# Секция «Теория кодирования и математические вопросы защиты информации»

## ВЕРХНИЕ ОЦЕНКИ СЛОЖНОСТИ РЕАЛИЗАЦИИ КВАНТОВОГО ОРАКУЛА ДЛЯ ЗАДАЧИ НАХОЖДЕНИЯ КРАТЧАЙШЕГО ВЕКТОРА ЦЕЛОЧИСЛЕННОЙ РЕШЁТКИ

**А. О. Бахарев (Новосибирск)**

В силу развития квантовых вычислений возникает необходимость в разработке и анализе криптосистем, устойчивых к атакам с использованием квантового компьютера — алгоритмов постквантовой криптографии. Важными направлениями анализа постквантовых криптосистем являются построение и исследование квантовых схем, которые могут быть использованы для атак на данные криптосистемы. Одним из подходов к разработке постквантовых криптосистем является подход на основе решёток.

**Определение.** Пусть $u_1, \ldots, u_d \in \mathbb{R}^n$ линейно независимые векторы и $d \leq n$. *Решёткой размерности* $d$ называется множество

$$\mathbb{Z}u_1 \oplus \ldots \oplus \mathbb{Z}u_d = \Big\{ \sum_{i=1}^{d} b_i u_i | b_i \in \mathbb{Z} \Big\}.$$

Линейно независимая система векторов, порождающая решётку, называется *базисом решётки*.

В данной работе рассматриваются целочисленные решётки.

**Определение.** *Задача нахождения кратчайшего вектора (SVP)* — найти в заданной своим базисом решётке вектор, имеющий наименьшую длину.

В общем случае SVP является NP-трудной задачей. Стойкость систем, основанных на решётках, зависит от эффективности решения SVP, так как большинство известных атак сводятся к решению этой проблемы. Перспективными являются разработка и анализ квантовых алгоритмов, которые позволяют ускорить решение данной задачи.

Одним из самых эффективных классических алгоритмов решения SVP является алгоритм GaussSieve [4]. Самой трудозатратной операцией этого алгоритма является поиск в неупорядоченном списке элемента, удовлетворяющего условию поиска, так как размер списка увеличивается экспонециально с ростом размерности решётки. В статье [3] представлен гибридный подход к ускорению алгоритма GaussSieve, который использует квантовый алгоритм поиска в неупорядоченном списке.

Задача, состоящая в поиске элемента в неупорядоченном списке, называется *задачей поиска*. Предполагается, что есть неупорядоченный список из $K$ элементов, и требуется найти один элемент, удовлетворяющий некоторому условию. Другими словами, определена булева функция $f$, которая по номеру элемента (его двоичному представлению $x$) определяет, является ли элемент подходящим. Если элемент подходящий, то $f(x) = 1$, иначе $f(x) = 0$. В такой постановке задача поиска сводится к нахождению решения уравнения $f(x) = 1$.

В классическом варианте при условии, что решение одно, требуется $\sim K/2$ обращений к функции $f$ для нахождения решения. Квантовый алгоритм поиска элемента в неупорядоченном списке (алгоритм Гровера [2]) решает данную задачу за $\sim \sqrt{K}$ обращений к *оракулу* — квантовому аналогу функции $f$. Известно, что любая булева функция может быть реализована на квантовом компьютере. В данной работе для построения квантового оракула рассматривается подход, минимизирующий используемое количество *кубит* [5].

В работе [1] была предложена модель оракула, при которой список хранится в квантовой памяти. Для данной модели в настоящей работе получены новые уточнённые верхние оценки сложности реализации.

**Теорема 1.** *Пусть имеется список длины $K$, состоящий из целочисленных векторов размерности $d \geq 2$, каждая координата которых кодируется битовой строкой длины $m \geq 3$. Тогда для реализации квантового оракула, при котором список хранится в квантовой памяти, потребуется не более*

$$\lceil \log_2 K \rceil + 2^{\lceil \log_2 K \rceil} + Kdm + 3dm^2 + 13dm + 2d + 6m + 3\lceil \log_2 d \rceil + 3$$

*кубит. При этом глубина схемы не превосходит*

$$2 \cdot 3^{\lceil \log_2 K \rceil} + 2K(2\lceil \log_2 dm \rceil + 1) + 20m^2 + 4\lceil \log_2 m \rceil + 21 + \lceil \log_2 d \rceil (3\lceil \log_2 d \rceil + 12m + 5).$$

Как видно из теоремы 1, верхняя асимптотическая оценка сложности реализации данной модели оракула равна $\mathcal{O}(Kdm + dm^2)$ кубит. Таким образом, хранение списка в квантовой памяти приводит к линейному росту используемого числа кубит от длины $K$, которая растёт экспоненциально с увеличением размерности решётки.

В настоящей работе предложена новая модель оракула, при которой список хранится в классической памяти. Получены верхние оценки сложности реализации данной модели.

**Теорема 2.** *Пусть имеется список длины $K$, состоящий из целочисленных векторов размерности $d \geq 2$, каждая координата которых кодируется битовой строкой длины $m \geq 3$. Тогда для реализации квантового оракула, при котором неупорядоченный список хранится в классической памяти, потребуется не более*

$$\lceil \log_2 K \rceil + 13dm + 5d + 6m + 3\lceil \log_2 d \rceil + 3 + \\ + \max(3d(m^2 - 1), \lceil \log_2 K \rceil + \lceil \frac{dm}{4} \rceil - 3)$$

*кубит. При этом глубина схемы не превосходит*

$$2^{\lceil \log_2 K \rceil + 2} - 4\lceil \log_2 K \rceil + \lceil \log_2 dm \rceil (2^{\lceil \log_2 K \rceil + 1} - 2) + 20m^2 + \\ + \lceil \log_2 d \rceil (3\lceil \log_2 d \rceil + 12m + 5) + 4\lceil \log_2 m \rceil + 15.$$

Как видно из теоремы 2, верхняя асимптотическая оценка сложности реализации данной модели оракула равна $\mathcal{O}(\log_2 K + dm^2)$ кубит. Следовательно, число кубит, используемое для реализации квантового оракула с классическим списком, растёт логарифмически от длины списка. Однако, хранение списка в классической памяти приводит к её экспоненциальному росту от размерности решётки.

Работа выполнена при поддержке Математического Центра в Академгородке, соглашение с Министерством науки и высшего образования Российской Федерации номер 075-15-2022-281.

**Список литературы**

1. Бахарев А. О. Разработка и анализ оракула для гибридной атаки на криптографическую систему NTRU с использованием алгоритма квантового поиска // Прикладная дискретная математика. Приложение. — 2021. — № 14. — С. 62–67.

2. Grover L. K. A fast quantum mechanical algorithm for database search // Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. — 1996. — P. 212–219.

3. Laarhoven T., Mosca M., van de Pol J. Finding shortest lattice vectors faster using quantum search // Designs, Codes and Cryptography 77. — 2015. — № 2. — P. 375–400.

4. Micciancio D., Voulgaris P. Faster exponential time algorithms for the shortest vector problem // Proceedings of the twenty-first annual ACM-SIAM symposium on Discrete Algorithms. Society for Industrial and Applied Mathematics. — 2010. — P. 1468–1480.

5. Nielsen M. A., Chuang I. L. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2010.

DOI: 10.20948/dms-2022-79

# О МОЩНОСТИ ОБРАЗА ПРАВИЛЬНЫХ СЕМЕЙСТВ БУЛЕВЫХ ФУНКЦИЙ

**А. В. Галатенко, В. А. Носов, А. Е. Панкратьев, К. Д. Царегородцев (Москва)**

Конечные квазигруппы являются перспективной структурой для реализации различных криптографических примитивов [1, 2]. Табличное задание квазигрупповой операции требует квадатичного от порядка квазигруппы объема памяти; как следствие, при использовании квазигрупп большого порядка становится актуальной задача минимизации пространственной сложности. Одно из возможных решений — переход от табличного задания операции к функциональному. В. А. Носовым была предложена конструкция, основанная на правильных семействах функций и позволяющая задавать большие параметрические семества квазигрупп большого порядка [3]. В работе [4] были анонсированы результаты о мощности множества квазигрупп, порождаемых заданным правильным семейством. Оказалось, что эта мощность оценивается снизу с помощью функции от мощности образа правильного семейства. В нашей работе представлен ряд результатов о мощности образа правильных семейств булевых функций.

**Определение.** Пусть $n \in \mathbb{N}$. Семейство $(g_1, \ldots, g_n)$ булевых функций арности $n$ называется правильным, если для любой пары различных входных наборов $\alpha = (a_1, \ldots, a_n)$ и $\beta = (b_1, \ldots, b_n)$ найдется индекс $i$, $1 \leq i \leq n$, такой что $a_i \neq b_i$, но $g_i(\alpha) = g_i(\beta)$.