Ежегодная международная научно-практическая конференция РусКрипто'2020, *www.ruscrypto.ru*

О комбинации квантовых алгоритмов перечисления и поиска на примере квантового разностного метода

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

18 марта 2020 г.

Структура доклада

1. О моделях Q1 и Q2. Квантовые алгоритмы поиска и перечисления.
2. О квантовом разностном методе.
3. О комбинации квантовых алгоритмов перечисления и поиска.

Модели Q1 и Q2 квантовых вычислений [5, 6, 7, 8]

Q1

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

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

Q2

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

Superposition queries access quantum circuit implementing the primitive with a secret key.
Example: breaking CBC MAC with Simon's algorithm.

Квантовые алгоритмы. Алгоритм Гровера.

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

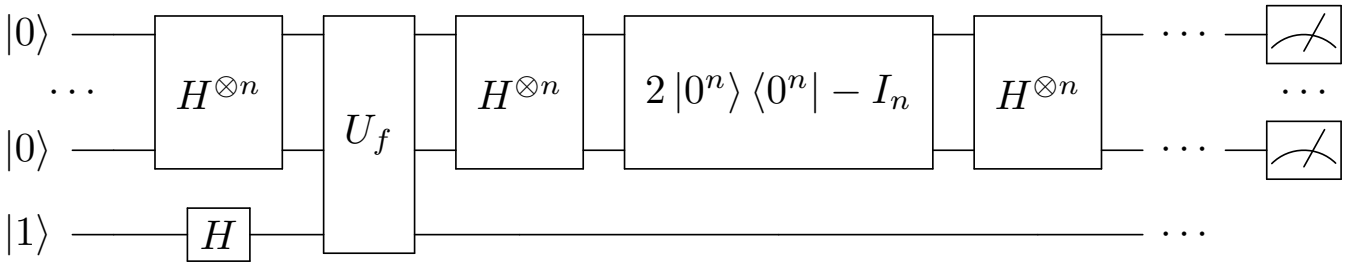

Рис. 1: Итерация Гровера «G» относительно булевой функции f.

- 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 $|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$.
- $|\psi\rangle = cos(\frac{\theta}{2}) |\alpha\rangle + sin(\frac{\theta}{2}) |\beta\rangle$, при измерении $|\psi\rangle$ вероятность получить какое-либо из M возможных решений равна $sin^2(\frac{\theta}{2})$.
- После k итераций Гровера получим состояние

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

Квантовое перечисление (QC)

Задача: дана случайная булева функция $f : V_n \to V_1$, требуется оценить $M = \left|f^{-1}(1)\right|$ – количество аргументов, на которых рассматриваемая булева функция принимает значение 1.
С помощью квантовой схемы на рис. 2 можно оценить $\theta = 2 \arcsin \sqrt{M/N}$.

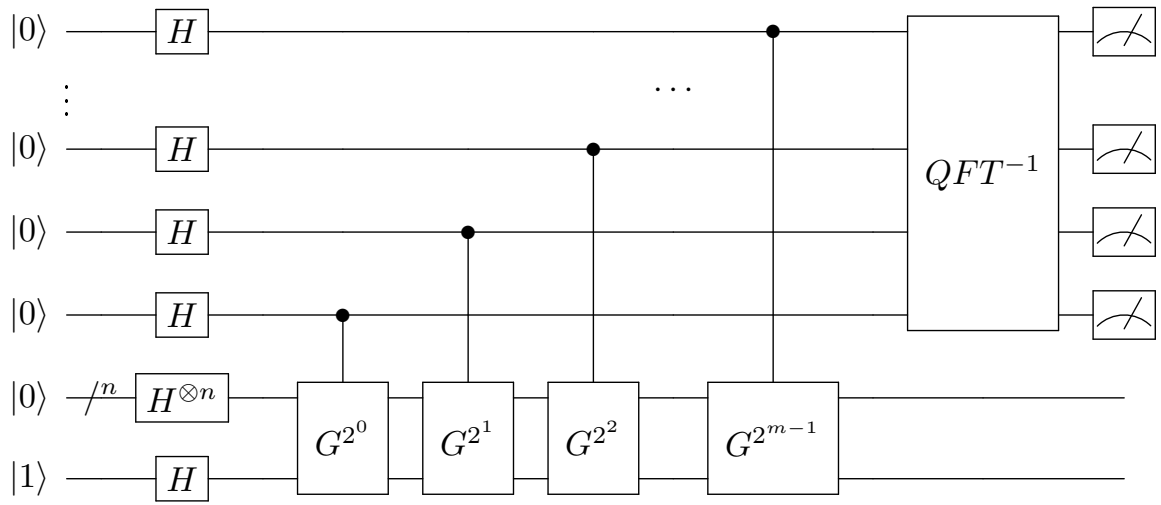

Рис. 2: Квантовая схема для алгоритма определения угла поворота θ итерации Гровера G. Регистр управления содержит m кубитов.

При $m \approx n/2$ получим оценку $|f^{-1}(1)|$ с заданным уровнем погрешности и вероятностью успеха не менее $4/\pi^2 = 0.405285$.

Квантовое перечисление (пример из [12])

$f(x_1, x_2, x_3, x_4, x_5, x_6) = x_1 x_2 x_3 x_4 x_5$, $M = ||f|| = 2$, $N = 2^6$,
$\theta = 2 \arcsin \sqrt{M/N} = 0.355421$. В верхнем регистре 5 кубитов, т.е. $m = 5$.
В базисе $|\alpha\rangle, |\beta\rangle$ $G = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, собств. числа равны $e^{i\theta}$ и $e^{i(2\pi-\theta)}$.

Значение первого регистра $\|x\rangle$	Вероятность получить $\|x\rangle$	$\widetilde{\theta}$	$\|\theta - \widetilde{\theta}\|$	$\widetilde{M}$	$\|M - \widetilde{M}\|$
01011	0.000480423	0.34375	0.0116712	1.87208	0.127919
01100	0.000480423	0.375	0.0195788	2.22376	0.223756
01010	0.00128371	0.3125	0.0429212	1.54983	0.450174
01101	0.00128371	0.40625	0.0508288	2.60451	0.604507
01001	0.444656	0.28125	0.0741712	1.2573	0.742696
01110	0.444656	0.4375	0.0820788	3.01396	1.01396
01000	0.000331911	0.25	0.105421	0.994803	1.0052
01111	0.000331911	0.46875	0.113329	3.45172	1.45172
00111	0.000378872	0.21875	0.136671	0.762577	1.23742
10000	0.000321445	0.5	0.144579	3.91736	1.91736
00110	0.00391337	0.1875	0.167921	0.560854	1.43915
⋮	⋮	⋮	⋮	⋮	⋮
11100	0.000568263	0.875	0.519579	11.4881	9.4881
11101	0.00091356	0.90625	0.550829	12.2655	10.2655
11110	0.0264812	0.9375	0.582079	13.0622	11.0622
11111	0.000321445	0.96875	0.613329	13.8774	11.8774

Таблица 1: Если t = 2, то сумма вероятностей по тем строкам у которых погрешность $|\theta - \widetilde{\theta}| < 0.25$ равна 0.930373 (с 1 по 16 строку). Если t = 3, то сумма вероятностей по тем строкам у которых погрешность $|\theta - \widetilde{\theta}| < 0.125$ равна 0.893504 (с 1 по 8 строку).

Квантовый разностный метод

Поиск разностных(и линейных) соотношений – квантовые алгоритмы Бернштейна-Вазирани и Саймона (см. [1], [2], [3]). Поиск итерационных ключей описан в [4], [5].

- Для $E : V_n \times V_m \to V_m$, $C = E(key, P)$, известно разностное соотношение (a, b) с характеристикой $p_{(a,b)}$. Предполагается, что на истинном ключе key:

$$P(E(key, P) \oplus E(key, P \oplus a) = b) = p_{(a,b)}, \quad p_{(a,b)} = \max_{a,b \in V_m \setminus \overrightarrow{0}} p_{(a,b)}.$$

- Известно N пар (P_i, C_i), полученных на ключе key. Необходимо по заданному разностному (линейному) соотношению (a, b) и имеющемуся материалу восстановить key.
- Согласно [4], трудоёмкость поиска итерационных ключей составляет $O(\sqrt{N}) + O(\sqrt{K})$, в то время как трудоемкость классического разностного метода авторы [4] оценивают величиной $O(N) + O(K)$, при этом длина итерационного ключа равна $log_2 K$ бит.

Восстановление итерационных ключей [4]

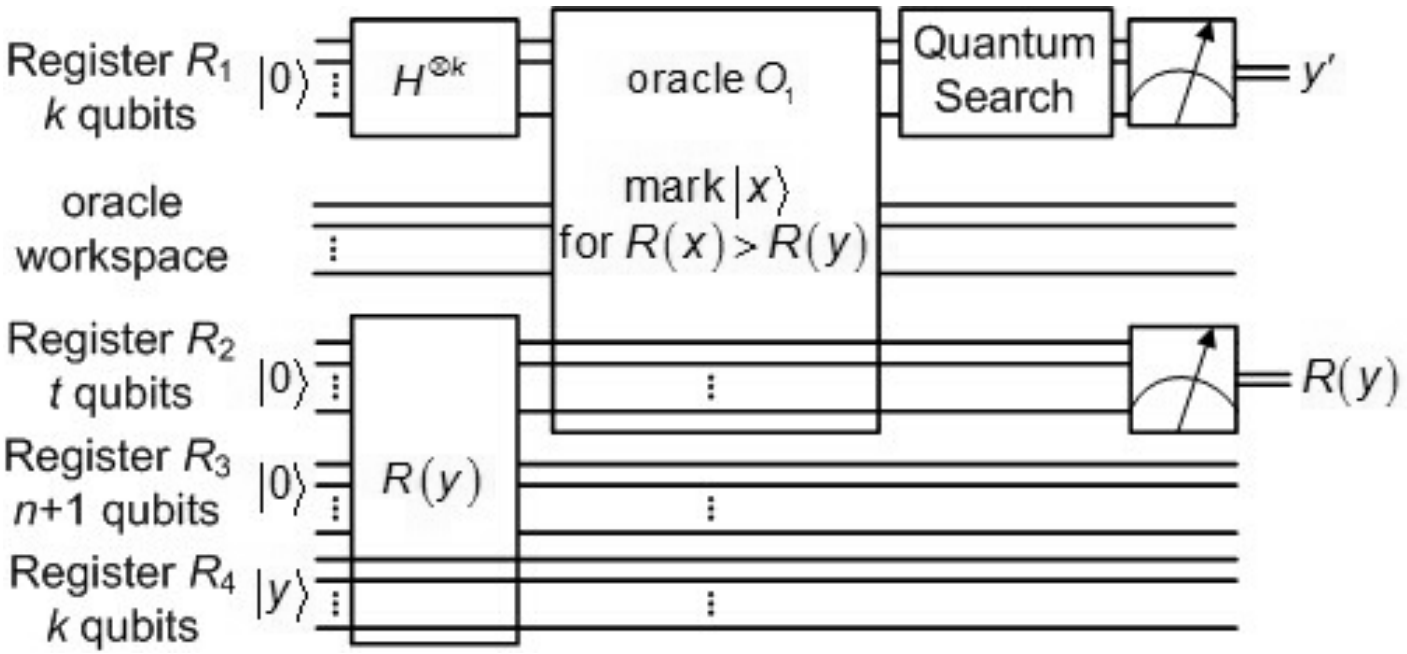

Рис. 3: Schematic circuit for the quantum differential cryptanalysis

Восстановление итерационных ключей [4]

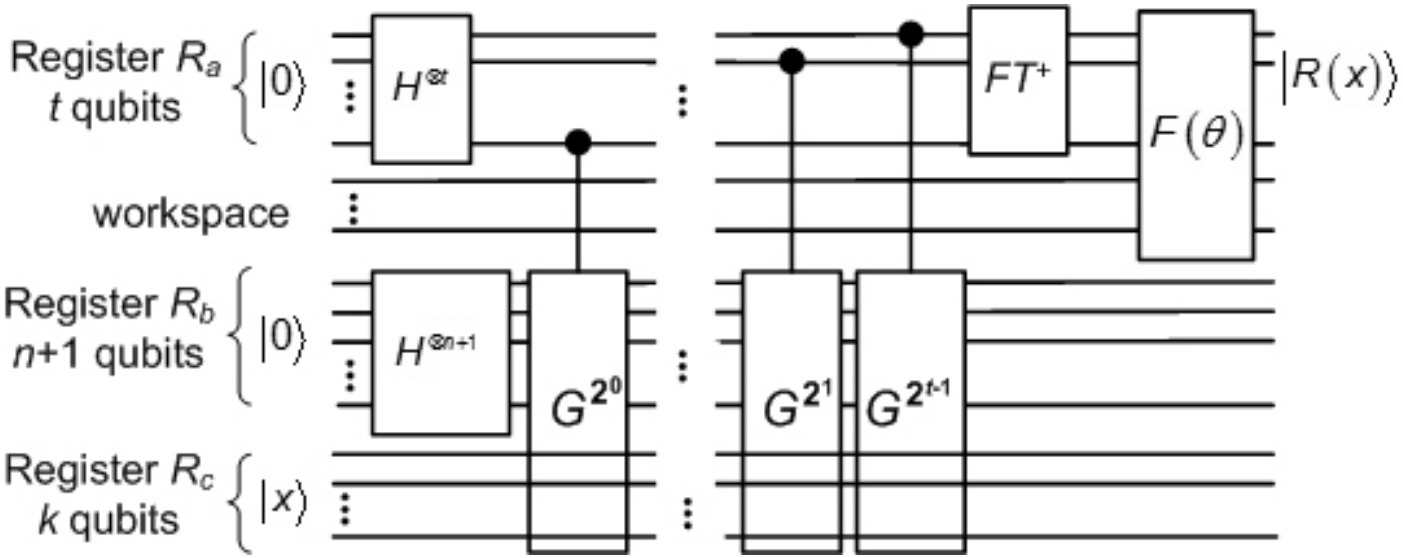

Рис. 4: Circuit for calculating $R(x)$

Комбинация алгоритмов перечисления и поиска

1. Корректная схема реализации одной итерации Гровера представлена на рисунке 5.

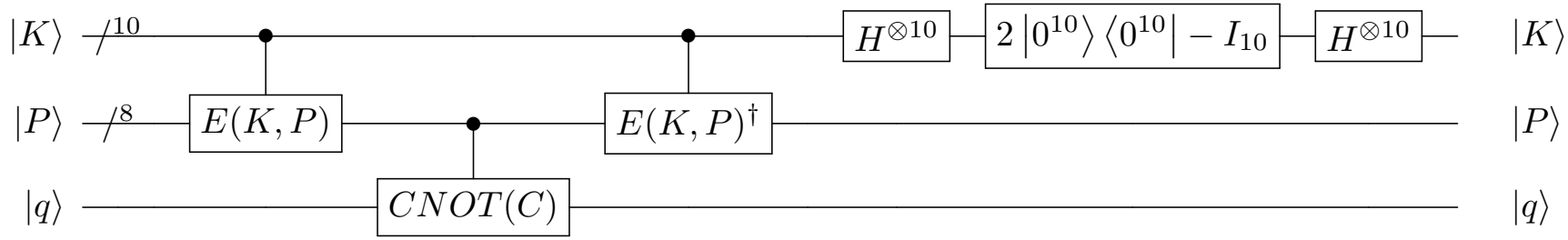

Рис. 5: Реализация одной итерации алгоритма Гровера в задаче поиска ключа учебного алгоритма шифрования SDES (см. [9]).

2. Чтобы «инверсия относительно среднего» увеличила амплитуду вероятности искомого секретного ключа, необходимо на каждой итерации алгоритма Гровера реализовывать $E(K,P)$ и $E(K,P)^{\dagger}$.

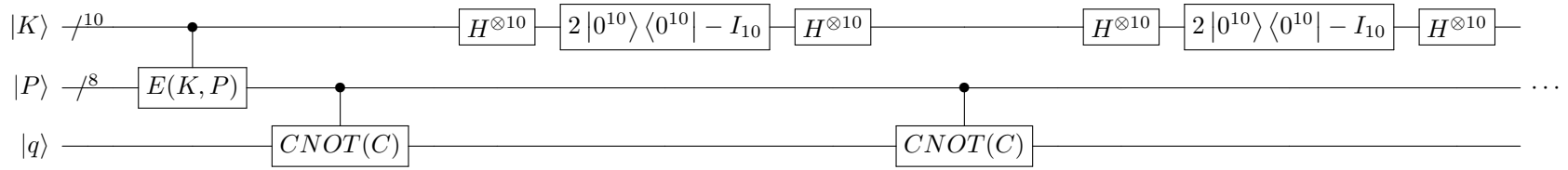

Рис. 6: Неправильная реализация итераций Гровера на примере поиска ключа SDES.

Комбинация алгоритмов перечисления и поиска

3. Следовательно, для приготовления $\sum_{K_1} \frac{1}{\sqrt{2^k}} |K_1\rangle \left|\widetilde{\theta}_{K_1}\right\rangle$ квантовое перечисление и его обращение должны выполняться на каждой итерации Гровера!

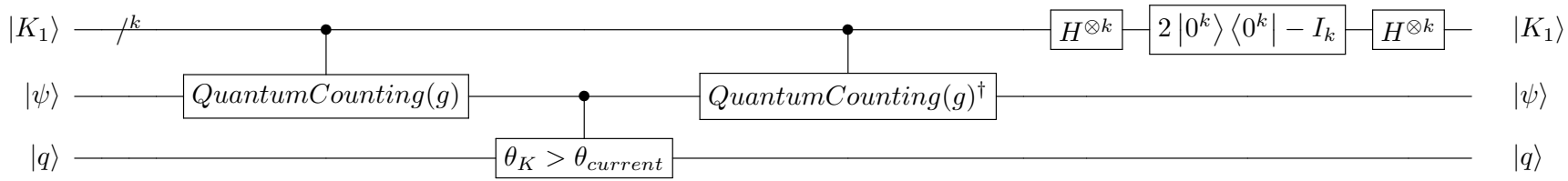

Рис. 7: Реализация одной итерации алгоритма Гровера с использованием квантового перечисления в качестве «подпрограммы».

Вывод

- Квантовое перечисление в качестве «подпрограммы» алгоритма Гровера нивелирует квантовое ускорение, т.к.

$$O(\sqrt{K}) \cdot O(\sqrt{K}) \approx O(K).$$

- Вероятность успеха алгоритма Гровера следует умножить на $\left(\frac{4}{\pi^2}\right)^{\left[\frac{\pi}{4}\sqrt{\frac{K}{M}}\right]}$.

Спасибо за внимание.

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

[2] Hong-Wei Li, Li Yang. A quantum algorithm to approximate the linear structures of Boolean functions. DOI:10.1017/S0960129516000013, https://arxiv.org/abs/1404.0611, 2015.

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

[4] Zhou Q., Lu S., Zhang A., Sun J. *Quantum differential cryptanalysis,.* https://arxiv.org/abs/1811.09931, 2019.

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

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

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

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

[9] 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.

[10] 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.

[11] Денисенко Д.В. *О реализации подстановок в виде квантовых схем без использования дополнительных кубитов*, ЖЭТФ, том 155, вып. 5, 2019. DOI: 10.1134/S00444510190600 4X.

[12] Денисенко Д.В. Применение алгоритма квантового перечисления для оценки веса булевых функций в квантовом симуляторе Quipper, готовится к печати в ЖЭТФ, 2020.