Решение некоторых задач криптографического анализа схем на основе целочисленных решеток с использованием метода квантовой нормализации

Лысаков Иван Вячеславович

Студент

Факультет ВМК МГУ им. М. В. Ломоносова, Москва, Россия

E-mail: lysakoviv@my.msu.ru

Научный руководитель *— Применко Эдуард Андреевич*

Модель квантовых вычислений, предложенная Д. Дойчем в 80-х годах прошлого века, является развитием теории вычислений А. Тьюринга. Известно, что в квантовой модели вычислений существуют эффективные алгоритмы решения сложных математических задач, на предположении о вычислительной сложности которых основывается стойкость подавляющего большинства современных асимметричных криптографических схем.

С течением времени появлялись новые модели вычислений, основанные на принципах квантовой механики. В наших исследованиях рассмотрена адиабатическая модель вычислений. Считается, что в ней возможно эффективное решение ряда задач оптимизации на дискретных множествах.

Предполагается, что семейство криптографических схем, стойкость которых основана на задачах из теории решеток, устойчиво к атакам с использованием квантового или адиабатического вычислителя. Зачастую в качестве такой задачи используется задача поиска ближайшего вектора (closest vector problem, CVP). Однако для вскрытия системы не всегда необходимо полностью решать CVP, иногда для этого достаточно решить более простую задачу - задачу декодирования с ограниченным расстоянием (bounded distance decoding, BDD_γ). Параметр γ в этой задаче отвечает за степень удаленности ближайшего вектора от заданного.

В статье [2] представлен алгоритм, позволяющий решить задачу поиска кратчайшего вектора (shortest vector problem, SVP) в адиабатической системе вычислений. В этой же работе дана оценка сверху на количество кубит, требуемых при решения данной задачи для решетки размерности N с абсолютным значением определителя равным D.

$$\frac{3\,N}{2}\log N + N + \log D.$$

Нами было предложено обобщение упомянутого выше алгоритма на задачи поиска ближайшего вектора и декодирования с ограниченным расстоянием. Также была получена оценка на число кубит, требуемых для решения задачи декодирования с ограниченным расстоянием с параметром γ для решеток, у которых существует эрмитова нормальная форма с единственным ведущим элементом, отличным от единицы.

Теорема 1. *Для решетки Λ размерности N с эрмитовой нормальной формой, у которой только один ведущий элемент отличен от 1, и определителем, равным по модулю D, существует квантовый алгоритм в адиабатической модели вычислений решения задачи BDD_γ для точки $t \notin \Lambda$, требующий не более чем $N \log(2\,\gamma\, N^{3/2}\, D^{1/N} + \|t\|_{L_1})$ кубит.*

Также была дана оценка на количество кубит, требуемых для работы предложенного нами алгоритма с решетками, определенными открытыми ключами криптосистемы NTRUEncrypt [3] (схема-участница конкурса NIST PQC). Для системы с параметрами безопасности N и q потребуется не больше следующего числа кубит:

$$2\,N \log(\gamma\, 2\sqrt{2}\, N^{3/2}\, q^{1/2} + N\, q).$$

Для достижения уровня стойкости в 128 бит, создателями было предложено выбрать $N = 509$ и $q = 2048$ [3]. Это означает, что для решения задачи декодирования с ограниченным расстоянием с параметром $\gamma = 1$ будет задействовано примерно 21000 кубит.

Литература

1. Cohen H. A Course in Computational Algebraic Number Theory. Springer, Berlin, 1993.
2. Joseph D., Callison A., Ling C., Mintert F. Two quantum Ising algorithms for the shortest-vector problem, Physical Review A, 2021, Vol. 103, no. 3.
3. NTRU NIST submission 2020: https://ntru.org/release/NIST-PQ-Submission-NTRU-20201016.tar.gz