УДК 003.26.09

Ковальчук А. В., здобувач
Ядуха Д. В., асистент
НТУУ «Київський політехнічний інститут ім. Ігоря Сікорського»

ПОБУДОВА МОДИФІКАЦІЇ ПОСТКВАНТОВОГО МЕХАНІЗМУ ІНКАПСУЛЯЦІЇ КЛЮЧА НА ОСНОВІ AJPS

Станом на сьогодні одними з найпоширеніших асиметричних криптопримітивів є RSA та ЕльГамаля, стійкість яких ґрунтується на складності розв'язання задач факторизації та дискретного логарифмування. Однак П. Шор ще в 1997 р. представив алгоритм, користуючись яким ці задачі можуть бути ефективно розв'язані у квантовій моделі обчислень. Як наслідок, використання асиметричних криптосистем, що побудовані на задачах факторизації та дискретного логарифмування, вважається безпечним лише з огляду на те, що науковцям досі не вдалося побудувати масштабований квантовий комп'ютер. У 2017 році NIST оголосив конкурс постквантових асиметричних криптопримітивів, які є стійкими до атак з використанням як класичних, так і квантових комп'ютерів. Одним із учасників конкурсу є механізм інкапсуляції ключа Mersenne-756839 з сімейства криптосистем AJPS, особливість яких полягає у використанні арифметики за модулем числа Мерсенна $M_n = 2^n - 1$, $n \in N$ [1]. Одним з представників сімейства AJPS є побітова схема шифрування AJPS-1. В [2] побудовано модифікацію схеми шифрування AJPS-1, а саме механізм інкапсуляції ключа AJPS-KEM$_1$, який також ґрунтується на використанні чисел Мерсенна M_n як модуля, та працює за допомогою побудованої функції Solve для цього класу чисел. Пізніше було побудовано модифікацію для схеми шифрування AJPS-1, в якій було замінено клас чисел Мерсенна для арифметики за модулем на клас узагальнених чисел Мерсенна $GM_{n,m} = 2^n - 2^m - 1$, де $n, m \in N$, $n > m$ [3]. В цій роботі зосередимось на побудові модифікації AJPS-KEM$_1$ для класу узагальнених чисел Мерсенна $GM_{n,m}$.

Нехай AJPSGM-KEM$_1$ = (KeyGen, Encap, Decap) – модифікований механізм інкапсуляції ключа з використанням арифметики за модулем узагальнених чисел Мерсенна з трьома процедурами: генерація ключів, інкапсуляція та декапсуляція ключа.

KeyGen. З урахуванням параметра захищеності λ обирається число $GM_{n,m}$ та число h, що задовольняє умовам: $4h^2 < n \leq 16h^2$ та

$C_n^h \geq 2^\lambda$. З множини лишків за модулем узагальненого числа Мерсенна, що мають вагу Геммінга h, обираються два n-бітові числа F, G рівноймовірно та незалежно. Відкритим ключем є значення $pk: = H = F \cdot G^{-1} \pmod{GM_{n,m}}$, особистим ключем є $sk := G$, а значення F є секретним параметром.

Encap. Рівноймовірно та незалежно обираються A, B – два лишки за модулем $GM_{n,m}$, причому $Ham(A) = Ham(B) = h$. Обчислюється значення $C = A \cdot H + B \pmod{GM_{n,m}}$. В результаті алгоритму інкапсуляції повертається шифротекст C, в який вбудовані значення A, B як інкапсульований ключ.

Decap. Використовуючи функцію Solve, отримувач розв'язує рівняння $G \cdot C \pmod{GM_{n,m}} = Fx + Gy \pmod{GM_{n,m}}$, використовуючи функцію Solve. Якщо розв'язок знайдено, то повертається пара (A, B), де $A = x$, $B = y$, яка і є інкапсульованим ключем.

В оригінальній схемі AJPS-KEM$_1$, що використовує клас чисел Мерсенна, функція Solve працює ітеративно, відновлюючи значення r-го біта невідомого числа A, та базується на тому, що множення чисел на степені двійки за модулем M_n є циклічним зсувом і, відповідно, вага Геммінга такого добутку дорівнює вазі Геммінга числа до множення [1, 2]. Алгоритм Solve знаходить r-й біт A таким чином:

$$\begin{cases} 1, \text{ якщо } \Delta = h, \\ 0, \text{ якщо } \Delta \approx 0 \ (\Delta \neq h), \text{ де } \Delta = Ham(W) - Ham(W - 2^r \cdot F(\bmod M_n)), \end{cases} Ham(F) = h,$$

$$W = C \cdot G = A \cdot F + B \cdot G \ (\bmod M_n).$$

Однак множення чисел на степені двійки за модулем узагальнених чисел Мерсенна не є циклічним зсувом, а тому реалізація такої перевірки як для модуля M_n, не спрацює для модуля $GM_{n,m}$. Далі наведена можлива реалізація Solve для модуля $GM_{n,m}$, ідея якої полягає у перевірці та встановленні r-го біта невідомого числа A шляхом порівняння значення $\Delta_r = Ham(W) - Ham(W - 2^r \cdot F \ (\bmod GM_{n,m}))$ з верхньою межею ваги Геммінга добутка числа та степенів двійки за модулем $GM_{n,m}$, яка визначається за співвідношенням [4]:

$$Ham(2^r \cdot F(\bmod GM_{n,m})) \leq Ham(F) + \mathrm{I}\{r \geq n - m\} \cdot (r - n + m).$$

В функції Solve для модуля $GM_{n,m}$ на кожній ітерації обчислюється Δ_r $\Delta_r \approx Ham(2^r \cdot F(\bmod GM_{n,m}))$. та очікується, що Тоді згідно наведеної верхньої оцінки ваги Геммінга добутка за модулем класу $GM_{n,m}$, r-й біт визначається як:

$$\begin{cases} 1, \text{ якщо } r \geq n-m \text{ і } 0 < \Delta_r \leq h+r-n+m, \\ 1, \text{ якщо } r < n-m \text{ і } 0 < \Delta_r \leq h, \\ 0, \text{ інакше.} \end{cases}$$

Висновки. У цій роботі розглянуто механізм інкапсуляції ключа AJPS-KEM$_1$, який базується на арифметиці за модулем числа Мерсенна та працює з використанням функції Solve для цього класу чисел. У роботі побудовано модифікацію AJPSGM-KEM$_1$ з використанням узагальнених чисел Мерсенна як модуля. Для побудови такої модифікації, враховуючи особливості реалізації функції Solve для класу чисел Мерсенна, розроблено алгоритм Solve для чисел за модулем узагальненого числа Мерсенна. Отримані результати демонструють можливість перенесення AJPS-KEM$_1$ на клас узагальнених чисел Мерсенна для арифметики за модулем, що дозволяє збільшити варіативність параметрів криптопримітиву.

Список використаних джерел

1. 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/2017/481.

2. Ferradi H., Naccache D. Integer Reconstruction Public-Key Encryption. *Cryptology ePrint Archive*. 2017. URL: https://eprint.iacr.org/2017/1231.

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.

4. Ядуха Д. В., Фесенко А. В. Оцінка ваги Хеммінга суми та добутку чисел за модулем узагальненого числа Мерсенна. *Теоретичні і прикладні проблеми фізики, математики та інформатики*, 2020. С. 350–352. URL: https://drive.google.com/file/d/1BcmU79pwMDtgA7ZXqTd5Gtw6CO6Av1ou/view.