УДК 003.26.09

Шевченко А. Є., здобувач
Ядуха Д. В., асистент
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

АНАЛІЗ СТІЙКОСТІ МОДИФІКОВАНОЇ КРИПТОСИСТЕМИ AJPS-1 З УЗАГАЛЬНЕНИМИ ЧИСЛАМИ МЕРСЕННА ДО АТАК НА ОСНОВІ РЕШІТОК

В 2017 році у межах конкурсу постквантових криптопримітивів NIST [1] було запропоновано механізм інкапсуляції ключів Mersenne-756839, що побудований на основі криптосистеми AJPS. В будові криптосистеми використовується арифметика за модулем числа Мерсенна, а також обмеження ваги Геммінга секретних параметрів. Однією з версій криптосистеми AJPS є схема шифрування біту повідомлення – криптосистема AJPS-1 [2]. Стійкість криптосистеми AJPS-1 ґрунтується на складності задачі ділення чисел з малою вагою Геммінга за модулем числа Мерсенна (MLHRSP).

Означення 1 (Задача MLHRSP). Нехай є $M_n = 2^n - 1$, $n \in N$ – число Мерсенна, додатне ціле число h та нехай F та G – два випадкові лишки за модулем M_n, що мають вагу Геммінга h. Число H обчислюється як $H = F \cdot G^{-1} \pmod{M_n}$. За відомими H, h, M_n необхідно знайти F і G.

На сьогодні задача MLHRSP вважається обчислювально складною, оскільки до неї було застосовано ряд атак, наприклад, «Вгадай і виграй», «Зустріч посередині», а також атака на основі алгоритму LLL, проте жодна з них не змогла розв'язати задачу MLHRSP для рекомендованих розмірів параметрів криптосистеми.

У [3] побудовано модифікацію AJPS-1, що використовує узагальнені числа Мерсенна. Стійкість такої модифікації ґрунтується на складності задачі GMLHRSP.

Означення 2 (Задача GMLHRSP). Маючи узагальнене число Мерсенна $M_{n,m} = 2^n - 2^m - 1$, $n \in N$, $m \in N$, $m < n$, число H та значення h, необхідно знайти два числа F та G, що мають вагу Геммінга h, які задовольняють співвідношенню $H = F \cdot G^{-1} \pmod{M_{n,m}}$.

Для аналізу складності задачі GMLHRSP необхідно дослідити можливість застосування проведених атак на оригінальну задачу MLHRSP та перевірити їхню результативність у разі використання альтернативних модулів.

Розглянемо атаку на основі алгоритму LLL для задачі GMLHRSP. Нехай маємо рівняння $H = F \cdot G^{-1} \pmod{M_{n,m}}$. Помноживши його на G,

отримаємо $H \cdot G = F \pmod{M_{n,m}}$. Представивши секретні параметри F та G через суму степенів двійки, тобто $G = \sum_{i=0}^{n-1} g_i \cdot 2^i$, $g_i \in \{0, 1\}$ та $F = \sum_{j=0}^{n-1} f_j \cdot 2^j$, $f_j \in \{0, 1\}$, маємо рівняння $H \cdot \sum_{i=0}^{n-1} g_i \cdot 2^i = \sum_{j=0}^{n-1} f_j \cdot 2^j \pmod{M_{n,m}}$. Перенесемо усі доданки у ліву частину рівняння та замінимо редукцію за модулем $M_{n,m}$ на віднімання даного модуля t разів. Тепер початкове співвідношення має вигляд $H \cdot \sum_{i=0}^{n-1} g_i \cdot 2^i - \sum_{j=0}^{n-1} f_j \cdot 2^j - t \cdot M_{n,m} = 0$. Домноживши отриманий вираз на достатньо великий множник K, отримаємо $K \cdot \sum_{i=0}^{n-1} g_i \cdot 2^i \cdot H - K \cdot \sum_{j=0}^{n-1} f_j \cdot 2^j - K \cdot t \cdot M_{n,m} = 0$.

Наступним кроком будуємо $(2n+1)$-вимірну решітку $L(B)$, базис якої заданий стовпцями матриці B:

$$B = \begin{pmatrix} K \cdot H & K \cdot (2H \pmod{M_{n,m}}) & \cdots & K \cdot (2^{n-1} H \pmod{M_{n,m}}) & K \cdot 1 & K \cdot 2 & \cdots & K \cdot 2^{n-1} & K \cdot M_{n,m} \\ 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

Таким чином, якщо вдасться знайти вектор решітки $L(B)$, для якого перша координата дорівнює 0, тоді буде виконуватись рівняння $K \cdot g_0 \cdot H + K \cdot g_1 \cdot (2H(\bmod M_{n,m})) + \cdots + K \cdot g_{n-1} \cdot (2^{n-1} H(\bmod M_{n,m})) - K \cdot f_0 \cdot 1 - K \cdot f_1 \cdot 2 - \cdots - K \cdot f_{n-1} \cdot 2^{n-1} - K \cdot t \cdot M_{n,m} = 0$, отже, і рівняння $K \cdot \sum_{i=1}^{n-1} g_i \cdot 2^i \cdot H - K \cdot \sum_{j=1}^{n-1} f_j \cdot 2^j - K \cdot t \cdot M_{n,m} = 0$, що відповідає умові задачі GMLHRSP. Помітимо, що такий вектор решітки буде мати вигляд $(0, g_0, g_1, \ldots, g_{n-1}, -f_0, -f_1, \ldots, -f_{n-1}, t)^T$, тому за значеннями g_i, f_j можна буде відновити числа F та G. Оскільки за умовою задачі числа F та G мають малу вагу Геммінга h, то серед чисел g_i, $i = \overline{0, n-1}$ буде рівно h одиниць, а інші значення 0, та серед чисел f_j, $j = \overline{0, n-1}$ буде рівно h одиниць, а інші значення 0. Отже, отриманий вектор буде мати норму $\sqrt{\|G\|^2 + \|F\|^2} = \sqrt{h + h} = \sqrt{2h}$ і є коротким вектором решітки, тому можна спробувати його знайти за допомогою алгоритму LLL. Варто зазначити, що при побудові базисної матриці спеціально застосовано великий множник K, що дозволяє кратно збільшити норму векторів, що мають ненульову першу координату, для того, щоб такі вектори не виникали як результат після застосування алгоритму LLL. Отже, якщо після застосування алгоритму LLL до базисної матриці B перший LLL-

редукований базисний вектор буде мати координату 0, то отримані значення *F* та *G* є кандидатами на розв'язок задачі GMLHRSP.

Однак, через будову базисної матриці, у решітці існують «паразитні» вектори, які є значно коротшими за шуканий. Прикладом такого вектора є $(0,0^{i-1},2,-1,0^{2n-i-1})^T$, що матиме норму $\sqrt{5}$. Для узагальнених чисел Мерсенна можна побудувати інші «паразитні» вектори з нормою $\sqrt{6}$.

Таким чином,у решітці $L(B)$ існує кілька типів векторів, що є коротшими за шуканий з нормою $\sqrt{2h}$, тому, під час пошуку короткого вектору решітки за допомогою алгоритму LLL, результатом будуть саме ці вектори. Тому така атака не призводить до успішного відновлення секретних параметрів *F* та *G*, що доводить стійкість модифікованої криптосистеми AJPS-1 з використанням узагальнених чисел Мерсенна до такого типу атаки на решітках.

Висновки. У роботі проведено аналіз стійкості задачі GMLHRSP, що лежить в основі модифікації AJPS-1 з узагальненими числами Мерсенна, до атаки на основі алгоритму LLL. Розроблено алгоритм атаки, шляхом побудови решітки $L(B)$, на основі співвідношення задачі GMLHRSP та застосування до *B* алгоритму LLL. У результаті з короткого вектору решітки, який буде отримано в результаті LLL можна відновити секретні параметри *F* та *G*. Проте, у результаті дослідження виявлено, що у решітці $L(B)$ існують «паразитні» вектори, що мають норму значно меншу за очікувану. Таким чином, в результаті застосування алгоритму LLL будуть отримані саме ці вектори, які не можуть бути використані для відновлення шуканих секретних параметрів. Отримані результати доводять стійкість модифікованої криптосистеми AJPS-1 з використанням узагальнених чисел Мерсенна до такого типу атак на решітках.

Список використаних джерел

1. NIST's Post-Quantum Cryptography (PQC) Project.URL:https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

2. A New Public-Key Cryptosystem via Mersenne Numbers / D. Aggarwal, A. Joux, A. Prakash, M. Santha. Cryptology ePrint Archive, 2017. URL:https://eprint.iacr.org/archive/2017/481/20170530:072202.

3. Yadukha D. The Modification of the Quantum-Resistant AJPS-1 Cryptographic Primitive. Theoretical and Applied Cybersecurity. 2022. T. 4, вип. 1. URL: http://tacs.ipt.kpi.ua/article/view/274116.