УДК 519.7

А.В. КОНОВАЛОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

АНАЛИЗ КОРРЕКТНОСТИ И СТОЙКОСТИ ШИФРСИСТЕМЫ UFHE-ILC

Целью работы является анализ семейства, основанного на круговом поле, неограниченной полностью гомоморфной шифрсистемы UFHE-ILC, предложенной [1]. В ходе исследования выявлена неточность в процедуре генерации ключей, связанная с проверкой взаимной простоты идеалов, и предложен корректный критерий. Основным результатом является разработка и реализация полиномиального алгоритма восстановления секретного ключа, основанного на поиске целочисленного корня специально построенного многочлена.

В [1] была предложена неограниченная полностью гомоморфная шифрсистема (UFHE-ILC), основанная на идеальных решётках в кольце многочленов $\mathbb{Z}[x]/g(x)$ и китайской теореме об остатках. Для практического применения авторы представили семейство данной системы, где в качестве $g(x)$ выбирается круговой многочлен $g(x) = x^{p-1} + \cdots + x + 1$ для простого p, а закрытый ключ строится на основе главных идеалов вида $\Lambda_{q_i} = < x^{p-2} + q_i >$. Безопасность системы, согласно авторам, основывается на сложности задачи нахождения корня многочлена высокой степени.

Во-первых, был проанализирован алгоритм генерации ключей. В [1] утверждается, что для взаимной простоты идеалов Λ_{q_1} и Λ_{q_2} достаточно взаимной простоты чисел q_1 и q_2. Было показано, что это утверждение неверно. На основании работ [2, 3] сформулирован и доказан точный критерий:

Теорема 1. *Идеалы Λ_{q_1} и Λ_{q_2} взаимно просты тогда и только тогда, когда взаимно просты их одномерные модули $t(\Lambda_{q_1})$ и $t(\Lambda_{q_2})$, где $t(\Lambda_q) = g(-q)$.*

Таким образом, для корректной генерации ключей необходимо выполнять проверку $\text{НОД}\big(g(-q_1),\ g(-q_2)\big) = 1$.

Во-вторых, была продемонстрирована уязвимость системы. Открытый ключ содержит значение одномерного модуля $t = t(\Lambda_q) = g(-q)$. Задача восстановления секрета q сводится к нахождению целочисленного корня многочлена $h(x) = g(-x) - t$.

Теорема 2. *Пусть задано значение одномерного модуля* $t = g(-q)$ *и параметр* $r = O(1)$. *Тогда секретный параметр* q *может быть восстановлен за полиномиальное время от* $\deg g$ *и* $\log q$.

Шаги алгоритма:

1. Выбрать набор простых чисел $p_1, \dots, p_r$.
2. Для каждого p_i находятся корни многочлена $h(x)$ $(mod\ p_i)$. Шаг основан на вероятностных методах факторизации над конечными полями, в частности на алгоритме Кантора-Зассенхауса [4].
3. С помощью китайской теоремы об остатках из наборов корней по разным модулям восстанавливаются кандидаты на целочисленный корень q'.
4. Выполняется проверка $h(q') = 0$.

Сложность алгоритма оценивается как $O(\log^2 q \cdot \deg^{O(1)} g)$.

Эффективность шага 2, ключевого для практической реализации атаки, была подтверждена моделированием. Эксперименты по факторизации многочленов степени n показали, что среднее число итераций алгоритма Кантора-Зассенхауса демонстрирует логарифмический рост, при этом распределение числа итераций сконцентрировано вокруг среднего значения, что иллюстрируется табл. 1.

Таблица 1. Результаты моделирования алгоритма Кантора-Зассенхауса.

n	Среднее число итераций	Медиана	Стандартное отклонение
5	4.85	4	1.71
10	6.86	7	1.78
20	8.89	9	1.77
30	10.07	10	1.80
40	10.93	11	1.86
50	11.54	11	1.80

Список литературы

1. Zheng Zhiyong, Liu Fengxia, Tian Kun. An Unbounded Fully Homomorphic Encryption Scheme Based on Ideal Lattices and Chinese Remainder. 2023, arXiv:2301.12060.

2. Marcus Daniel A. Number Fields. Universitext. 2 ed, Springer, 2018, ISBN: 978-3-319-90232-6.

3. Buhler Jonathan. Resultants, Discriminants, Bezout, Nullstellensatz, etc. Algebraic Number Theory Class Notes, Reed College, https://people.reed.edu/~jpb/alg/notes/101.pdf.

4. Joachim von zur Gathen, Panario Daniel. Factoring Polynomials Over Finite Fields: A Survey // Journal of Symbolic Computation, 2001, Vol. 31, no. 1–2, p. 3–17.