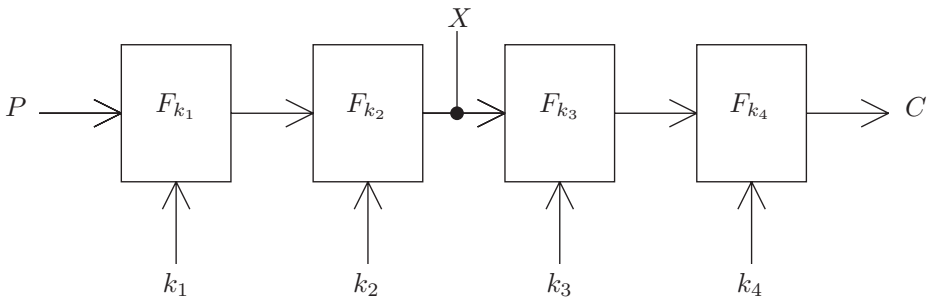


Рис. 9: Трудоемкость восстановления $(K_1, K_2, K_3, K_4) \in V_{4n}$ составляет $O(2^{7n/6})$ квантовых операций, тогда как трудоемкость поиска $(K_1, K_2, K_3, K_4) \in V_{4n}$ алгоритмом Гровера составляет $O(2^{2n})$. Требуется память (кубиты) порядка $O(2^{2n/3})$.

3.Квантовый метод связанных ключей

Методы связанных ключей предполагают наличие у криптоаналитика блоков открытого и шифрованного текста на специально подобранных аналитиком ключах, связанных некоторой зависимостью с искомым секретным ключом.

Предполагается выполнение следующих условий:

- Блочный шифр $E : V_n \times V_m \to V_m$ может быть эффективно реализован в виде квантовых схем.
- Для однозначного определения секретного ключа достаточно небольшого количества пар блоков (о.т., ш.т.) (расстояние единственности блочного шифра невелико).
- Криптоаналитик имеет доступ к оракулу E, который для $s, K \in V_n$ и $P \in V_m$ возвращает результат зашифрования $E(s \oplus K, P)$, s – искомый секретный ключ, на котором $C = E_s(P)$. Пространство всех возможных ключей описывается системой из n кубитов.

Методы связанных ключей предполагают наличие у криптоаналитика блоков открытого и шифрованного текста на специально подобранных аналитиком ключах, связанных некоторой зависимостью с искомым секретным ключом.

Предполагается выполнение следующих условий:

- Блочный шифр $E : V_n \times V_m \to V_m$ может быть эффективно реализован в виде квантовых схем.
- Для однозначного определения секретного ключа достаточно небольшого количества пар блоков (о.т., ш.т.) (расстояние единственности блочного шифра невелико).
- Криптоаналитик имеет доступ к оракулу E, который для $s, K \in V_n$ и $P \in V_m$ возвращает результат зашифрования $E(s \oplus K, P)$, s – искомый секретный ключ, на котором $C = E_s(P)$. Пространство всех возможных ключей описывается системой из n кубитов.

Методы связанных ключей предполагают наличие у криптоаналитика блоков открытого и шифрованного текста на специально подобранных аналитиком ключах, связанных некоторой зависимостью с искомым секретным ключом.

Предполагается выполнение следующих условий:

- Блочный шифр $E : V_n \times V_m \to V_m$ может быть эффективно реализован в виде квантовых схем.
- Для однозначного определения секретного ключа достаточно небольшого количества пар блоков (о.т., ш.т.) (расстояние единственности блочного шифра невелико).
- Криптоаналитик имеет доступ к оракулу E, который для $s, K \in V_n$ и $P \in V_m$ возвращает результат зашифрования $E(s \oplus K, P)$, s – искомый секретный ключ, на котором $C = E_s(P)$. Пространство всех возможных ключей описывается системой из n кубитов.

- Пусть $\overrightarrow{P} = (P_1, \dots P_r)$ – r блоков открытого текста, r – расстояние единственности рассматриваемого блочного шифра.
- Каждому ключу $K \in V_n$ ставим в соответствие множество из двух шифртекстов

$$\left\{E(K, \overrightarrow{P}), E(s \oplus K, \overrightarrow{P})\right\} \subset V_{2mr}.$$

- Образы $E(K, \overrightarrow{P})$ и $E(s \oplus K, \overrightarrow{P})$ интерпретируются как два целых числа без знака (unsigned integers).
- Для фиксированного неизвестного ключа s определим отображение

$$f_s : x \mapsto \left(\min\left\{E(K, \overrightarrow{P}), E(s \oplus K, \overrightarrow{P})\right\}, \max\left\{E(K, \overrightarrow{P}), E(s \oplus K, \overrightarrow{P})\right\}\right).$$

- Решив задачу Саймона для отображения f_s на квантовом компьютере можно восстановить секретный ключ s блочного шифра с полиномиальной трудоемкостью, тогда как трудоемкость восстановления n-битного ключа с помощью квантового алгоритма Гровера $O(2^{n/2})$ итераций Гровера.

- Пусть $\overrightarrow{P} = (P_1, \dots P_r)$ – r блоков открытого текста, r – расстояние единственности рассматриваемого блочного шифра.
- Каждому ключу $K \in V_n$ ставим в соответствие множество из двух шифртекстов

$$\left\{E(K, \overrightarrow{P}), E(s \oplus K, \overrightarrow{P})\right\} \subset V_{2mr}.$$

- Образы $E(K, \overrightarrow{P})$ и $E(s \oplus K, \overrightarrow{P})$ интерпретируются как два целых числа без знака (unsigned integers).
- Для фиксированного неизвестного ключа s определим отображение

$$f_s : x \mapsto \left(\min\left\{E(K, \overrightarrow{P}), E(s \oplus K, \overrightarrow{P})\right\}, \max\left\{E(K, \overrightarrow{P}), E(s \oplus K, \overrightarrow{P})\right\}\right).$$

- Решив задачу Саймона для отображения f_s на квантовом компьютере можно восстановить секретный ключ s блочного шифра с полиномиальной трудоемкостью, тогда как трудоемкость восстановления n-битного ключа с помощью квантового алгоритма Гровера $O(2^{n/2})$ итераций Гровера.

- Пусть $\overrightarrow{P} = (P_1, \dots P_r)$ – r блоков открытого текста, r – расстояние единственности рассматриваемого блочного шифра.
- Каждому ключу $K \in V_n$ ставим в соответствие множество из двух шифртекстов

$$\left\{E(K, \overrightarrow{P}), E(s \oplus K, \overrightarrow{P})\right\} \subset V_{2mr}.$$

- Образы $E(K, \overrightarrow{P})$ и $E(s \oplus K, \overrightarrow{P})$ интерпретируются как два целых числа без знака (unsigned integers).
- Для фиксированного неизвестного ключа s определим отображение

$$f_s : x \mapsto \left(\min\left\{E(K, \overrightarrow{P}), E(s \oplus K, \overrightarrow{P})\right\}, \max\left\{E(K, \overrightarrow{P}), E(s \oplus K, \overrightarrow{P})\right\}\right).$$

- Решив задачу Саймона для отображения f_s на квантовом компьютере можно восстановить секретный ключ s блочного шифра с полиномиальной трудоемкостью, тогда как трудоемкость восстановления n-битного ключа с помощью квантового алгоритма Гровера $O(2^{n/2})$ итераций Гровера.

- Пусть $\overrightarrow{P} = (P_1, \dots P_r)$ – r блоков открытого текста, r – расстояние единственности рассматриваемого блочного шифра.
- Каждому ключу $K \in V_n$ ставим в соответствие множество из двух шифртекстов

$$\left\{E(K, \overrightarrow{P}), E(s \oplus K, \overrightarrow{P})\right\} \subset V_{2mr}.$$

- Образы $E(K, \overrightarrow{P})$ и $E(s \oplus K, \overrightarrow{P})$ интерпретируются как два целых числа без знака (unsigned integers).
- Для фиксированного неизвестного ключа s определим отображение

$$f_s : x \mapsto \left(\min\left\{E(K, \overrightarrow{P}), E(s \oplus K, \overrightarrow{P})\right\}, \max\left\{E(K, \overrightarrow{P}), E(s \oplus K, \overrightarrow{P})\right\}\right).$$

- Решив задачу Саймона для отображения f_s на квантовом компьютере можно восстановить секретный ключ s блочного шифра с полиномиальной трудоемкостью, тогда как трудоемкость восстановления n-битного ключа с помощью квантового алгоритма Гровера $O(2^{n/2})$ итераций Гровера.

- Пусть $\overrightarrow{P} = (P_1, \dots P_r)$ – r блоков открытого текста, r – расстояние единственности рассматриваемого блочного шифра.
- Каждому ключу $K \in V_n$ ставим в соответствие множество из двух шифртекстов

$$\left\{E(K, \overrightarrow{P}), E(s \oplus K, \overrightarrow{P})\right\} \subset V_{2mr}.$$

- Образы $E(K, \overrightarrow{P})$ и $E(s \oplus K, \overrightarrow{P})$ интерпретируются как два целых числа без знака (unsigned integers).
- Для фиксированного неизвестного ключа s определим отображение

$$f_s : x \mapsto \left(\min\left\{E(K, \overrightarrow{P}), E(s \oplus K, \overrightarrow{P})\right\}, \max\left\{E(K, \overrightarrow{P}), E(s \oplus K, \overrightarrow{P})\right\}\right).$$

- Решив задачу Саймона для отображения f_s на квантовом компьютере можно восстановить секретный ключ s блочного шифра с полиномиальной трудоемкостью, тогда как трудоемкость восстановления n-битного ключа с помощью квантового алгоритма Гровера $O(2^{n/2})$ итераций Гровера.

4.Квантовый метод восстановления ключа схемы Эвана-Мансура.

- В 1997 году предложена схема $E : V_n \times V_n \times V_n \to V_n$;
- $E(m) = c$, m – блок открытого текста, c – блок зашифрованного текста;
- k_1, k_2 – секретные ключи;
- P – известная подстановка;

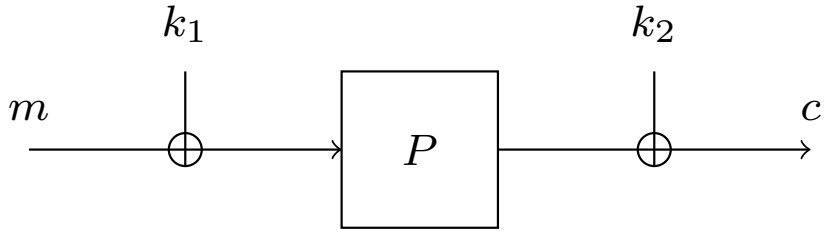


Рис. 10: Схема Эвана-Мансура.

Рассматривается функция

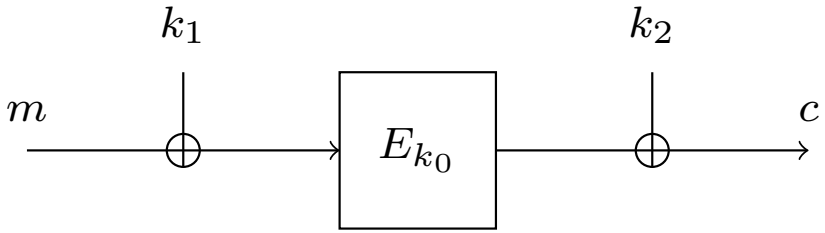
$$f(x) = P(x \oplus k_1) \oplus k_2 \oplus P(x),$$

для которой на всех $x \in V_n$ выполняется равенство $f(x) = f(x \oplus k_1)$.

- Для поиска неизвестного ключа k_1 применим квантовый алгоритм Саймона.
- После определения k_1 по известным парам (о.т., ш.т.) легко восстанавливается k_2.

4.Квантовый метод восстановления ключа FX-конструкций. Попытка увеличить длину ключа №2.

- FX-конструкция – обобщение схемы Эвана-Мансура;
- $Enc : V_t \times V_n \times V_n \times V_n \to V_n$.
- $Enc(x) = E_{k_0}(x \oplus k_1) \oplus k_2$, где $E : V_t \times V_n \to V_n$ – некоторый блочный шифр.



Алгоритм Саймона в чистом виде неприменим, в работе [17] представлен алгоритм восстановления (k_0, k_1, k_2):

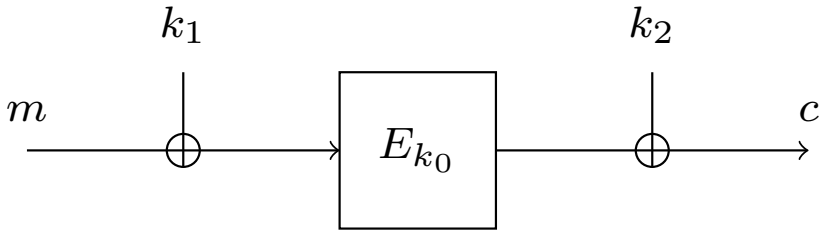
- трудоемкость $2^{t/2}O(a+n)$ квантовых операций;
- вероятность успеха не менее $\frac{2}{5}$;
- требуется не менее $t + 4n(n + \sqrt{n})$ кубитов.

Основная идея – применение комбинации алгоритмов Гровера и Саймона: для поиска ключа k_0 требуется $O(2^{t/2})$ итераций Гровера, в каждой из которых применяется алгоритм Саймона для поиска k_1. После измерения кубитов определяются k_0 и k_1, затем восстанавливается ключ k_2.

Трудоемкость поиска ключа $(k_0, k_1, k_2) \in V_{t+2n}$ сравнима с трудоемкостью восстановления ключа $k_0 \in V_t$ блочного шифра $E : V_t \times V_n \to V_n$ с помощью алгоритма Гровера, $O(2^{t/2})$.

4.Квантовый метод восстановления ключа FX-конструкций. Попытка увеличить длину ключа №2.

- FX-конструкция – обобщение схемы Эвана-Мансура;
- $Enc : V_t \times V_n \times V_n \times V_n \to V_n$.
- $Enc(x) = E_{k_0}(x \oplus k_1) \oplus k_2$, где $E : V_t \times V_n \to V_n$ – некоторый блочный шифр.



Алгоритм Саймона в чистом виде неприменим, в работе [17] представлен алгоритм восстановления (k_0, k_1, k_2):

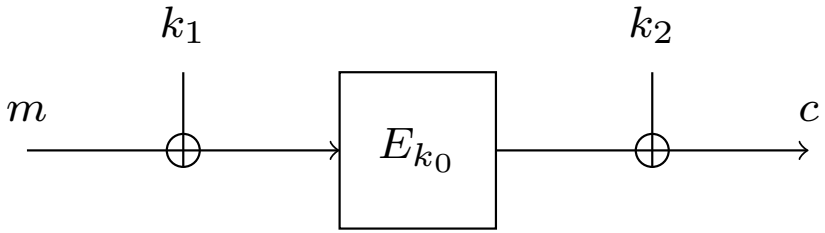
- трудоемкость $2^{t/2}O(a+n)$ квантовых операций;
- вероятность успеха не менее $\frac{2}{5}$;
- требуется не менее $t + 4n(n + \sqrt{n})$ кубитов.

Основная идея – применение комбинации алгоритмов Гровера и Саймона: для поиска ключа k_0 требуется $O(2^{t/2})$ итераций Гровера, в каждой из которых применяется алгоритм Саймона для поиска k_1. После измерения кубитов определяются k_0 и k_1, затем восстанавливается ключ k_2.

Трудоемкость поиска ключа $(k_0, k_1, k_2) \in V_{t+2n}$ сравнима с трудоемкостью восстановления ключа $k_0 \in V_t$ блочного шифра $E : V_t \times V_n \to V_n$ с помощью алгоритма Гровера, $O(2^{t/2})$.

4.Квантовый метод восстановления ключа FX-конструкций. Попытка увеличить длину ключа №2.

- FX-конструкция – обобщение схемы Эвана-Мансура;
- $Enc : V_t \times V_n \times V_n \times V_n \to V_n$.
- $Enc(x) = E_{k_0}(x \oplus k_1) \oplus k_2$, где $E : V_t \times V_n \to V_n$ – некоторый блочный шифр.



Алгоритм Саймона в чистом виде неприменим, в работе [17] представлен алгоритм восстановления (k_0, k_1, k_2):

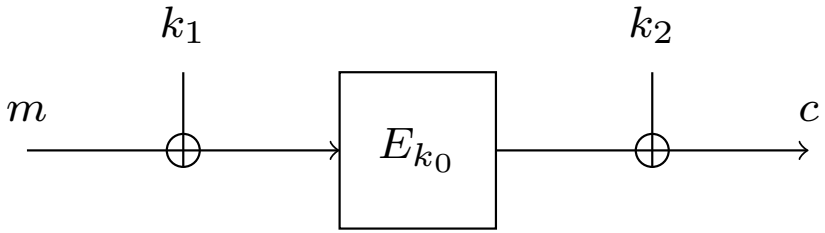
- трудоемкость $2^{t/2}O(a+n)$ квантовых операций;
- вероятность успеха не менее $\frac{2}{5}$;
- требуется не менее $t + 4n(n + \sqrt{n})$ кубитов.

Основная идея – применение комбинации алгоритмов Гровера и Саймона: для поиска ключа k_0 требуется $O(2^{t/2})$ итераций Гровера, в каждой из которых применяется алгоритм Саймона для поиска k_1. После измерения кубитов определяются k_0 и k_1, затем восстанавливается ключ k_2.

Трудоемкость поиска ключа $(k_0, k_1, k_2) \in V_{t+2n}$ сравнима с трудоемкостью восстановления ключа $k_0 \in V_t$ блочного шифра $E : V_t \times V_n \to V_n$ с помощью алгоритма Гровера, $O(2^{t/2})$.

4.Квантовый метод восстановления ключа FX-конструкций. Попытка увеличить длину ключа №2.

- FX-конструкция – обобщение схемы Эвана-Мансура;
- $Enc : V_t \times V_n \times V_n \times V_n \to V_n$.
- $Enc(x) = E_{k_0}(x \oplus k_1) \oplus k_2$, где $E : V_t \times V_n \to V_n$ – некоторый блочный шифр.



Алгоритм Саймона в чистом виде неприменим, в работе [17] представлен алгоритм восстановления (k_0, k_1, k_2):

- трудоемкость $2^{t/2}O(a+n)$ квантовых операций;
- вероятность успеха не менее $\frac{2}{5}$;
- требуется не менее $t + 4n(n + \sqrt{n})$ кубитов.

Основная идея – применение комбинации алгоритмов Гровера и Саймона: для поиска ключа k_0 требуется $O(2^{t/2})$ итераций Гровера, в каждой из которых применяется алгоритм Саймона для поиска k_1. После измерения кубитов определяются k_0 и k_1, затем восстанавливается ключ k_2.

Трудоемкость поиска ключа $(k_0, k_1, k_2) \in V_{t+2n}$ сравнима с трудоемкостью восстановления ключа $k_0 \in V_t$ блочного шифра $E : V_t \times V_n \to V_n$ с помощью алгоритма Гровера, $O(2^{t/2})$.

4.Восстановление итерационных ключей сети Фейстеля, см. [18].

В работе [18] рассмотрено применение комбинации квантовых алгоритмов Саймона и Гровера для восстановления ключей пяти итераций сети Фейстеля $E : V_n \to V_n$ с раундовыми ключами $k_i \in V_{n/2},\ i = 1, 2, ..., 5$.

- Рассматривается отображение $f : V_{n/2+1} \to V_{n/2}$,

  $$f(b, x_{R_0}) = F_2(k_2, x_{R_0} \oplus F_1(k_1, a_b)) = a_b \oplus x_{R_3} = a_b \oplus F_4(k_4, F_5(k_5, x_{R_5}) \oplus x_{L_5}) \oplus x_{R_5},$$

  где $b \in \{0, 1\},\ a_0, a_1$ - случайные константы из $V_{n/2}$, $(x_{L_5} \| x_{R_5}) = Enc(a_b \| x_{R_0})$.
- Утверждается, что для правильной пары (k_4, k_5)

  $$f(b, x_{R_0}) = f(b \oplus 1, x_{R_0} \oplus F_1(k_1, a_0) \oplus F_1(k_1, a_1)),$$

  т.е. у $f(b, x_{R_0}) = a_b \oplus F_4(k_4, F_5(k_5, x_{R_5}) \oplus x_{L_5})$ существует нетривиальный период $s = 1 || F_1(k_1, a_0) \oplus F_1(k_1, a_1)$, для поиска которого применим алгоритм Саймона.
- Относительно специального классификатора $B : V_{n+(n/2+1)l} \to \{0, 1\}$ применяется алгоритм Гровера, после $2^{n/2}$ итераций Гровера с высокой вероятностью определяются истинные (k_4, k_5).
- Для применения метода требуется $n + (n + 1)(n + 2 + 2\sqrt{n/2 + 1})$ кубитов и порядка $O(2^{n/2})$ квантовых запросов.
- При $r > 5$ раундов, трудоемкость восстановления r независимых итерационных ключей $O(2^{nr/4 - 3n/4})$ квантовых запросов ($O(2^{1.25n})$ при $r = 8$, $O(2^{7.25n})$ при $r = 32$).

4.Восстановление итерационных ключей сети Фейстеля, см. [18].

В работе [18] рассмотрено применение комбинации квантовых алгоритмов Саймона и Гровера для восстановления ключей пяти итераций сети Фейстеля $E : V_n \to V_n$ с раундовыми ключами $k_i \in V_{n/2},\ i = 1, 2, ..., 5$.

- Рассматривается отображение $f : V_{n/2+1} \to V_{n/2}$,

  $f(b, x_{R_0}) = F_2(k_2, x_{R_0} \oplus F_1(k_1, a_b)) = a_b \oplus x_{R_3} = a_b \oplus F_4(k_4, F_5(k_5, x_{R_5}) \oplus x_{L_5}) \oplus x_{R_5}$,

  где $b \in \{0, 1\},\ a_0, a_1$ - случайные константы из $V_{n/2}$, $(x_{L_5} \| x_{R_5}) = Enc(a_b \| x_{R_0})$.
- Утверждается, что для правильной пары (k_4, k_5)

  $$f(b, x_{R_0}) = f(b \oplus 1, x_{R_0} \oplus F_1(k_1, a_0) \oplus F_1(k_1, a_1)),$$

  т.е. у $f(b, x_{R_0}) = a_b \oplus F_4(k_4, F_5(k_5, x_{R_5}) \oplus x_{L_5})$ существует нетривиальный период $s = 1 || F_1(k_1, a_0) \oplus F_1(k_1, a_1)$, для поиска которого применим алгоритм Саймона.
- Относительно специального классификатора $B : V_{n+(n/2+1)l} \to \{0, 1\}$ применяется алгоритм Гровера, после $2^{n/2}$ итераций Гровера с высокой вероятностью определяются истинные (k_4, k_5).
- Для применения метода требуется $n + (n + 1)(n + 2 + 2\sqrt{n/2 + 1})$ кубитов и порядка $O(2^{n/2})$ квантовых запросов.
- При $r > 5$ раундов, трудоемкость восстановления r независимых итерационных ключей $O(2^{nr/4 - 3n/4})$ квантовых запросов ($O(2^{1.25n})$ при $r = 8$, $O(2^{7.25n})$ при $r = 32$).

4.Восстановление итерационных ключей сети Фейстеля, см. [18].

В работе [18] рассмотрено применение комбинации квантовых алгоритмов Саймона и Гровера для восстановления ключей пяти итераций сети Фейстеля $E : V_n \to V_n$ с раундовыми ключами $k_i \in V_{n/2},\ i = 1, 2, ..., 5$.

- Рассматривается отображение $f : V_{n/2+1} \to V_{n/2}$,

$$f(b, x_{R_0}) = F_2(k_2, x_{R_0} \oplus F_1(k_1, a_b)) = a_b \oplus x_{R_3} = a_b \oplus F_4(k_4, F_5(k_5, x_{R_5}) \oplus x_{L_5}) \oplus x_{R_5},$$

где $b \in \{0, 1\},\ a_0, a_1$ - случайные константы из $V_{n/2}$, $(x_{L_5} \| x_{R_5}) = Enc(a_b \| x_{R_0})$.

- Утверждается, что для правильной пары (k_4, k_5)

$$f(b, x_{R_0}) = f(b \oplus 1, x_{R_0} \oplus F_1(k_1, a_0) \oplus F_1(k_1, a_1)),$$

т.е. у $f(b, x_{R_0}) = a_b \oplus F_4(k_4, F_5(k_5, x_{R_5}) \oplus x_{L_5})$ существует нетривиальный период $s = 1 || F_1(k_1, a_0) \oplus F_1(k_1, a_1)$, для поиска которого применим алгоритм Саймона.

- Относительно специального классификатора $B : V_{n+(n/2+1)l} \to \{0, 1\}$ применяется алгоритм Гровера, после $2^{n/2}$ итераций Гровера с высокой вероятностью определяются истинные (k_4, k_5).
- Для применения метода требуется $n + (n + 1)(n + 2 + 2\sqrt{n/2 + 1})$ кубитов и порядка $O(2^{n/2})$ квантовых запросов.
- При $r > 5$ раундов, трудоемкость восстановления r независимых итерационных ключей $O(2^{nr/4 - 3n/4})$ квантовых запросов ($O(2^{1.25n})$ при $r = 8$, $O(2^{7.25n})$ при $r = 32$).

4.Восстановление итерационных ключей сети Фейстеля, см. [18].

В работе [18] рассмотрено применение комбинации квантовых алгоритмов Саймона и Гровера для восстановления ключей пяти итераций сети Фейстеля $E : V_n \to V_n$ с раундовыми ключами $k_i \in V_{n/2},\ i = 1, 2, ..., 5$.

- Рассматривается отображение $f : V_{n/2+1} \to V_{n/2}$,

  $$f(b, x_{R_0}) = F_2(k_2, x_{R_0} \oplus F_1(k_1, a_b)) = a_b \oplus x_{R_3} = a_b \oplus F_4(k_4, F_5(k_5, x_{R_5}) \oplus x_{L_5}) \oplus x_{R_5},$$

  где $b \in \{0, 1\},\ a_0, a_1$ - случайные константы из $V_{n/2}$, $(x_{L_5} \| x_{R_5}) = Enc(a_b \| x_{R_0})$.
- Утверждается, что для правильной пары (k_4, k_5)

  $$f(b, x_{R_0}) = f(b \oplus 1, x_{R_0} \oplus F_1(k_1, a_0) \oplus F_1(k_1, a_1)),$$

  т.е. у $f(b, x_{R_0}) = a_b \oplus F_4(k_4, F_5(k_5, x_{R_5}) \oplus x_{L_5})$ существует нетривиальный период $s = 1 || F_1(k_1, a_0) \oplus F_1(k_1, a_1)$, для поиска которого применим алгоритм Саймона.
- Относительно специального классификатора $B : V_{n+(n/2+1)l} \to \{0, 1\}$ применяется алгоритм Гровера, после $2^{n/2}$ итераций Гровера с высокой вероятностью определяются истинные (k_4, k_5).
- Для применения метода требуется $n + (n + 1)(n + 2 + 2\sqrt{n/2 + 1})$ кубитов и порядка $O(2^{n/2})$ квантовых запросов.
- При $r > 5$ раундов, трудоемкость восстановления r независимых итерационных ключей $O(2^{nr/4 - 3n/4})$ квантовых запросов ($O(2^{1.25n})$ при $r = 8$, $O(2^{7.25n})$ при $r = 32$).

4.Восстановление итерационных ключей сети Фейстеля, см. [18].

В работе [18] рассмотрено применение комбинации квантовых алгоритмов Саймона и Гровера для восстановления ключей пяти итераций сети Фейстеля $E : V_n \to V_n$ с раундовыми ключами $k_i \in V_{n/2},\ i = 1, 2, ..., 5$.

- Рассматривается отображение $f : V_{n/2+1} \to V_{n/2}$,

  $$f(b, x_{R_0}) = F_2(k_2, x_{R_0} \oplus F_1(k_1, a_b)) = a_b \oplus x_{R_3} = a_b \oplus F_4(k_4, F_5(k_5, x_{R_5}) \oplus x_{L_5}) \oplus x_{R_5},$$

  где $b \in \{0, 1\},\ a_0, a_1$ - случайные константы из $V_{n/2}$, $(x_{L_5} \| x_{R_5}) = Enc(a_b \| x_{R_0})$.
- Утверждается, что для правильной пары (k_4, k_5)

  $$f(b, x_{R_0}) = f(b \oplus 1, x_{R_0} \oplus F_1(k_1, a_0) \oplus F_1(k_1, a_1)),$$

  т.е. у $f(b, x_{R_0}) = a_b \oplus F_4(k_4, F_5(k_5, x_{R_5}) \oplus x_{L_5})$ существует нетривиальный период $s = 1 || F_1(k_1, a_0) \oplus F_1(k_1, a_1)$, для поиска которого применим алгоритм Саймона.
- Относительно специального классификатора $B : V_{n+(n/2+1)l} \to \{0, 1\}$ применяется алгоритм Гровера, после $2^{n/2}$ итераций Гровера с высокой вероятностью определяются истинные (k_4, k_5).
- Для применения метода требуется $n + (n + 1)(n + 2 + 2\sqrt{n/2 + 1})$ кубитов и порядка $O(2^{n/2})$ квантовых запросов.
- При $r > 5$ раундов, трудоемкость восстановления r независимых итерационных ключей $O(2^{nr/4 - 3n/4})$ квантовых запросов ($O(2^{1.25n})$ при $r = 8$, $O(2^{7.25n})$ при $r = 32$).

4.Восстановление итерационных ключей сети Фейстеля, см. [18].

В работе [18] рассмотрено применение комбинации квантовых алгоритмов Саймона и Гровера для восстановления ключей пяти итераций сети Фейстеля $E : V_n \to V_n$ с раундовыми ключами $k_i \in V_{n/2},\ i = 1, 2, ..., 5$.

- Рассматривается отображение $f : V_{n/2+1} \to V_{n/2}$,

  $$f(b, x_{R_0}) = F_2(k_2, x_{R_0} \oplus F_1(k_1, a_b)) = a_b \oplus x_{R_3} = a_b \oplus F_4(k_4, F_5(k_5, x_{R_5}) \oplus x_{L_5}) \oplus x_{R_5},$$

  где $b \in \{0, 1\},\ a_0, a_1$ - случайные константы из $V_{n/2}$, $(x_{L_5} \| x_{R_5}) = Enc(a_b \| x_{R_0})$.
- Утверждается, что для правильной пары (k_4, k_5)

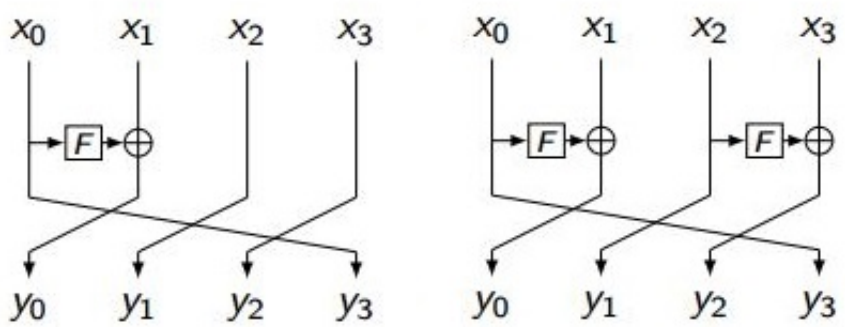
  $$f(b, x_{R_0}) = f(b \oplus 1, x_{R_0} \oplus F_1(k_1, a_0) \oplus F_1(k_1, a_1)),$$

  т.е. у $f(b, x_{R_0}) = a_b \oplus F_4(k_4, F_5(k_5, x_{R_5}) \oplus x_{L_5})$ существует нетривиальный период $s = 1 || F_1(k_1, a_0) \oplus F_1(k_1, a_1)$, для поиска которого применим алгоритм Саймона.
- Относительно специального классификатора $B : V_{n+(n/2+1)l} \to \{0, 1\}$ применяется алгоритм Гровера, после $2^{n/2}$ итераций Гровера с высокой вероятностью определяются истинные (k_4, k_5).
- Для применения метода требуется $n + (n + 1)(n + 2 + 2\sqrt{n/2 + 1})$ кубитов и порядка $O(2^{n/2})$ квантовых запросов.
- При $r > 5$ раундов, трудоемкость восстановления r независимых итерационных ключей $O(2^{nr/4 - 3n/4})$ квантовых запросов ($O(2^{1.25n})$ при $r = 8$, $O(2^{7.25n})$ при $r = 32$).

Для d-branch Type-1 GFS (CAST256-like Feistel structure)

Построен квантовый различитель на $2d-1$-раундов. Например (рисунок слева), при $d=4$ различитель на $2\cdot 4-1=7$ раундов строим по

$$F(x)=f^4(f^3(f^2(f^1(x_1^0)\oplus x_2^0)\oplus x_2^0)\oplus x_2^0\oplus x)$$



Для 2d-branch Type-2 GFS (RC6/CLEFIA-like Feistel structure)

Построен квантовый различитель на $2d+1$-раундов. Например (рисунок справа), при $d=2$ различитель на $2\cdot 2+1=5$ раундов строим по

$$F(x)=f^4(f^3(f^2(f^1(x_1^0)\oplus x)\oplus x_3^0)\oplus f^2(x_3^0)\oplus x_4^0)$$

Для восстановления ключа применяется комбинация алгоритмов Саймона и Гровера.

4.Квантовые различители для сетей Фейстеля, см. [20].

В [20] описан алгоритм различения сетей Фейстеля от случайной подстановки, в основе которого лежит квантовый алгоритм Саймона, но не предъявляющий период в явном виде. Трудоемкость алгоритма – полиномиальна.

Обозначим $(a_i, b_i) \in V_{n/2} \times V_{n/2}$ - состояние очередного шифруемого блока после i-ой итерации зашифрования некоторой сети Фейстеля:

Схема	Преобразование полублоков	Кол-во итераций	Сложность восстановления ключей r-раундов
$Feistel - F$	$b_{i+1} \leftarrow a_i \oplus F_{K_i}(b_i),\ a_{i+1} \leftarrow b_i$	4	$O(2^{(r-5)n/4})$
$Feistel - KF$	$b_{i+1} \leftarrow a_i \oplus F(K_i \oplus b_i),\ a_{i+1} \leftarrow b_i$	4	$O(2^{(r-4)n/4})$
$Feistel - FK$	$b_{i+1} \leftarrow a_i \oplus F(b_i) \oplus K_i,\ a_{i+1} \leftarrow b_i$	6	$O(2^{(r-6)n/4})$

Таблица 1: Типовые сети Фейстеля, см. [20].

4.Квантовые различители для сетей Фейстеля, см. [20].

В [20] описан алгоритм различения сетей Фейстеля от случайной подстановки, в основе которого лежит квантовый алгоритм Саймона, но не предъявляющий период в явном виде. Трудоемкость алгоритма – полиномиальна.

Обозначим $(a_i, b_i) \in V_{n/2} \times V_{n/2}$ - состояние очередного шифруемого блока после i-ой итерации зашифрования некоторой сети Фейстеля:

Схема	Преобразование полублоков	Кол-во итераций	Сложность восстановления ключей r-раундов
$Feistel - F$	$b_{i+1} \leftarrow a_i \oplus F_{K_i}(b_i),\ a_{i+1} \leftarrow b_i$	4	$O(2^{(r-5)n/4})$
$Feistel - KF$	$b_{i+1} \leftarrow a_i \oplus F(K_i \oplus b_i),\ a_{i+1} \leftarrow b_i$	4	$O(2^{(r-4)n/4})$
$Feistel - FK$	$b_{i+1} \leftarrow a_i \oplus F(b_i) \oplus K_i,\ a_{i+1} \leftarrow b_i$	6	$O(2^{(r-6)n/4})$

Таблица 1: Типовые сети Фейстеля, см. [20].

5.Квантовый разностный и линейный методы. Поиск итерационных ключей по имеющимся разностным соотношениям алгоритмом Гровера.

- Поиск разностных (линейных) соотношений с высокими разностными (линейными) характеристиками с помощью квантового алгоритма Бернштейна-Вазирани (поиск квазилинейных структур булевой функции).
- Для $E : V_n \times V_m \to V_m$, $C = E(key, P)$, известно некоторое разностное соотношение (a, b) с характеристикой $p_{(a,b)}$. Предполагается, что на истинном ключе key:

$$P(E(key, P) \oplus E(key, P \oplus a) = b) = p_{(a,b)},$$

$$p_{(a,b)} = \max_{a,b \in V_m \setminus \overrightarrow{0}} p_{(a,b)}.$$

- Известно N пар открытых и шифрованных текстов (P_i, C_i), $i \in \{1, \ldots, N\}$, полученных при шифровании на одном и том же ключе key. Необходимо по заданному разностному (линейному) соотношению (a, b) и имеющемуся материалу восстановить key.
- Согласно [28], трудоёмкость восстановления ключа key на квантовом компьютере составляет $O(\sqrt{N}) + O(2^{n/2})$ (применяется вариант алгоритма Гровера для поиска итерационного ключа, на котором рассматриваемое соотношение выполняется с максимальной вероятностью), в то время как трудоемкость классического разностного метода авторы [28] оценивают величиной $O(N) + O(2^n)$.

5.Квантовый разностный и линейный методы. Поиск итерационных ключей по имеющимся разностным соотношениям алгоритмом Гровера.

- Поиск разностных (линейных) соотношений с высокими разностными (линейными) характеристиками с помощью квантового алгоритма Бернштейна-Вазирани (поиск квазилинейных структур булевой функции).
- Для $E : V_n \times V_m \to V_m$, $C = E(key, P)$, известно некоторое разностное соотношение (a, b) с характеристикой $p_{(a,b)}$. Предполагается, что на истинном ключе key:

$$P(E(key, P) \oplus E(key, P \oplus a) = b) = p_{(a,b)},$$

$$p_{(a,b)} = \max_{a,b \in V_m \setminus \overrightarrow{0}} p_{(a,b)}.$$

- Известно N пар открытых и шифрованных текстов (P_i, C_i), $i \in \{1, \ldots, N\}$, полученных при шифровании на одном и том же ключе key. Необходимо по заданному разностному (линейному) соотношению (a, b) и имеющемуся материалу восстановить key.
- Согласно [28], трудоёмкость восстановления ключа key на квантовом компьютере составляет $O(\sqrt{N}) + O(2^{n/2})$ (применяется вариант алгоритма Гровера для поиска итерационного ключа, на котором рассматриваемое соотношение выполняется с максимальной вероятностью), в то время как трудоемкость классического разностного метода авторы [28] оценивают величиной $O(N) + O(2^n)$.

5.Квантовый разностный и линейный методы. Поиск итерационных ключей по имеющимся разностным соотношениям алгоритмом Гровера.

- Поиск разностных (линейных) соотношений с высокими разностными (линейными) характеристиками с помощью квантового алгоритма Бернштейна-Вазирани (поиск квазилинейных структур булевой функции).
- Для $E : V_n \times V_m \to V_m$, $C = E(key, P)$, известно некоторое разностное соотношение (a, b) с характеристикой $p_{(a,b)}$. Предполагается, что на истинном ключе key:

$$P(E(key, P) \oplus E(key, P \oplus a) = b) = p_{(a,b)},$$

$$p_{(a,b)} = \max_{a,b \in V_m \setminus \overrightarrow{0}} p_{(a,b)}.$$

- Известно N пар открытых и шифрованных текстов (P_i, C_i), $i \in \{1, \ldots, N\}$, полученных при шифровании на одном и том же ключе key. Необходимо по заданному разностному (линейному) соотношению (a, b) и имеющемуся материалу восстановить key.
- Согласно [28], трудоёмкость восстановления ключа key на квантовом компьютере составляет $O(\sqrt{N}) + O(2^{n/2})$ (применяется вариант алгоритма Гровера для поиска итерационного ключа, на котором рассматриваемое соотношение выполняется с максимальной вероятностью), в то время как трудоемкость классического разностного метода авторы [28] оценивают величиной $O(N) + O(2^n)$.

5.Квантовый разностный и линейный методы. Поиск итерационных ключей по имеющимся разностным соотношениям алгоритмом Гровера.

- Поиск разностных (линейных) соотношений с высокими разностными (линейными) характеристиками с помощью квантового алгоритма Бернштейна-Вазирани (поиск квазилинейных структур булевой функции).
- Для $E : V_n \times V_m \to V_m$, $C = E(key, P)$, известно некоторое разностное соотношение (a, b) с характеристикой $p_{(a,b)}$. Предполагается, что на истинном ключе key:

$$P(E(key, P) \oplus E(key, P \oplus a) = b) = p_{(a,b)},$$

$$p_{(a,b)} = \max_{a,b \in V_m \setminus \overrightarrow{0}} p_{(a,b)}.$$

- Известно N пар открытых и шифрованных текстов (P_i, C_i), $i \in \{1, \ldots, N\}$, полученных при шифровании на одном и том же ключе key. Необходимо по заданному разностному (линейному) соотношению (a, b) и имеющемуся материалу восстановить key.
- Согласно [28], трудоёмкость восстановления ключа key на квантовом компьютере составляет $O(\sqrt{N}) + O(2^{n/2})$ (применяется вариант алгоритма Гровера для поиска итерационного ключа, на котором рассматриваемое соотношение выполняется с максимальной вероятностью), в то время как трудоемкость классического разностного метода авторы [28] оценивают величиной $O(N) + O(2^n)$.

Поиск коллизий

Для псевдослучайной функции $H : V_n \to V_n$ требуется найти такие $x \neq y$, $x, y \in V_n$, на которых $H(x) = H(y)$.

	Трудоемкость	Q-память	Память	Кол-во процессоров при распараллелива-нии
Classical, [36]	$2^{n/2-s}$	-	2^s	2^s
Improved Grover search, [35]	$2^{n/3}$	$2^{n/3}$	-	$2^{n/3}$
Ambainis's algorithm, [33]	$2^{n/3}$	$2^{n/3}$	-	no
Single processor [40]	$2^{2n/5}$	$O(n)$	$2^{n/5}$	no
Parallelization [40]	$2^{2n/5-3s/5}$	$O(2^s n)$	$2^{n/5+s/5}$	2^s

Таблица 2: Сравнительная таблица алгоритмов поиска коллизий, $s \leq n/4$.

2^s – количество процессоров при распараллеливании вычислений.

Поиск прообраза

Для псевдослучайной функции $H : V_n \to V_n$ и множества образов $T = \{y_1, \ldots, y_{2^t}\}$ требуется найти хотя бы одно значение $x \in V_n$, на котором $H(x) = y_i$, $y_i \in T$.

	Трудоемкость	Q-память	Память
Classical, no parallel	2^{n-t}	-	2^t
Classical, parallel	2^{n-t-s}	-	$2^t + 2^s$
Naive quantum algorithm	$2^{n/2}$	$O(n)$	-
Single processor [40]	$2^{n/2-t/6} + min\{2^t, 2^{3n/7}\}$	$O(n)$	$min\{2^{t/3}, 2^{n/7}\}$
Parallelization [40]	$2^{n/2-t/6-s/2} + min\{2^t, 2^{\frac{(3n-4s)}{7}}\}$	$O(2^s n)$	$min\{2^{t/3}, 2^{n/7+s/7}\}$

Таблица 3: Сравнительная таблица алгоритмов поиска второго прообраза.

Слайд-атака + алгоритм Саймона, см. [11].

- CBC-MAC, PMAC, GMAC, GCM и OCB в модели квантовых вычислений являются нестойкими.
- Также это относится к кандидатам международного конкурса CAESAR, алгоритмам CLOC, AEZ, COPA, OTR, POET, OMD и Minalpher.
- Трудоемкость применения квантовой слайд атаки, основанной на задаче Саймона, составляет $O(n)$ квантовых операций, в то время как трудоемкость классической слайд-атаки авторы оценивают величиной $O(2^{n/2})$.

Слайд-атака + алгоритм Саймона, см. [15].

- Применение к SP-сетям и сетям Фейстеля с модульным сложением (см.[15], табл. 1). Эффективность атак зависит от структуры шифра, получены варианты как полиномиального, так и экспоненциального ускорения.

8.Решение СЛУ, алгебраическая атака на AES, Trivium, SHA-3, МРКС

Алгоритм Harrow-Hassidim-Lloyd (HHL) – квантовый алгоритм поиска решения системы линейных уравнений, дающий экспоненциальное ускорение по сравнению с лучшим классическим алгоритмом – градиентным спуском (см. [45]).

Таблица 4: Сравнительная таблица трудоёмкостей алгоритмов решения СЛУ.

Задача	Алгоритм	Трудоемкость
LSP	CG, см. [46]	$O(Nsk \cdot log(1/\epsilon))$
QLSP	HHL, см. [44]	$O(log(N)s^2k^2/\epsilon))$
QLSP	VTAA-HHL, см. [47]	$O(log(N)s^2k/\epsilon))$
QLSP	Childs et. al., см. [48]	$O(sk \cdot \text{poly}log(sk/\epsilon))$
QLSP	QLSA, см. [49]	$O(k^2\text{poly}log(N)\|\|A\|\|_F/\epsilon))$

Параметры:

- N - размерность системы $Ax = b$, $A \in \mathbb{C}^{N \times N}$;
- s - показатель разреженности матрицы A;
- k - число обусловленности (condition number of A), показывает насколько сильно меняется значение Ax при небольшом изменении x;
- ϵ - требуемая точность;
- $||A||_F = \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}^2}$;

Алгоритм Harrow-Hassidim-Lloyd (HHL) – квантовый алгоритм поиска решения системы линейных уравнений, дающий экспоненциальное ускорение по сравнению с лучшим классическим алгоритмом – градиентным спуском (см. [45]).

Таблица 4: Сравнительная таблица трудоёмкостей алгоритмов решения СЛУ.

Задача	Алгоритм	Трудоемкость
LSP	CG, см. [46]	$O(Nsk \cdot log(1/\epsilon))$
QLSP	HHL, см. [44]	$O(log(N)s^2k^2/\epsilon))$
QLSP	VTAA-HHL, см. [47]	$O(log(N)s^2k/\epsilon))$
QLSP	Childs et. al., см. [48]	$O(sk \cdot \text{poly}log(sk/\epsilon))$
QLSP	QLSA, см. [49]	$O(k^2\text{poly}log(N)\|\|A\|\|_F/\epsilon))$

Параметры:

- N - размерность системы $Ax = b$, $A \in \mathbb{C}^{N \times N}$;
- s - показатель разреженности матрицы A;
- k - число обусловленности (condition number of A), показывает насколько сильно меняется значение Ax при небольшом изменении x;
- ϵ - требуемая точность;
- $||A||_F = \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}^2}$;

В таблицах c – константа из приблизительного равенства $O\left(\log\left(N+M\right)s\kappa^2/\varepsilon\right) \simeq c\log\left(N+M\right)s\kappa^2/\varepsilon$, – оценка сложности HHL алгоритма [44] (в квантовых операциях).

	Кол-во раундов	Кол-во переменных	Кол-во уравнений	T	Трудоемкость
AES-128	4	1792	4400	101376	$2^{69.07}c\kappa^2$
AES-128	6	2624	6472	151680	$2^{71.16}c\kappa^2$
AES-128	8	3456	8544	201984	$2^{72.65}c\kappa^2$
AES-128	10	4288	10616	252288	$2^{73.80}c\kappa^2$
AES-192	12	7488	18096	421248	$2^{76.44}c\kappa^2$
AES-256	14	11904	29520	696384	$2^{79.04}c\kappa^2$

Таблица 5: Сложность квантовой алгебраической атаки на AES ($\varepsilon = 1\%$)

Кол-во раундов	Кол-во переменных	Кол-во уравнений	T	Трудоемкость
288	951	951	5331	$2^{49.48}c\kappa^2$
576	1815	2103	11667	$2^{53.36}c\kappa^2$
1152	3543	4407	24339	$2^{57.08}c\kappa^2$
2304	6999	9015	49683	$2^{60.74}c\kappa^2$

Таблица 6: Сложность квантовой алгебраической атаки на Trivium ($\varepsilon = 1\%$)

8.Решение СЛУ, алгебраическая атака на AES, Trivium, SHA-3, MPKC

Длина хэш-кода, бит	Размер внутреннего состояния b (бит)	Кол-во раундов	Кол-во переменных	Кол-во уравнений	T	Трудоемкость
224	1600	24	76800	77000	610377	$2^{78.04}c\kappa^2$
256	1600	24	76800	77032	610506	$2^{78.04}c\kappa^2$
384	1600	24	76800	77160	611023	$2^{78.04}c\kappa^2$
512	1600	24	76800	77288	611540	$2^{78.04}c\kappa^2$

Таблица 7: Сложность восстановления прообраза SHA3 ($\varepsilon = 1\%$)

Multivariate Public Key Cryptosystem, один из кандидатов PQC

- Оценка трудоемкости применения алгебраической атаки к MPKC, полученная в [43], составляет $O\left(n^{10.5}\kappa^2 \log(1/\varepsilon)\right)$ квантовых операций.
- Лучшая известная не квантовая атака на MPKC – атака с помощью построения базиса Грёбнера с трудоемкостью порядка $O\left(2^{0.841 \cdot n}\right)$.

Одно из следствий [43]

При построении стойких в модели квантовых вычислений криптоалгоритмов соответствующая система уравнений должна иметь большое число обусловленности (condition number).

Для применения квантовых алгоритмов к криптографическим алгоритмам необходимо представить криптографические алгоритмы в виде квантовых схем.

Как реализовать существующие криптографические преобразования в виде квантовых схем?

Simplified-DES

Simplified-DES – двухраундовая сеть Фейстеля $E_{SDES} : V_{10} \times V_8 \to V_8$, ключ $K \in V_{10}$.

Quantum exhaustive key search with simplified-DES as a case study, [6]

- реализация SDES – 60 кубитов;
- поиск ключа алгоритмом Гровера на квантовом симуляторе *libquantum* – 61 кубит.

Денисенко Д.В., Никитенкова М.В. *Применение квантового алгоритма Гровера в задаче поиска ключа блочного шифра SDES*, [1]

- реализация SDES – 18 кубитов;
- поиск ключа алгоритмом Гровера на квантовом симуляторе *quipper* – 19 кубитов.

- В работе [1] показано, что минимальная оценка количества кубитов для поиска ключа SDES квантовым алгоритмом Гровера ($18 + 1 = 19$ кубитов) достижима;
- представлены подробные примеры применения алгоритма Гровера, программные реализации в Wolfram Mathematica и квантовом симуляторе *quipper*.

Реализация криптографических преобразований в виде квантовых схем

Для применения квантовых алгоритмов к криптоалгоритмам, например шифрам, необходимо представить функцию зашифрования $E : V_n \times V_m \to V_m$ в виде квантовой схемы.

В работе Денисенко Д.В., Маршалко Г.Б., Никитенкова М.В., Рудской В.И., Шишкин В.А. *Оценка сложности реализации алгоритма Гровера для перебора ключей алгоритмов блочного шифрования ГОСТ Р 34.12-2015*, [2], использован подход с представлением координатных функций в виде квантовых схем (см. рис. 1).

Преобразование над битовыми строками длины n	Количество дополнительных кубитов	Количество вентилей
$P \oplus Key$	0	n
$P + Key \bmod 2^n$	1	$\frac{2}{3}n^3 + \frac{3}{2}n^2 - \frac{25}{6}n + 8$
S-box	n	Сильно зависит от S-box, $> n$
Линейное преобразование	n	$\leq n(n-1)$
Циклический сдвиг	0	0

Таблица 8: Количество ресурсов для реализации элементарных преобразований

ГОСТ Р 34.12-2015 «Кузнечик»

Для реализации одной итерации функции зашифрования $E : V_{128} \times V_{128} \to V_{128}$ в виде квантовой схемы требуется $128 + 128 + 128 + 128 = 512$ кубитов (рис. 11).

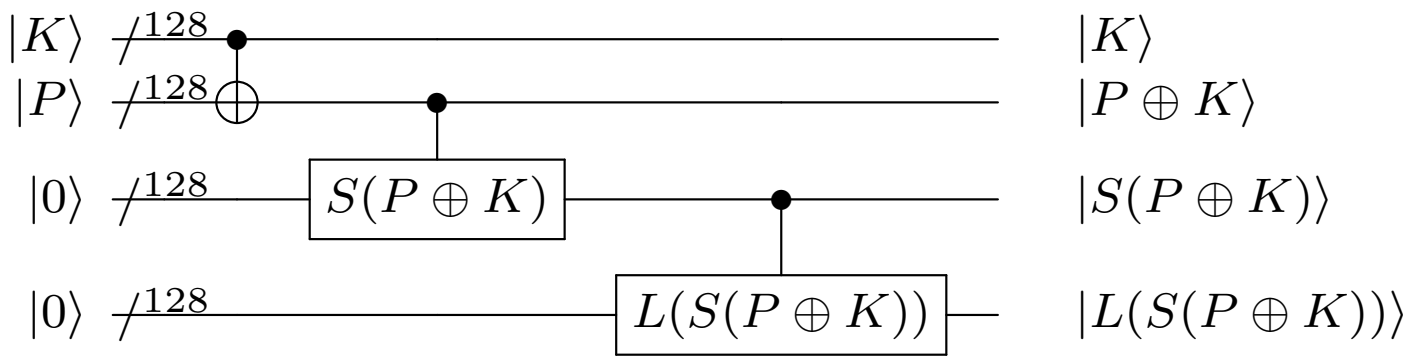


Рис. 11: Квантовая схема одной итерации алгоритма «Кузнечик».

ГОСТ Р 34.12-2015 «Магма»

Для реализации одной итерации функции зашифрования $E : V_{32} \times V_{64} \to V_{64}$ в виде квантовой схемы без повторного использования кубитов требуется $32 + 32 + 32 + 32 + 32 + 1 = 161$ кубит (см. рис. 12).

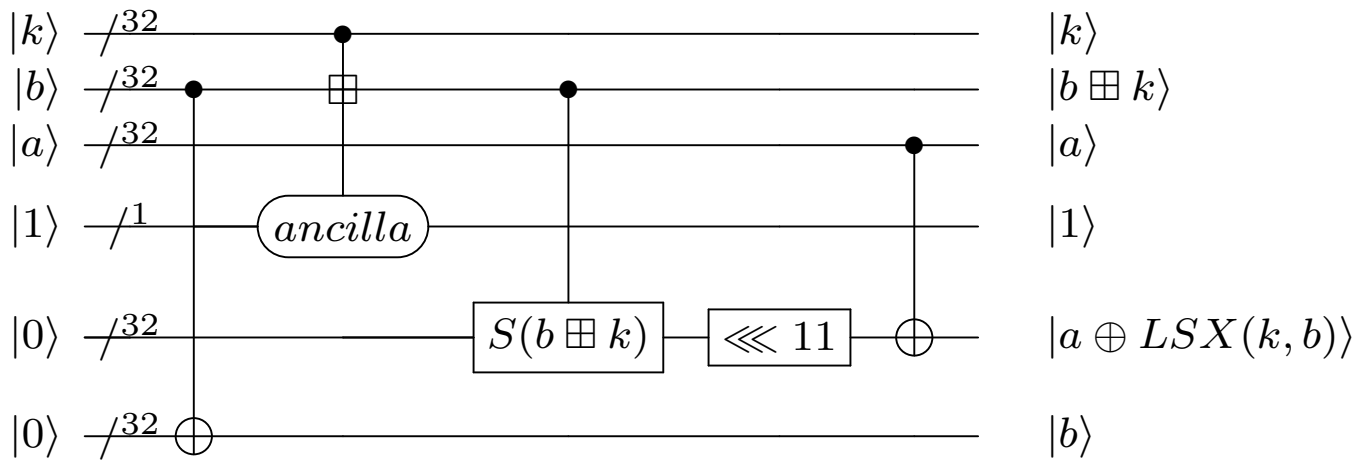


Рис. 12: Квантовая схема одной итерации алгоритма «Магма».

Квантовая схема на рис. 12 специально построена без повторного использования кубитов, что может пригодиться в другой модели квантовых вычислений (см. measurement-based quantum computation, one-way quantum computer [51]).

ГОСТ Р 34.12-2015 «Магма»

Для реализации одной итерации функции зашифрования $E : V_{32} \times V_{64} \to V_{64}$ с повторным использованием кубитов требуется $32 + 32 + 32 + 32 + 1 = 129$ кубитов (см. рис. 13).

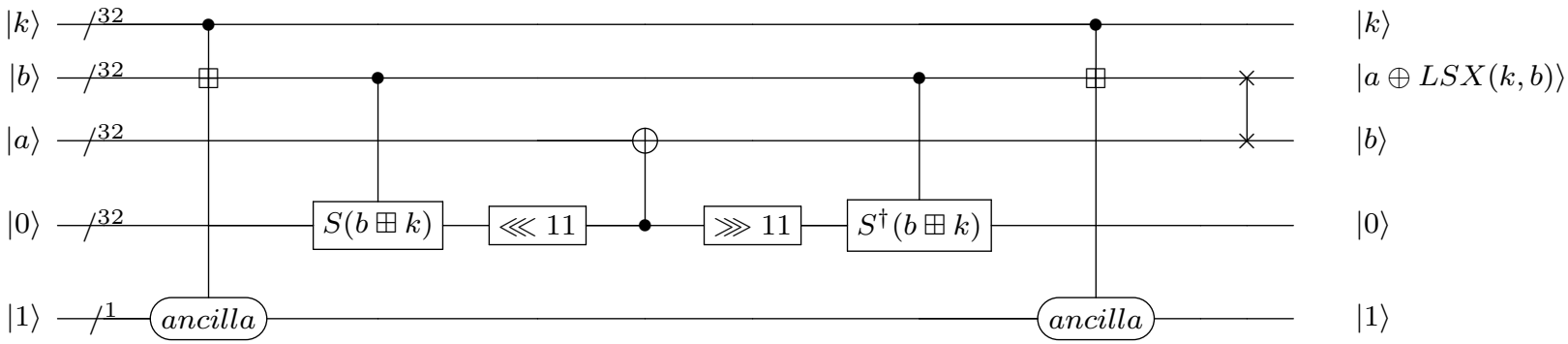


Рис. 13: Квантовая схема одной итерации алгоритма «Магма» с повторным использованием кубитов.

Реализация ГОСТ Р 34.12-2015 «Кузнечик» с повторным использованием кубитов

В алгоритме ГОСТ Р 34.12-2015 «Кузнечик» применяется 9 полных итераций, а в 10 итерации применяется только наложение ключа.

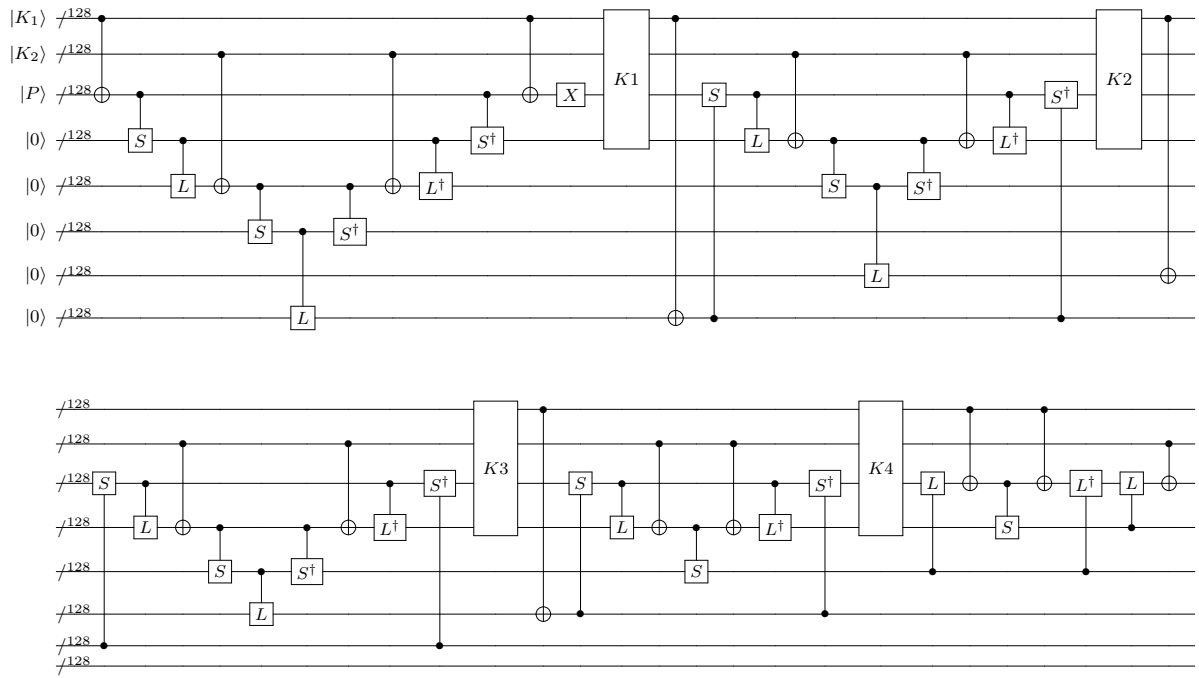


Рис. 14: Квантовая схема 10 раундов алгоритма «Кузнечик» с повторным использованием кубитов (сверху – первые 4 итерации алгоритма, снизу – оставшиеся 5 полных итераций и одна – неполная).

Реализация развёртывания ключа ГОСТ Р 34.12-2015 «Кузнечик» с повторным использованием кубитов

На рис. 14 в блоках Ki $(i = 1, 2, 3, 4)$ формируются раундовые ключи алгоритма шифрования «Кузнечик». Каждый такой блок включает 8 итераций квантовой схемы, изображенной на рис. 15.

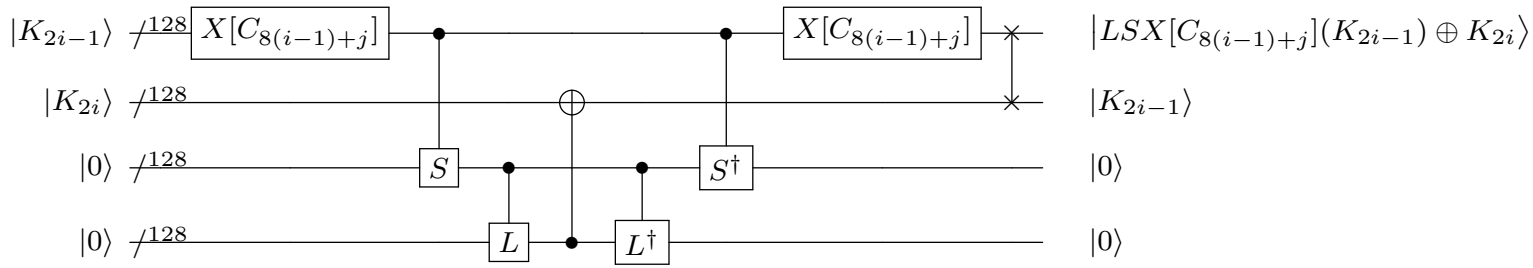


Рис. 15: Квантовая схема для одной итерации алгоритма развёртывания ключа алгоритма шифрования ГОСТ Р 34.12-2015 «Кузнечик» с повторным использованием кубитов, $i = 1, 2, 3, 4, j = 1, 2, \ldots, 8$.

Реализация S-боксов в виде квантовых схем без доп. кубитов.

В работе Денисенко Д.В. «О реализации подстановок в виде квантовых схем без использования дополнительных кубитов» [3] представлены квантовые схемы, реализующие S-боксы ГОСТ Р 34.12-2015 «Магма» без использования дополнительных кубитов.

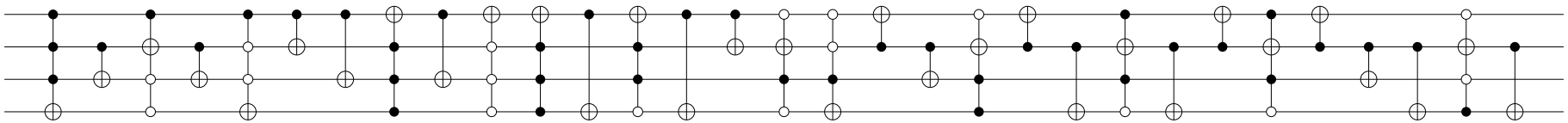


Рис. 16: Реализация $\pi_0 = (12, 4, 6, 2, 10, 5, 11, 9, 14, 8, 13, 7, 0, 3, 15, 1)$.

Вывод:

Преобразования X, S и L можно представить в виде квантовых схем без использования дополнительных кубитов.

Реализация криптографических преобразований в виде квантовых схем (true)

Если в структуре $E : V_n \times V_m \to V_m$ отсутствует операция $\boxplus mod 2^t$, $t > 1$, то достаточно $n + m$ логических кубитов.

Для операции $\boxplus \bmod 2^t$, где $t > 1$, может потребоваться 1 дополнительный кубит и $\frac{2}{3}n^3 + \frac{3}{2}n^2 - \frac{25}{6}n + 8$ квантовых вентилей (см. [52]).

При наличии возможности применения квантового преобразования Фурье, операцию модульного сложения можно реализовать без использования вспомогательных кубитов [53].

Преобразование над битовыми строками длины n	Количество дополнительных кубитов	Количество вентилей
$P \oplus Key$	0	n
$P + Key \; mod \; 2^n$	1	$\frac{2}{3}n^3 + \frac{3}{2}n^2 - \frac{25}{6}n + 8$
S-box	0	Сильно зависит от S-box, $> n$
Линейное преобразование	0	$> n$
Циклический сдвиг	0	0

Таблица 9: Количество ресурсов для реализации элементарных преобразований

Достаточное количество логических кубитов при реализации алгоритмов ГОСТ Р 34.12-2015 и AES.

ГОСТ Р 34.12-2015 «Магма»	$256 + 64 = 320$
ГОСТ Р 34.12-2015 «Кузнечик»	$256 + 128 = 384$
AES-128	$128 + 128 = 256$
AES-192	$192 + 128 = 320$
AES-256	$256 + 128 = 384$

Реализация хэш-функций в виде квантовых схем

Минимальное количество логических кубитов, необходимое для реализации хэш-функции в виде квантовой схемы, определяется максимальной длиной внутреннего состояния рассматриваемой хэш-функции.

Достаточное количество логических кубитов при реализации алгоритмов SHA-2, SHA-3 и ГОСТ Р 34.11-2012

Алгоритм	Минимальное кол-во кубитов для реализации в виде квантовой схемы
SHA-2 (224, 256)	512
SHA-2 (384, 512)	1024
SHA-3	1600
ГОСТ Р 34.11-2012	1024

Основные выводы *Quantum Computing: Progress and Prospects* [4]

Криптосхема	Размер ключа, бит	Эффективная стойкость, бит	Требуемое количество логических кубитов	Требуемое количество физических кубитов	Оценка времени
AES	128	128	2953	4.61×10^6	2.61×10^{12} лет
	192	192	4449	1.68×10^7	1.97×10^{22} лет
	256	256	6681	3.36×10^7	2.29×10^{32} лет
RSA	1024	80	2290	2.56×10^6	3.58 часа
	2048	112	4338	6.2×10^6	28.63 часов
	4096	128	8434	1.47×10^7	229 часов
ECDLP, (NIST P-256 NIST P-386 NIST P-521)	256	128	2330	3.21×10^6	10.5 часа
	386	192	3484	5.01×10^6	37.67 часа
	512	256	4719	7.81×10^6	95 часов
SHA256	N/A	72	2403	2.23×10^6	1.8×10^4лет

Таблица 10: Стойкость различных криптосхем согласно [4].

Основные выводы *Quantum Computing: Progress and Prospects* [4]

1.Наиболее развитые реализации физических кубитов

- ионы в ловушках;
- сверхпроводящие кубиты;

Ещё рано делать ставку на какую-то конкретную технологию квантовых вычислений.

2.Квантовая память

- В данный момент квантовые компьютеры не могут эффективно обрабатывать классические данные.
- Требуется разработка квантовой памяти (QRAM) – массива кубитов, способного долго хранить записанные в него квантовые состояния, как в базисные, так и состояния суперпозиции.

3.Коррекция ошибок

- Error rate - важнейший параметр, характеризующий точность вычислений.
- Обеспечение низкого уровня ошибок базовых операций - трудная задача.
- Необходимо применение алгоритмов коррекции ошибок, без применения которых маловероятно, что какая-либо сложная квантовая схема будет правильно работать.
- Применение коррекции ошибок на порядок увеличивает количество физических кубитов, необходимых для реализации одного логического кубита.

Основные выводы *Quantum Computing: Progress and Prospects* [4]

1.Наиболее развитые реализации физических кубитов

- ионы в ловушках;
- сверхпроводящие кубиты;

Ещё рано делать ставку на какую-то конкретную технологию квантовых вычислений.

2.Квантовая память

- В данный момент квантовые компьютеры не могут эффективно обрабатывать классические данные.
- Требуется разработка квантовой памяти (QRAM) – массива кубитов, способного долго хранить записанные в него квантовые состояния, как в базисные, так и состояния суперпозиции.

3.Коррекция ошибок

- Error rate - важнейший параметр, характеризующий точность вычислений.
- Обеспечение низкого уровня ошибок базовых операций - трудная задача.
- Необходимо применение алгоритмов коррекции ошибок, без применения которых маловероятно, что какая-либо сложная квантовая схема будет правильно работать.
- Применение коррекции ошибок на порядок увеличивает количество физических кубитов, необходимых для реализации одного логического кубита.

Основные выводы *Quantum Computing: Progress and Prospects* [4]

1.Наиболее развитые реализации физических кубитов

- ионы в ловушках;
- сверхпроводящие кубиты;

Ещё рано делать ставку на какую-то конкретную технологию квантовых вычислений.

2.Квантовая память

- В данный момент квантовые компьютеры не могут эффективно обрабатывать классические данные.
- Требуется разработка квантовой памяти (QRAM) – массива кубитов, способного долго хранить записанные в него квантовые состояния, как в базисные, так и состояния суперпозиции.

3.Коррекция ошибок

- Error rate - важнейший параметр, характеризующий точность вычислений.
- Обеспечение низкого уровня ошибок базовых операций - трудная задача.
- Необходимо применение алгоритмов коррекции ошибок, без применения которых маловероятно, что какая-либо сложная квантовая схема будет правильно работать.
- Применение коррекции ошибок на порядок увеличивает количество физических кубитов, необходимых для реализации одного логического кубита.

Основные выводы *Quantum Computing: Progress and Prospects* [4]

4.Квантовое превосходство

«Квантовое превосходство» – решение некоторой задачи с использованием квантового вычислителя, которую трудно решить на классическом компьютере, независимо от того, имеет ли эта задача практическую полезность – ещё не было продемонстрировано.

5.Как отслеживать уровень прогресса?

Уровень прогресса в гейтовой модели квантовых вычислений можно отслеживать по ключевым параметрам, определяющим качество квантового процессора:

- уровень ошибок при выполнении базовых операций с одним и двумя кубитами;
- связность кубитов в одном аппаратном модуле.

6.Прогнозы?

- Точное прогнозирование временных рамок создания квантового компьютера невозможно.
- Несмотря на значительный прогресс, нет никаких гарантий, что все проблемы будут преодолены.
- Следует отслеживать масштабирование систем из физических кубитов при постоянном среднем уровне ошибок базовых логических элементов и количество логических кубитов в разрабатываемых системах.

Основные выводы *Quantum Computing: Progress and Prospects* [4]

4.Квантовое превосходство

«Квантовое превосходство» – решение некоторой задачи с использованием квантового вычислителя, которую трудно решить на классическом компьютере, независимо от того, имеет ли эта задача практическую полезность – ещё не было продемонстрировано.

5.Как отслеживать уровень прогресса?

Уровень прогресса в гейтовой модели квантовых вычислений можно отслеживать по ключевым параметрам, определяющим качество квантового процессора:

- уровень ошибок при выполнении базовых операций с одним и двумя кубитами;
- связность кубитов в одном аппаратном модуле.

6.Прогнозы?

- Точное прогнозирование временных рамок создания квантового компьютера невозможно.
- Несмотря на значительный прогресс, нет никаких гарантий, что все проблемы будут преодолены.
- Следует отслеживать масштабирование систем из физических кубитов при постоянном среднем уровне ошибок базовых логических элементов и количество логических кубитов в разрабатываемых системах.

Основные выводы *Quantum Computing: Progress and Prospects* [4]

4.Квантовое превосходство

«Квантовое превосходство» – решение некоторой задачи с использованием квантового вычислителя, которую трудно решить на классическом компьютере, независимо от того, имеет ли эта задача практическую полезность – ещё не было продемонстрировано.

5.Как отслеживать уровень прогресса?

Уровень прогресса в гейтовой модели квантовых вычислений можно отслеживать по ключевым параметрам, определяющим качество квантового процессора:

- уровень ошибок при выполнении базовых операций с одним и двумя кубитами;
- связность кубитов в одном аппаратном модуле.

6.Прогнозы?

- Точное прогнозирование временных рамок создания квантового компьютера невозможно.
- Несмотря на значительный прогресс, нет никаких гарантий, что все проблемы будут преодолены.
- Следует отслеживать масштабирование систем из физических кубитов при постоянном среднем уровне ошибок базовых логических элементов и количество логических кубитов в разрабатываемых системах.

Основные выводы *Quantum Computing: Progress and Prospects* [4]

7.Возможно ли взломать в ближайшее время RSA-2048?

Учитывая текущие темпы прогресса, маловероятно, что в течение ближайшего десятилетия удастся построить квантовый компьютер, способный взломать RSA-2048 или сопоставимые криптосистемы с открытым ключом на основе дискретного логарифмирования.

8.Возможно ли создание квантовых компьютеров?

- Авторы [4] не нашли фундаментальных причин, по которым масштабируемый квантовый компьютер не может быть построен в принципе.
- Однако на пути к созданию такой системы и ее практическому использованию для решения важных задач остаются значительные технические проблемы.

9.Post-Quantum Cryptography, NISTIR 8240

- Существует большой коммерческий интерес к развертыванию постквантовых криптографических алгоритмов задолго до создания квантовых компьютеров.
- Авторы [4] считают, что для полного перехода к постквантовым криптографическим алгоритмам потребуется более 10 лет.

Основные выводы *Quantum Computing: Progress and Prospects* [4]

7.Возможно ли взломать в ближайшее время RSA-2048?

Учитывая текущие темпы прогресса, маловероятно, что в течение ближайшего десятилетия удастся построить квантовый компьютер, способный взломать RSA-2048 или сопоставимые криптосистемы с открытым ключом на основе дискретного логарифмирования.

8.Возможно ли создание квантовых компьютеров?

- Авторы [4] не нашли фундаментальных причин, по которым масштабируемый квантовый компьютер не может быть построен в принципе.
- Однако на пути к созданию такой системы и ее практическому использованию для решения важных задач остаются значительные технические проблемы.

9.Post-Quantum Cryptography, NISTIR 8240

- Существует большой коммерческий интерес к развертыванию постквантовых криптографических алгоритмов задолго до создания квантовых компьютеров.
- Авторы [4] считают, что для полного перехода к постквантовым криптографическим алгоритмам потребуется более 10 лет.

Основные выводы *Quantum Computing: Progress and Prospects* [4]

7.Возможно ли взломать в ближайшее время RSA-2048?

Учитывая текущие темпы прогресса, маловероятно, что в течение ближайшего десятилетия удастся построить квантовый компьютер, способный взломать RSA-2048 или сопоставимые криптосистемы с открытым ключом на основе дискретного логарифмирования.

8.Возможно ли создание квантовых компьютеров?

- Авторы [4] не нашли фундаментальных причин, по которым масштабируемый квантовый компьютер не может быть построен в принципе.
- Однако на пути к созданию такой системы и ее практическому использованию для решения важных задач остаются значительные технические проблемы.

9.Post-Quantum Cryptography, NISTIR 8240

- Существует большой коммерческий интерес к развертыванию постквантовых криптографических алгоритмов задолго до создания квантовых компьютеров.
- Авторы [4] считают, что для полного перехода к постквантовым криптографическим алгоритмам потребуется более 10 лет.

Company	Type	Technology	Now	Next Goal
D-Wave	Annealing	Superconducting	2048	5000
Fujitsu	Digital Annealer	Classical	1024	8192
Google	Gate	Superconducting	72	TBD
IBM	Gate	Superconducting	50	TBD
Intel	Gate	Superconducting	49	TBD
Univ. of Wisconsin	Gate	Neutral Atoms	49	TBD
Intel	Gate	Spin	26	TBD
IQOQI	Gate	Ion Trap	20	TBD
Rigetti	Gate	Superconducting	19	128
IonQ	Gate	Ion Trap	11	79
USTC (China)	Gate	Superconducting	10	20
NTT/Japan NII	Qtm Neural Network	Photonic	2048	>20,000
Univ. of Maryland / NIST	Quantum Simulator	Ion Trap	53	TBD
Harvard/MIT	Quantum Simulator	Rydberg Atoms	51	TBD
Huawei – HiQ Cloud	Software Simulator	Classical	42-169	N/A
Alibaba/Univ. of Michigan	Software Simulator	Classical	144	N/A
USTC/Origin QC	Software Simulator	Classical	64	N/A
University of Melbourne	Software Simulator	Classical	60	N/A
IBM Research	Software Simulator	Classical	56	N/A

Таблица 11: Квантовые процессоры на 21.01.2019, часть 1.

Company	Type	Technology	Now	Next Goal
ETH Zurich	Software Simulator	Classical	45	N/A
Intel–qHiPSTER	Software Simulator	Classical	43	N/A
Atos	Software Simulator	Classical	41	N/A
Microsoft–Azure	Software Simulator	Classical	40	N/A
Rigetti–Forest	Software Simulator	Classical	36	N/A
Microsoft–PC	Software Simulator	Classical	30	N/A
iARPA QEO	Annealing	Superconducting	N/A	100
NSF STAQ Pro	Gate	Ion Trap	N/A	>64
Silicon QC	Gate	Spin	N/A	10
CEA-Leti/INAC/	Gate	Spin	N/A	100

Таблица 12: Квантовые процессоры на 21.01.2019, часть 2.

Computer	1-Qubit Gate Fidelity	2-Qubit Gate Fidelity	Read Out Fidelity
IBM Q5 Tenerife	99.84%	95.98%	94.46%
IBM Q16 Melbourne	99.68%	92.84%	93.02%
IBM Q20 Poughkeepsie	99.89%	97.75%	TBD
IBM Q20 Tokyo	99.80%	97.16%	91.72%
IBM Q System One	99.96%	98.31%	TBD
Rigetti 16Q Aspen-1	97%	91%	93%
Rigetti 8Q Agave	96.15%	87.00%	83.84%
Rigetti 19Q Acorn	98.63%	87.50%	93.30%
IonQ 11 Qubit	>99%	>98%	99.80%

Таблица 13: Точность квантовых операций.

Спасибо за внимание.

[1] Денисенко Д.В., Никитенкова М.В. *Применение квантового алгоритма Гровера в задаче поиска ключа блочного шифра SDES*. ЖЭТФ, том 155, вып. 1, 2019. DOI:10.1134/S0044451019010036.

[2] Денисенко Д.В., Маршалко Г.Б., Никитенкова М.В., Рудской В.И., Шишкин В.А. *Оценка сложности реализации алгоритма Гровера для перебора ключей алгоритмов блочного шифрования ГОСТ Р 34.12-2015*. ЖЭТФ, том 155, вып. 4, 2019, DOI:10.1134/S0044451019040072.

[3] Денисенко Д.В. *О реализации подстановок в виде квантовых схем без использования дополнительных кубитов*, ЖЭТФ, том 155, вып. 5, 2019. Готовится к публикации, http://www.jetp.ac.ru/cgi-bin/e/index/forthcoming/62665?a=list.

[4] *Quantum Computing: Progress and Prospects*. National Academies of Sciences, Engineering, and Medicine. 2018. The National Academies Press, Washington DC, https://doi.org/10.17226/25196.

[5] Grassl M., Langenberg B., Roetteler M., Steinwandt R. *Applying Grover's algorithm to AES: quantum resource estimates.* arxiv.org/abs/1512.04965, 2015.

[6] Almazrooie M., Azman S., Rosni A., Mutter K. *Quantum exhaustive key search with simplified-DES as a case study.* SpringerPlus 2016 5:1494. DOI:10.1186/s40064-016-3159-4., 2016.

[7] Almazrooie M., Rosni A., Azman S., Mutter K. *Quantum Grover Attack on the Simplified-AES*. 204-211. DOI:10.1145/3185089.3185122, 2018.

[8] Kim P., Han D. Jeong K.C. *Time-space complexity of quantum search algorithms in symmetric cryptanalysis: applying to AES and SHA-2*. Quantum Inf Process (2018) 17: 339. https://doi.org/10.1007/s11128-018-2107-3.

[9] Akihiro Yamamura, Hirokazu Ishizuka *Quantum cryptanalysis of block ciphers*, 2000.

[10] Bonnetain X., Naya-Plasencia M., Schrottenloher A., *Quantum Security Analysis of AES* http://eprint.iacr.org/2019/272.pdf, 2019.

[11] Kaplan M., Leurent G., Leverrier A., Naya-Plasencia M. *Breaking Symmetric Cryptosystems using Quantum Period Finding.* http://arxiv.org/abs/1602.05973v3, 2016.

[12] Alagic G., Russell A. *Quantum-secure symmetric-key cryptography based on hidden shifts.* EUROCRYPT 2017, LNCS v. 10212. : http://eprint.iacr.org/2016/960.pdf, 2016.

[13] Santoli T., Schaffner C. *Using Simon's algorithm to attack symmetric-key cryptographic primitives.* http://arxiv.org/abs/1603.07856, 2016.

[14] Roetteler M., Steinwandt R., *A note on quantum related-key attacks*, arXiv:1306.2301v2 [quant-ph], 2013.

[15] Bonnetain X., Naya-Plasencia M., Schrottenloher A., *On Quantum Slide Attacks*. http://eprint.iacr.org/2018/1067.

[16] Hong Wang, Zhi Ma *Quantum Generic Attacks on Feistel Schemes*. arXiv:1010.1624v2 [quant-ph], 2010.

[17] Leander G., May A. *Grover Meets Simon - Quantumly Attacking the FX-construction.* ICTACIS, ASIACRYPT 2017. : http://eprint.iacr.org/2017/427.pdf, 2017.

[18] Dong XiaoYang, Wang Xiaoyng. *Quantum Key-recovery Attack on Feistel Structures.* http://eprint.iacr.org/2017/1199.pdf, 2017.

[19] Zheng Li, Xiaoyang Dong, Xiaoyun Wang. *Quantum Cryptanalysis on Some Generalized Feistel Schemes.* http://eprint.iacr.org/2017/1249.pdf, 2017.

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

[21] Kaplan M. *Quantum attacks against iterated block ciphers.* http://arxiv.org/abs/1410.1434, 2015.

[22] Akinori Hosoyamada, Yu Sasaki. *Quantum Meet-in-the-Middle Attacks: Applications to Generic Feistel Constructions.* http://eprint.iacr.org/2017/1229.pdf, 2017.

[23] Akinori Hosoyamada, Yu Sasaki. *Cryptanalysis against Symmetric-Key Schemes with Online Classical Queries and Offline Quantum Computations*, https://doi.org/10.1007/978-3-319-76953-0-11, 2018.

[24] Roetteler M., Naehrig M., Krysta M. Svore, Lauter K. *Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms.* https://eprint.iacr.org/2017/598.pdf., 2017.

[25] Ekera M., Hastad J. *Quantum algorithms for computing short discrete logarithms and factoring RSA integers.* http://arxiv.org/abs/1702.00249, 2017.

[26] Hong-Wei Li, Li Yang. *Quantum differential cryptanalysis to the block ciphers.* https://arXiv.org/pdf/1511.08800.pdf., 2015.

[27] Kaplan M., Leurent G., Leverrier A., Marna Naya-Plasencia,. *Quantum Differential and Linear Cryptanalysis.* http://arxiv.org/pdf/1510.05836v2.pdf. , 2015.

[28] Zhou Q., Lu S., Zhang A., Sun J. *Quantum differential cryptanalysis,.* https://www.researchgate.net/profile/Songfend_Lu/publication/275220662., 2015.

[29] Huiqin Xie, Li Yang *Using Bernstein-Vazirani algorithm to attack block ciphers.*, arXiv:1711.00853v3 [quant-ph], 2018.

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

[31] Xiaoyang Dong, Bingyou Dong, Xiaoyun Wang. *Quantum Attacks on Some Feistel Block Ciphers.* http://eprint.iacr.org/2018/504.pdf, 2018.

[32] Martin D.P., Montanaro A., Oswald E., Shepherd D. *Quantum Key Search with Side Channel Advice.*, https://doi.org/10.1007/978-3-319-72565-9-21, 2017.

[33] Ambainis, A. *Quantum walk algorithm for element distinctness.* FOCUS 2004 SIAM J. Comput. 37:210-239, 2003.

[34] Brassard G., Hoyer P., Tapp. A. *Quantum algorithm for the collision problem.* CoRR, quant-ph/9705004. DOI:10.1145/261342.261346, 1997.

[35] Brassard G., Hoyer P., Tapp. A. *Quantum cryptanalysis of hash and claw-free functions* In: LATIN. Lecture Notes in Computer Science, vol. 1380, pp. 163-169, Springer (1998).

[36] Van Oorschot, P.C., Wiener, M.J. *Parallel collision search with application to hash functions and discrete logarithms.* In: CCS '94, Proceedings of the 2nd ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, November 2-4, 1994. pp. 210-218. ACM (1994).

[37] Seiichiro, T. *Claw finding algorithms using quantum walk.* Theoretical Computer Science, 410 :5285-5297, Mathematical Foundations of Computer Science (MFCS 2007), 2009.

[38] Amy M., Matteo O., Gheorghiu V., Mosca M., Parent A., Schanck J. *Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3.* http://arxiv.org/abs/1603.09383, 2016.

[39] Czajkowski J., Bruinderink L.G., HulsingA., Christian S. *Quantum preimage, 2nd-preimage and collision resistance of SHA3.* http://eprint.iacr.org/2017/302, 2017.

[40] Chailloux A., Plasencia M., Schrottenloher A. *An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography*, http://eprint.iacr.org/2017/847, 2017.

[41] Balogh M., Eaton E., Song F. *Quantum Collision-Finding in Non-Uniform Random Functions*, http://eprint.iacr.org/2017/688, 2017.

[42] Hosoyamada A., Sasaki Y., Tani S, Xagawa k. *Improved Quantum Multicollision-Finding Algorithm*, http://eprint.iacr.org/2018/1122, 2018.

[43] Yu-Ao Chen, Xiao-Shan Gao. *Quantum Algorithms for Boolean Equation Solving and Quantum Algebraic Attack on Cryptosystems.* http://arxiv.org/abs/1712.06239, 2018.

[44] Harrow A.W., Hassidim A., Lloyd S. *Quantum algorithm for linear systems of equations.* Physical Review Letters, 103 : 150502, 2009.

[45] Dervovic D., Herbster M., Mountney P., Severini S., Usher N, Wossnig L. *Quantum linear systems algorithms: a primer*, arXiv:1802.08227v1 [quant-ph], 2018.

[46] Shewchuk J. R. *An Introduction to the Conjugate Gradient Method Without the Agonizing Pain*, https : //www.cs.cmu.edu/~quake-papers/painless-conjugate-gradient.pdf, 1994.

[47] Ambainis A. *Variable time amplitude amplification and a faster quantum algorithm for solving systems of linear equations*, eprint: arXiv:1010.4458, 2010.

[48] Childs A. M., Kothari R. and Somma R. D. *Quantum Algorithm for Systems of Linear Equations with Exponentially Improved Dependence on Precision*, In: SIAM Journal on Computing 46.6 (2017), pp. 1920–1950. DOI:10.1137/16M1087072.

[49] Wossnig L., Zhao Z., Prakash A. *Quantum Linear System Algorithm for Dense Matrices*, In: Phys. Rev. Lett. 120 (5 2018), p. 050502. DOI:10.1103/PhysRevLett.120.050502.

[50] Barenco A., Bennet C., et al. Elementary gates for quantum computation, https://arxiv.org/pdf/quant-ph/9503016.pdf, 1995.

[51] R. Raussendorf, D.E. Browne, H.J. Briegel *Measurement-based quantum computation with cluster states.* DOI:10.1103/PhysRevA.68.022312, https://arxiv.org/abs/quant-ph/0301052, 2003.

[52] Kaye P. *Reversible addition circuit using one ancillary bit with application to quantum computing*, https://arxiv.org/abs/quant-ph/0408173v2, 2004.

[53] Thomas G. Draper. *Addition on a Quantum Computer*. Quantum Physics (quant-ph), https://arxiv.org/abs/quant-ph/0008033.

[54] Dustin Moody, *Announcement and outline of NIST's Call for Submissions* (Fall 2016), PQCrypto 2016.

[55] NIST IR 8105, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

[56] FIRST PQC Standartization Conference, PQCrypto 2018, https://csrc.nist.gov/events/2018/first-pqc-standardization-conference

[57] NIST Post-Quantum Cryptography. Round 1 Submissions. https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions;

[58] Quantum-Safe: The next generation of cybersecurity https://www.isara.com/isara-radiate

[59] Manea A. *BlackBerry Partners with ISARA to Secure the Quantum Future*, 02.13.2017, http://blogs.blackberry.com/2017/02/blackberry-partners-with-isara-to-secure-the-quantum-future

[60] Reed J. *Quantum-Resistant Encryption Keys Signal a Return to Security Roots for BlackBerry*, http://ww2.frost.com/frost-perspectives/quantum-resistan-encryption-keys-sgnal-return-security-roots-blackberry.

[61] *Quantum Algorithm Implementations for Beginners*, arXiv:1804.03719v1, 2018.