О возможности восстановления ключа алгоритма Кузнечик с использованием алгоритма Гровера

Григорий Маршалко, Владимир Рудской, Василий Шишкин

Технический комитет по стандартизации ТК 26

26 марта 2014

Мотивировка: последние результаты по изучение вопросов «практической» реализации квантовых атак

- M. Grassl, B. Langenberg, M. Roetteler, R. Steinwandt, Applying Grover's algorithm to AES: quantum resourse estimation.
- M. Amy, O. Di Matteo, V. Gheorghiu, M. Mosca, A. Parent, J. Schanck, Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3

Квантовая механика. Экскурс

Постулат 1

С каждой изолированной физической системой связывается комплексное векторное пространство со скалярным произведением, т.е. гильбертово пространство, которое мы будем далее обозначать как $\mathcal{H}^d$, где d – размерность пространства. Это векторное пространство называется *пространством состояний* системы. Состояние системы описывается *вектором состояния*, который является единичным вектором в пространстве состояний.

Квантовая механика. Экскурс

Пример

Простейшей квантовомеханической системой является кубит. Пространство состояний кубита двумерно. Обозначим ортонормированные базисные векторы пространства как $|0\rangle$ и $|1\rangle$. Произвольный вектор состояния в этом пространстве может представлен в виде

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,,$$

где a и b – комплексные числа. Условие единичности вектора $|\psi\rangle$ эквивалентно условию $|a|^2 + |b|^2 = 1$. Неформально говоря, базисные векторы соответствуют классическим битам 0 и 1, а общий вид вектора состояния соответствует состоянию *суперпозиции*. Будем говорить, что линейная комбинация $\sum_i \alpha_i\,|\psi_i\rangle$ является суперпозицией состояний $|\psi_i\rangle$ с *амплитудами* α_i.

Квантовая механика. Экскурс

Постулат 2

Эволюция замкнутой квантовой системы описывается унитарным преобразованием, т.е. состояние системы $|\psi\rangle$ в некоторый момент времени t_1 связано с ее состоянием $|\psi'\rangle$ в момент времени t_2 посредством *унитарного оператора* U, зависящего только от моментов времени t_1 и t_2:

$$|\psi'\rangle = U(t_1, t_2)\,|\psi\rangle\,.$$

Постулат 2 показывает как связаны между собой состояния квантовой системы в два разных момента времени.

Квантовая механика. Экскурс

Постулат 3

Квантовые измерения описываются набором операторов измерения $\{M_m\}$. При этом если перед измерением квантовая система находилась в состоянии $|\psi\rangle$, то в результате измерения будет получен результат m с вероятностью

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle ,$$

а после измерения квантовая система будет находится в состоянии

$$\frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}.$$

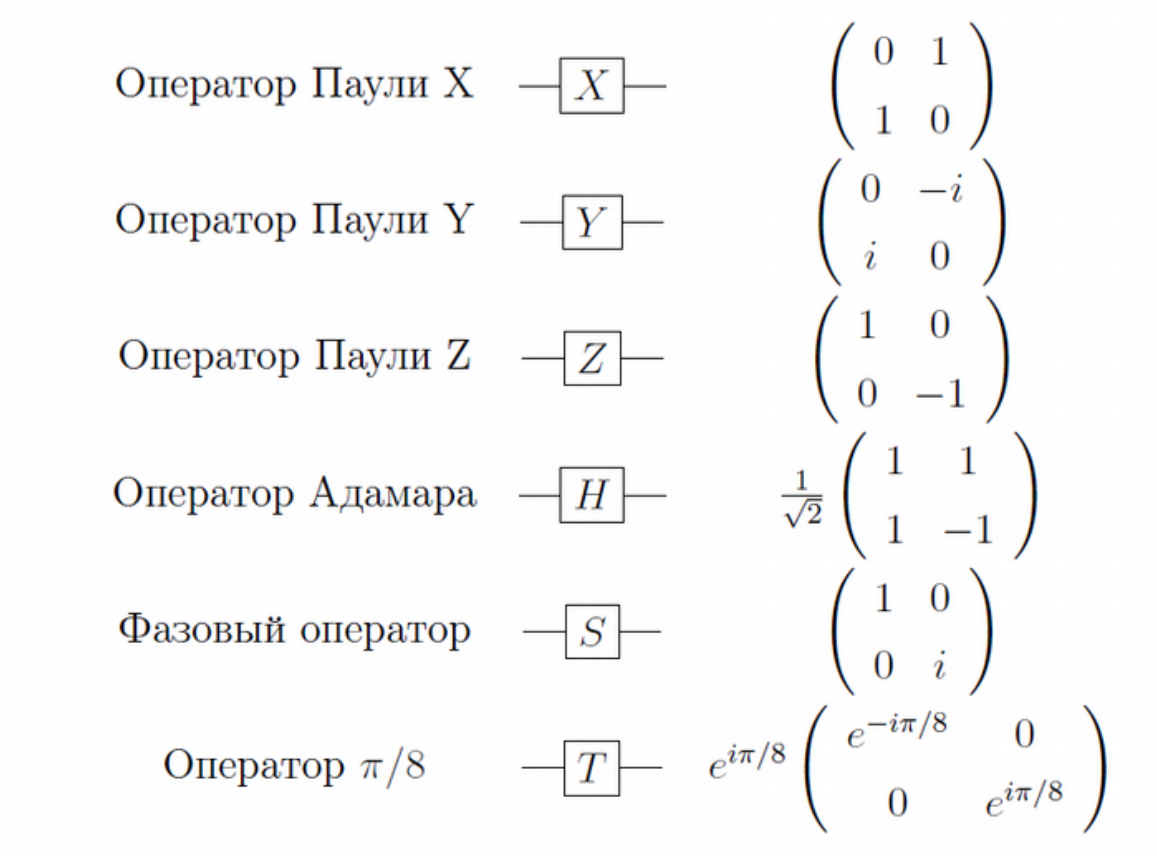
Система операторов измерения удовлетворяет условию полноты, т.е. сумма вероятностей всех возможных исходов измерений равна единице.

Постулат 4

Пространство состояний *составной системы* представляет собой тензорное произведение пространств состояний входящих в нее систем. Более того, если рассматривается составная система из n подсистем, а система с номером i находится в состоянии $|\psi_i\rangle$, то состояние составной системы описывается вектором

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle \,.$$

Квантовые схемы. Однокубитовые операторы



$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$e^{i\pi/8} \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$$

Квантовые схемы. Многокубитные операторы

Пусть U – произвольная унитарная операция на одном кубите. Определим двухкубитовую операцию *управлемое* U следующим образом. Один из кубитов является *управляющим*, а другой *управляемым*. При этом, если управляющий кубит установлен в единицу, то к управляемому кубиту применяется оператор U, в противном случае управляемый кубит не изменяется, т.е. $|c\rangle\,|t\rangle \to |c\rangle\,U^c\,|t\rangle$.

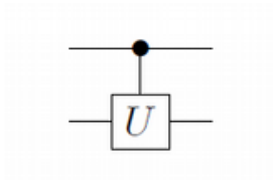


Рис.: Управляемое «U»

Квантовые схемы. Многокубитные операторы

Можно обобщить введенное определение на случай большего числа кубитов. Пусть у нас есть система из n управляющих и k управляемых кубит, и унитарный оператор U, действующий на k кубит. Определим операцию $C^n(U)$ следующим образом:

$$C^n(U)\,|x_1x_2\ldots x_n\rangle\,|\psi\rangle = |x_1x_2\ldots x_n\rangle\,U^{x_1x_2\ldots x_n}\,|\psi\rangle\,,$$

где $x_1x_2\ldots x_n$ в верхнем индексе U есть *произведение* битов, т.е. оператор U применяется к управляемым кубитам только если все n управляющих кубит установлены в единицу.

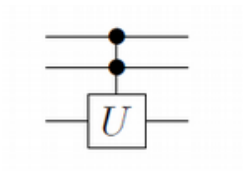


Рис.: Оператор с двумя управляющими входами. Оператор Тоффоли

Алгоритм Гровера. Постановка задачи

Пусть имеется некоторое проиндексированное множество из $N = 2^n$ элементов. Требуется в этом множестве найти индекс элемента, удовлетворяющего некоторому критерию поиска, причем такой элемент существует и единственен. Иными словам, можно считать, что задана некоторая булева функция, $f : V_n \to V_1$, причем $f(x) = 1$ тогда и только тогда, когда элемент множества с индексом x удовлетворяет критерию поиска $(x = \omega)$. При этом считается, что указанная функция f реализована как черный ящик, или оракул. При решении задачи на классическом вычислителе в общем случае необходимо перебрать все возможные значения индекса, что в итоге дает трудоемкость порядка $O(N)$.

Алгоритм Гровера. Квантовый поиск

При решении задачи на квантовом вычислителе алгоритм Гровера имеет трудоемкость $O(\sqrt{N})$ и представляет собой следующее. Прежде всего, считается, что существует квантовый оракул, проверяющий выполнение критерия поиска, который представляет собой унитарный оператор U_ω, действующий следующим образом:

$$\begin{cases} U_\omega |x\rangle = -|x\rangle, & \text{если} x = \omega, \text{т.е.} f(x) = 1 \\ U_\omega |x\rangle = |x\rangle, & \text{если} x \neq \omega, \text{т.е.} f(x) = 0 \end{cases}. \tag{1}$$

Алгоритм Гровера. Квантовый поиск

Чтобы связать квантовый оракул с классической булевой функцией f используют эквивалентное задание с использованием вспомогательного кубита:

$$\begin{cases} U_\omega |x\rangle |y\rangle = |x\rangle |y \oplus 1\rangle, & \text{если} x = \omega, \text{т.е.} f(x) = 1 \\ U_\omega |x\rangle |y\rangle = |x\rangle |y\rangle, & \text{если} x \neq \omega, \text{т.е.} f(x) = 0 \end{cases}, \tag{2}$$

или кратко $U_\omega |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$.

Алгоритм Гровера. Квантовый поиск

Легко убедиться, что если вспомогательный кубит приведен в состояние $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = H|1\rangle$, то действие оператора U_ω в форме (2) эквивалентно заданию в форме (1):

$$U_\omega(|x\rangle \otimes |-\rangle) = \begin{cases} -|x\rangle \otimes |-\rangle \\ |x\rangle \otimes |-\rangle \end{cases}$$

Алгоритм Гровера. Квантовый поиск

Формируется состояние, являющееся равномерной суперпозицией всех $N = 2^n$ значений аргумента x (для чего потребуется n кубит):

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle .$$

К этому состоянию (или к состоянию $|s\rangle \otimes |-\rangle$, в зависимости от способа задания оператора оракула) применяется оператор «итерации Гровера», состоящий из последовательного применения оператора оракула U_ω и оператора «рассеивания Гровера» U_s,

$$U_s = 2 |s\rangle \langle s| - I.$$

После $O(\sqrt{N})$ итераций выполняется измерение всех (или первых n) кубит, а результат измерения с большой вероятностью будет давать искомое значение ω.

Алгоритм Гровера. Квантовый поиск

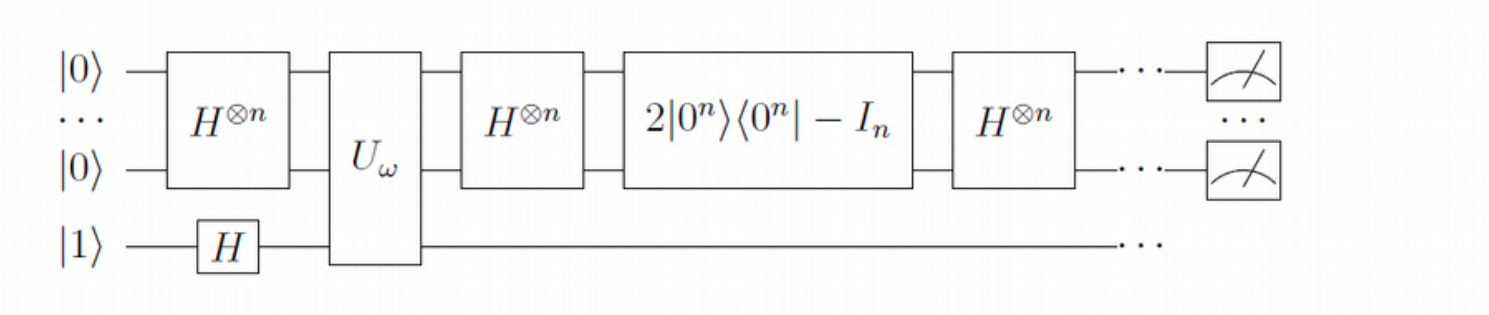


Рис.: Схема применения алгоритма Гровера

Сложность реализации:

$$O(\sqrt{N}) \cdot (t_{U_\omega} + t_{U_s})$$

Алгоритм Гровера для блочных шифров

Рассмотрим алгоритм блочного шифрования с длиной ключа n и блока m бит, $E : V_n \times V_m \to V_m$. Пусть известно некоторое количество пар открытых и шифрованных текстов, полученных при шифровании на одном и том же ключе, $C_i = E(K, P_i)$, $i = 1, t$ и решается стандартная задача по восстановлению ключа. Нам необходимо задать оператор U_ω. Исходя из расстояния единственности шифра количество пар текстов должно быть равным $t = \left\lceil \frac{n}{m} \right\rceil$. В этом случае ключ будет с большой вероятностью единственным, а соответствующая булева функция оракула $f : V_n \to V_1$ определяется следующим образом

$$f(x) = \bigwedge_{i=1}^{t} z\left(E(x, P_i) \oplus C_i\right),$$

где $z : V_m \to V_1$, причем $z(x) = 1$, если $x = 0^m$ и $z(x) = 0$ иначе.

Проблемы при реализации алгоритмов на квантовых компьютерах

- Выбор «элементной» базы – определяет физические характеристики системы (декогеретизация)
- Применение квантовых корректирующих кодов – число реальных физических кубитов существенно больше числа логических
- Эффективная реализация криптографической схемы – баланс между числом используемых кубитов и временем выполнения преобразований (числа операций)

«Физическая» реализация алгоритма Гровера

- Уровень математической модели алгоритма
- Логическая модель (выбор обратимых операторов, реализующих криптографический алгоритм)
- Уровень исправления ошибок (реализация квантовых корректирующих кодов)
- Физический уровень (требуемые ресурсы: число кубитов/ время реализации)

«Физическая» реализация алгоритма Гровера

- Уровень математической модели алгоритма
- Логическая модель (выбор обратимых операторов, реализующих криптографический алгоритм)

Реализация криптографических схем на квантовых компьютерах. Выбор стратегии

- Использование большего количества кубитов – меньшее число операций
- Ограничение на количество кубитов – увеличение числа операций

Реализация криптографических схем на квантовых компьютерах. Проблема итеративных преобразований

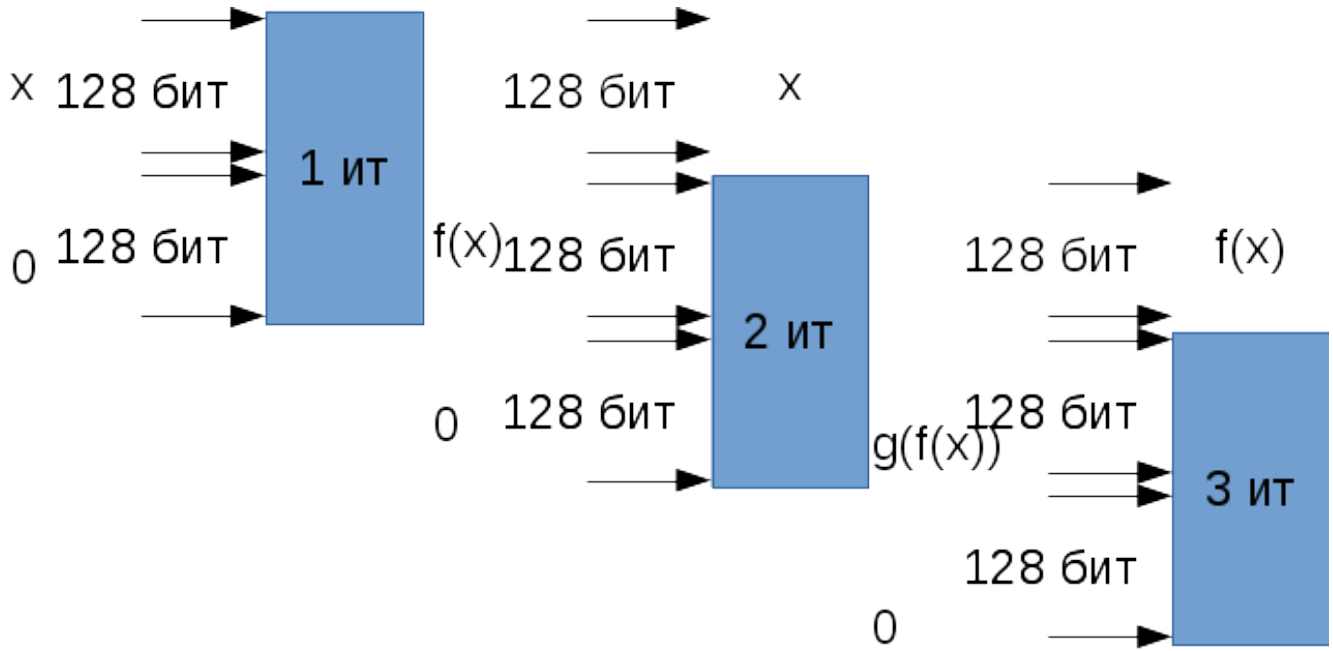


Рис.: Рост числа кубитов при итеративных преобразованиях

Реализация криптографических схем на квантовых компьютерах. Проблема последовательных преобразований

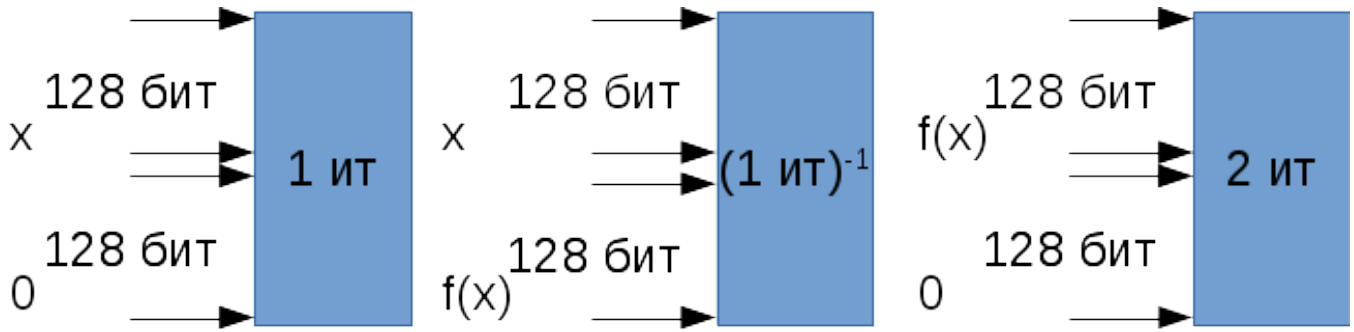


Рис.: Компенсация роста числа кубитов за счет введения обратных преобразований

Реализация алгоритма Кузнечик. Элементарные преобразования

- Сложение с константой константы – NOT (однокубитовый оператор)
- XOR – CNOT (двухкубитовый оператор)
- AND, OR, NOR ... – (многокубитовые операторы, оператор Тоффоли – 3 кубита)
- перестановка бит – бесплатно

Реализация алгоритма Кузнечик. Структурные преобразования

- Сложение со 128-битной константой ($\approx$ 64 NOT)
- Сложение со 128-битным ключом (128 CNOT, дополнительные 128 кубитов для хранения результата)
- Линейное преобразование
- Нелинейное преобразование

Реализация алгоритма Кузнечик. Линейное преобразование

Наименьшее число операций XOR получается в случае 16 применений сопровождающей матрицы минимального многочлена линейной рекурренты, задающей линейное преобразование алгоритма. Число операций XOR (CNOT) в таком случае равно 6640. Также это преобразование потребует использования дополнительного 128 кубитного регистра для хранения данных.

Реализация алгоритма Кузнечик. Нелинейное преобразование

В работе Борисенко и Дук Хо «Algorithms for determining logic circuit implementing Boolean Functions of S-box with minimum number of logic elements» получено представление для нелинейного преобразования имеющее 245 операций AND и 412 XOR.

Реализация алгоритма Кузнечик. Нелинейное преобразование

Простой способ реализации подстановки – с использованием 248 дополнительных кубитов вычисляем все мономы. Это потребует $\sum_{i=2}^{7} \binom{8}{i} = 247$ применений оператора Тоффоли. Результирующее преобразование может быть получено путем применения 412 операторов CNOT. Полученные значения должны быть удвоены для применения обратных преобразований. В результате получаем 494 оператора Тоффоли и 824 оператора CNOT.

Реализация алгоритма Кузнечик. Нелинейное преобразование

В целом нелинейный слой потребует 254 дополнительных кубита, $16 \cdot 494 = 7904$ оператора Тоффоли и $16 \cdot 824 = 13184$ операторов CNOT.

Реализация алгоритма Кузнечик. Итерационное преобразование

Итерационное преобразование потребует 254 дополнительных кубита $128 + 6640 + 13184 = 19952$ операторов CNOT и 7904 операторов Тоффоли.

Реализация алгоритма Кузнечик. Выработка итерационного ключа

Вычисление каждого итерационного ключа задействует 8 итерационных преобразования, которые используются при применении 8 итераций сети Фейстеля к входному 256 кубитному вектору. Наложение ключа при этом заменяется наложением итерационной константы, задействующим в среднем 64 операции NOT.
Выработка ключа потребует 254 дополнительных кубита $19952 \cdot 8 = 159616$ операторов CNOT, $7904 \cdot 8 = 63232$ операторов Тоффоли и $64 \cdot 8 = 512$ операторов NOT.

Реализация алгоритма Кузнечик. Ключевая развертка

Приведенная процедура выполняется 4 раза. Таким образом всего для ключевой развертки задействуется 254 дополнительных кубита $159616 \cdot 4 = 636644$ операторов CNOT, $63232 \cdot 8 = 252928$ операторов Тоффоли и $512 \cdot 4 = 2048$ операторов NOT.

Реализация алгоритма Кузнечик. Итерационные преобразования

В алгоритме Кузнечик итерационные преобразования применяются 9 раз в полном виде и один раз – в виде финального наложения ключа. Это требует 254 дополнительных кубита $19952 \cdot 9 + 128 = 179696$ операторов CNOT и $7904 \cdot 9 = 71136$ операторов Тоффоли.

Реализация алгоритма Кузнечик. Общие затраты

В результате нам потребуется

- $254 + 128 + 256 + 254 = 892$ кубита,
- $636644 + 179696 = 816340$ операторов CNOT,
- $252928 + 71136 = 324064$ операторов Тоффоли и
- 2048 операторов NOT.

Реализация алгоритма Гровера. Общие затраты

Пользуясь выражением из работы для оценки числа ресурсов, необходимых для реализации алгоритма Гровера M. Grassl, B. Langenberg, M. Roetteler, R. Steinwandt, Applying Grover's algorithm to AES: quantum resourse estimation получаем оценку в $1.6 \cdot 2^{150}$ операторов, и $892 \cdot 2 + 1 = 1785$ кубитов.