УДК 530.145

Крылова Алина Андреевна
Студент
РГУ нефти и газа (НИУ) имени И. М. Губкина

«КВАНТОВЫЕ АЛГОРИТМЫ: АЛГОРИТМ ШОРА, АЛГОРИТМ ГРОВЕРА И ИХ ЗНАЧЕНИЕ»

Аннотация: Статья посвящена исследованию двух ключевых квантовых алгоритмов — алгоритма Шора и алгоритма Гровера. Рассматриваются их математические основания, вычислительная сложность и практическое применение. Изложены фундаментальные принципы квантовых вычислений: суперпозиция, запутанность, квантовый параллелизм. Проведен сравнительный анализ с классическими методами. В практической части представлены реализации алгоритмов на языке QCEngine для интерактивной среды O'Reilly Quantum Computing Playground.

Ключевые слова: квантовые вычисления, алгоритм Шора, алгоритм Гровера, кубит, суперпозиция, квантовое преобразование Фурье, RSA, постквантовая криптография.

Krylova A.A.

Student

Gubkin Russian State University of Oil and Gas (National Research University)

«QUANTUM ALGORITHMS: SHOR'S ALGORITHM, GROVER'S ALGORITHM AND THEIR SIGNIFICANCE»

Abstract: This paper investigates two fundamental quantum algorithms — Shor's algorithm and Grover's algorithm — examining their mathematical foundations, computational complexity, and practical applications. The core principles of quantum computing are discussed: superposition, entanglement, and quantum parallelism. A comparative analysis with classical methods is conducted. The practical section presents algorithm implementations in QCEngine for the O'Reilly Quantum Computing Playground interactive environment.

Keywords: quantum computing, Shor's algorithm, Grover's algorithm, qubit, superposition, quantum Fourier transform, RSA, post—quantum cryptography.

ВВЕДЕНИЕ

Квантовые вычисления — область на стыке физики, математики и информатики, использующая квантово-механические явления для обработки информации принципиально новым способом. Интерес к ним резко возрос после публикации алгоритма Питера Шора в 1994 году: было показано, что квантовый компьютер способен факторизовать большие целые числа за полиномиальное время, что ставит под угрозу криптосистему RSA. [1] В 1996 году Лов Гровер предложил алгоритм квадратичного ускорения поиска в неструктурированных базах данных. [2]

Цель статьи — систематическое изложение принципов работы обоих алгоритмов, анализ их вычислительной сложности и практическая демонстрация в среде QCEngine. Актуальность темы обусловлена стремительным развитием квантового аппаратного обеспечения: в 2023–2025 годах IBM и Google представили квантовые процессоры с числом кубитов свыше 1000, что приближает эпоху практически значимых квантовых вычислений. [5, 10]

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КВАНТОВЫХ ВЫЧИСЛЕНИЙ

Основной единицей информации в квантовом компьютере является кубит. В отличие от классического бита, кубит может находиться в суперпозиции состояний $|0\rangle$ и $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1$$

где α, β — комплексные амплитуды вероятности. При измерении кубит с вероятностью $|\alpha|^2$ принимает значение 0, с вероятностью $|\beta|^2$ — значение 1. Система из n кубитов описывается вектором в гильбертовом пространстве размерности 2^n, что обеспечивает квантовый параллелизм. [3]

Квантовая запутанность возникает, когда состояния двух частиц нельзя описать независимо. Пример — состояние Белла:

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Измерение одного кубита мгновенно определяет состояние второго. Запутанность является ключевым вычислительным ресурсом алгоритма Шора. [3]

Квантовые вентили реализуют унитарные (обратимые) преобразования кубитов. Ключевые однокубитные вентили представлены в таблице 1. [3]

Таблица 1 — Основные квантовые вентили

Вентиль	Матрица	Действие
Адамара (H)	[[1,1],[1,−1]]/√2	Равномерная суперпозиция
Паули—X	[[0,1],[1,0]]	Квантовый NOT
Паули—Z	[[1,0],[0,−1]]	Инверсия фазы $\|1\rangle$
T—вентиль	diag(1, e^{iπ/4})	Поворот фазы на π/4

АЛГОРИТМ ШОРА

Задача факторизации состоит в нахождении нетривиальных делителей числа N. Лучший классический алгоритм — решето числового поля (GNFS) — работает за субэкспоненциальное время:

$$T_{\text{GNFS}} = O(\exp(c \cdot n^{1/3} \cdot (\log n)^{2/3}))$$

где n = $\log_2 N$. Криптосистема RSA основана на вычислительной сложности этой задачи: факторизация числа RSA—2048 потребовала бы миллионы лет на современных суперкомпьютерах. [1]

Алгоритм Шора сводит факторизацию к нахождению периода r функции $f(x) = a^x \bmod N$ для случайного a, взаимно простого с N. Связь с факторизацией — через НОД:

$$\gcd(a^{r/2} \pm 1,\ N) \rightarrow \text{нетривиальные делители } N$$

Квантовое ядро — нахождение периода — реализуется через квантовое преобразование Фурье (КПФ):

$$\mathrm{QFT}|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k/N} |k\rangle$$

КПФ для n кубитов требует $O(n^2)$ вентилей — экспоненциально меньше, чем $O(n \cdot 2^n)$ для классического БПФ. Итоговая сложность алгоритма Шора — $O(n^3)$, что представляет экспоненциальное ускорение по сравнению с GNFS. Сравнение приведено в таблице 2. [1, 3]

Таблица 2 — Сравнение алгоритма Шора с классическим GNFS

Параметр	GNFS (классика)	Алгоритм Шора
Временная сложность	O(exp(n^{1/3}·(logn)^{2/3}))	$O(n^3)$
RSA—2048 (оценка)	~10^{13} лет	~10 минут
Тип ускорения	—	Экспоненциальное

АЛГОРИТМ ГРОВЕРА

Задача неструктурированного поиска: в базе из N элементов найти x*, для которого f(x*) = 1. Классический алгоритм требует O(N) запросов. Алгоритм Гровера решает задачу за $O(\sqrt{N})$ квантовых запросов — это оптимально согласно квантовой нижней оценке Беннетта–Бойера–Брасара–Хойера. [2, 8]

Инициализация: вентиль Адамара создает равномерную суперпозицию:

$$|s\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{x} |x\rangle$$

Каждая итерация G = D · Of включает: (1) оракул Of инвертирует фазу целевого элемента:

$$O_f|x\rangle = (-1)^{f(x)}|x\rangle$$

(2) Оператор диффузии $D = 2|s\rangle\langle s| - I$ усиливает отклонение амплитуды от среднего. Геометрически — поворот вектора состояния на угол 2θ, где $\sin\theta = 1/\sqrt{N}$. Оптимальное число итераций:

$$k_{\mathrm{opt}} = \left\lfloor \frac{\pi}{4\theta} \right\rfloor \approx \frac{\pi}{4} \cdot \sqrt{N}$$

После k_opt итераций вероятность измерить целевое состояние близка к 1. Сравнение с классическим поиском приведено в таблице 3.

Таблица 3 — Сравнение алгоритма Гровера с классическим поиском

Параметр	Классический поиск	Алгоритм Гровера
Сложность	O(N)	O(√N)
$N = 10^6$	1 000 000 запросов	1 000 запросов
$N = 10^{12}$	10^{12} запросов	10^6 запросов
Оптимальность	Нижняя граница Ω(N)	Квантово—оптимальный

СРАВНИТЕЛЬНЫЙ АНАЛИЗ

Алгоритм Шора демонстрирует экспоненциальное превосходство для алгебраической задачи факторизации, эксплуатируя периодическую структуру через КПФ. Алгоритм Гровера дает квадратичное ускорение для широкого класса задач поиска без предположений о структуре данных. С точки зрения постквантовой криптографии:

– алгоритм Шора полностью компрометирует RSA, ECC и системы на основе дискретного логарифма; [6]

– алгоритм Гровера снижает эффективную длину ключа симметричных шифров вдвое: AES—128 становится эквивалентен 64—битной стойкости; [6]

– NIST завершил стандартизацию постквантовых алгоритмов в 2024 году, утвердив CRYSTALS—Kyber, CRYSTALS—Dilithium и FALCON. [7]

Таблица 4 — Сводное сравнение алгоритмов

Характеристика	Алгоритм Шора	Алгоритм Гровера
Задача	Факторизация чисел	Поиск в неструкт. БД
Тип ускорения	Экспоненциальное	Квадратичное
Сложность	$O(n^3)$	O(√N)
Угроза для крипто	RSA, ECC (полная)	AES (частичная)

ПРАКТИЧЕСКАЯ ЧАСТЬ

Для реализации алгоритмов используется интерактивная среда O'Reilly Quantum Computing Playground: https://oreilly—qc.github.io. [4]

Пример 1. Алгоритм Гровера, N=4: поиск $|11\rangle$ (k_opt = 1, P = 100%)

```
// Алгоритм Гровера: поиск |11> в базе из N=4 элементов (2 кубита)
var num_qubits = 2;
qc.reset(num_qubits);
// Инициализация — равномерная суперпозиция
qc.had(0x3);
qc.label('Суперпозиция'); qc.nop();
// Шаг 2: Оракул — инвертирует фазу целевого |11>
qc.label('Оракул: инверсия фазы |11>');
qc.phase(180, 0x3); qc.nop();
// Диффузия Гровера
qc.label('Диффузия');
qc.had(0x3); qc.not(0x3);
qc.phase(180, 0x3);
qc.not(0x3); qc.had(0x3); qc.nop();
// Измерение (ожидается 3, P=1.0)
var result = qc.read(0x3);
qc.print('Результат: ' + result + ' (ожидается 3)');
```

Результат выполнения: Program output отображает «Результат: 3». Circle Notation демонстрирует полное амплитудное усиление: амплитуда состояния $|3\rangle = 1{,}0$, остальных — 0.

Пример 2. Алгоритм Гровера, N=8: поиск $|101\rangle$ (2 итерации)

$$k_{\text{opt}} = 2, \quad P_{\text{успех}} = \sin^2(5\theta) \approx 0{,}945, \quad \theta = \arcsin\left(\frac{1}{\sqrt{8}}\right)$$

```
// Алгоритм Гровера: поиск |101> (=5) в N=8, 2 итерации
var num_qubits = 3; qc.reset(num_qubits);
function grover_step() {
  qc.not(0x2); qc.phase(180, 0x7); qc.not(0x2);
  qc.had(0x7); qc.not(0x7);
  qc.phase(180, 0x7);
  qc.not(0x7); qc.had(0x7);
}
qc.had(0x7); qc.nop();
for (var i = 0; i < 2; i++) {
  qc.label('Итерация ' + (i+1)); grover_step(); qc.nop();
}
var result = qc.read(0x7);
qc.print('Результат: ' + result + ' (ожидается 5, P≈0.945)');
```

Пример 3. Квантовое преобразование Фурье (3 кубита)

$$R_k: \quad r_{00} = 1,\ r_{01} = 0,\ r_{10} = 0,\ r_{11} = e^{2\pi i/2^k}$$

```
// QFT — ядро алгоритма Шора. Вход: |010> = |2>
qc.reset(3); qc.write(2, 0x7);
qc.label('Вход |010>'); qc.nop();
```

```
qc.had(0x4);
qc.cphase(90, 0x2, 0x4);   // R2: π/2
qc.cphase(45, 0x1, 0x4);   // R3: π/4
qc.had(0x2);
qc.cphase(90, 0x1, 0x2);   // R2: π/2
qc.had(0x1);
qc.swap(0x1, 0x4);         // SWAP: реверс порядка битов
qc.label('QFT завершено'); qc.nop();
```

Пример 4. Обнаружение периода — ядро алгоритма Шора

```
// Обнаружение периода r=4 через QFT (4 кубита, N=16)
qc.reset(4);
qc.had(0xC);
qc.label('Период r=4'); qc.nop();
// QFT для 4 кубитов
qc.had(0x8);
qc.cphase(90,0x4,0x8); qc.cphase(45,0x2,0x8); qc.cphase(22.5,0x1,0x8);
qc.had(0x4); qc.cphase(90,0x2,0x4); qc.cphase(45,0x1,0x4);
qc.had(0x2); qc.cphase(90,0x1,0x2); qc.had(0x1);
qc.swap(0x1,0x8); qc.swap(0x2,0x4);
qc.label('Пики в 0,4,8,12 => период r=4'); qc.nop();
var result = qc.read(0xF);
var period = result > 0 ? 16/result : 'inf';
qc.print('Измерено: '+result+',  r = 16/'+result+' = '+period);
```

ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Практические эксперименты в среде QCEngine подтвердили теоретические предсказания. В Примере 1 (Гровер, N=4) однократная итерация переводит амплитуду целевого состояния от 0,5 до 1,0 — вероятность успеха 100%, что точно соответствует k_opt=1. В Примере 2 (N=8) две итерации дают вероятность ≈ 94,5% — полное совпадение с теоретической оценкой.

В Примере 4 периодическое состояние — суперпозиция {0, 4, 8, 12} с периодом r=4 — после применения КПФ концентрирует вероятность в четырех точках: 0, 4, 8, 12. Поскольку N=16, а пики отстоят на 4 = N/r, правильно извлекается период r=4. На реальных устройствах для взлома RSA—2048 потребуется порядка нескольких миллионов физических кубитов с коррекцией ошибок. По современным оценкам, это станет реальным не ранее 2030–2035 годов.

ВЫВОДЫ

Проведено систематическое исследование алгоритмов Шора и Гровера. Изложены математические основы квантовых вычислений и показано, что оба алгоритма эксплуатируют квантовые явления — суперпозицию, запутанность и интерференцию — для достижения преимуществ, недоступных классическим методам. [3, 9]

Алгоритм Шора обеспечивает экспоненциальное ускорение факторизации: $O(n^3)$ против субэкспоненциального GNFS, что напрямую угрожает системам RSA и ECC. Алгоритм Гровера дает квадратичное ускорение $O(\sqrt{N})$ при поиске и является оптимальным квантовым алгоритмом для данного класса задач. Практическая реализация в QCEngine подтвердила все теоретические результаты. Все примеры кода воспроизводимы на https://oreilly—qc.github.io.

Перспективы дальнейших исследований: вариационные алгоритмы QAOA и VQE для NISQ—устройств, алгоритм HHL для систем линейных уравнений, разработка постквантовых криптографических протоколов. [5]

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ:

1. Shor P.W. Polynomial—Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Journal on Computing. — 1997. — Vol. 26, No. 5. — P. 1484–1509.
2. Grover L.K. A Fast Quantum Mechanical Algorithm for Database Search // Proceedings of the 28th Annual ACM Symposium on Theory of Computing. — ACM, 1996. — P. 212–219.
3. Nielsen M.A., Chuang I.L. Quantum Computation and Quantum Information. — Cambridge University Press, 2010. — 702 p.
4. Johnston E., Harrigan N., Gimeno—Segovia M. Programming Quantum Computers: Essential Algorithms and Code Samples. — O'Reilly Media, 2019. — 360 p.

5. Preskill J. Quantum Computing in the NISQ era and beyond // Quantum. — 2018. — Vol. 2. — P. 79. DOI: 10.22331/q—2018—08—06—79.
6. Bernstein D.J., Lange T. Post—quantum cryptography // Nature. — 2017. — Vol. 549. — P. 188–194. DOI: 10.1038/nature23461.
7. NIST. Post—Quantum Cryptography: Final Standards FIPS 203, FIPS 204, FIPS 205. — National Institute of Standards and Technology, 2024. — URL: https://csrc.nist.gov/pubs/fips/203/final (дата обращения: 01.05.2026).
8. Montanaro A. Quantum algorithms: an overview // npj Quantum Information. — 2016. — Vol. 2. — 15023. DOI: 10.1038/npjqi.2015.23.
9. Aaronson S. Quantum Computing Since Democritus. — Cambridge University Press, 2013. — 398 p.
10. Arute F. et al. Quantum supremacy using a programmable superconducting processor // Nature. — 2019. — Vol. 574. — P. 505–510. DOI: 10.1038/s41586—019—1666—5.