СЕКЦИЯ «СИСТЕМ ТЕЛЕКОММУНИКАЦИЙ»

УДК 621.391

ОЦЕНКА СЛОЖНОСТИ АЛГОРИТМА ОБУЧЕНИЯ С ОШИБКАМИ АЛГЕБРАИЧЕСКИХ РЕШЕТЧАТЫХ КОДОВ

Алисеенко М.А.[1], аспирант

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Саломатин С.Б. – канд. тех. наук, доцент

Аннотация. Показана временная сложность вычисления алгоритма LWE, реализованного на языке программирования Python, для различных длин открытого сообщения и наличия ошибок.

Ключевые слова. Алгоритм обучения с ошибками, LWE, алгебраические решетки.

Одной из задач разработки алгоритмов защиты данных является их потенциальная способность противостоять различного вида атакам, в том числе на основе пост-квантовых и параллельных вычислений. Применение алгоритмов теории многомерных алгебраических решеток предоставляют возможность формирования пространственно-временного многообразия кодовых криптографических структур [1–4].

Алгоритм алгоритма обучения с ошибками LWE [5] реализован на Python 3.8.7 с использованием модуля numpy. Среднее время вычислений рассчитано из 20 измерений на каждую длину открытого текста с использованием встроенного модуля time. При вычислениях использовались следующие параметры: n=3, m=3, t=10, r=9, q=23, длина сообщения l, состоящего из случайных целых чисел от 0 до r, варьировалась от 2^1 до 2^{20}.

Результаты вычислений представлены в таблице и на рисунке 1 (график построен использованием модуля matplotlib). Сложность вычислений растет экспоненциально.

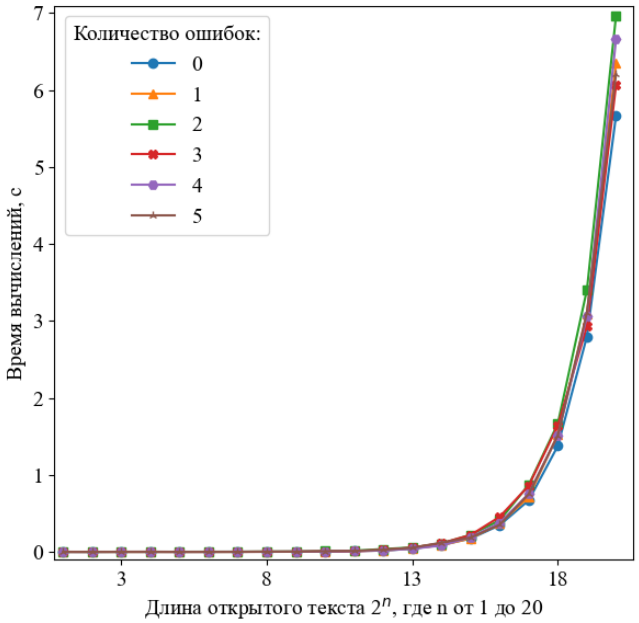

Рисунок 1 – График зависимости среднего времени вычислений в секундах от количества символов открытого текста и наличия ошибок

В настоящее время важность задачи разработки алгоритмов защиты данных определена их потенциальной способностью противостояния к разного рода атакам, таким как постквантовые и параллельные вычисления. Актуальной проблемой становится поиск быстрых алгоритмов шифрования с минимальной вычислительной сложностью для систем связи в сенсорных сетях. Временная сложность алгоритма обучения с ошибками LWE алгебраических

решетчатых кодов растет экспоненциально по мере увеличения длины открытого текста, что необходимо учитывать в аппаратном обеспечении устройств интернета вещей.

Список использованных источников:

1. Low complexity lattice codes for communication networks / Ferdinand N. S. // University of Oulu Graduate School, 2016. – P. 178.

2. The Geometry of Numbers / Olds C.D. // Mathematical Association of USA, 2012. – P. 192.

3. Quadratic integers and Coxeter groups / Johnson N. W., Weiss A. I. // Canadian Journal of Mathematics, 1999. – P. 192.

4. Stallings W. Cryptography and Network Security: Principles and Practice / Stallings W. – Prentice-Hall, Upper Saddle River, New-Jersey, fifth edition, 2006. – P 592.

5. Защита каналов передачи и хранения данных на основе алгебраических решетчатых кодов / М.А. Алисеенко, С.Б. Саломатин // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: материалы междунар. науч.-техн. семинара (Республика Беларусь, Минск, ноябрь – декабрь 2020 г.). Минск : БГУИР, 2020. – С. 23-27.