**УДК 003.26.09**

**doi.org/10.15407/fmmit2023.37.154**

# Визначення необхідних умов на значення ключів постквантової криптосистеми AJPS-1

Дарія Ядуха[1]

[1] аспірантка НН ФТІ НТУУ «КПІ ім. Ігоря Сікорського», асистент кафедри математичних методів захисту інформації НН ФТІ НТУУ «КПІ ім. Ігоря Сікорського», пр. Берестейський, 37, 03056, м. Київ,
e-mail: dariya.yadukha@gmail.com

*У роботі проведено аналіз постквантової криптосистеми AJPS-1, яка є учасником першого раунду конкурсу постквантових криптопримітивів NIST. Знайдено слабкі значення відкритого ключа криптосистеми та наведено необхідні умови на значення відкритого ключа для забезпечення захищеності криптосистеми. Узагальнюючи інші відомі атаки на AJPS-1, сформовано рекомендації щодо вибору особистого та відкритого ключів. Застосовано підхід подвійного шифрування до криптосистеми AJPS-1 та доведено, що в такому випадку не буде виникати обмежень на вибір відкритого ключа.*

**Ключові слова:** криптосистема AJPS, постквантова криптосистема, число Мерсенна, вага Геммінга

**Вступ.** Останні кілька років активно розвивається постквантова криптографія, задачею якої є розробка криптографічних примітивів, які є стійкими до атак як з використанням класичного, так і квантового комп'ютерів. З 2017 року триває конкурс постквантових криптопримітивів під егідою Національного інституту стандартів і технологій США (NIST), після закінчення якого будуть опубліковані перші версії стандартів постквантової криптографії [1]. Одним з учасників першого раунду конкурсу є механізм інкапсуляції Mersenne-756839, який оснований на криптосистемі AJPS [2]. Особливістю криптосистеми AJPS є використання арифметики за модулем числа Мерсенна, яка може бути ефективно реалізована шляхом застосування алгоритмів швидкого обчислення трудомістких операцій за модулем числа Мерсенна, таких як редукція, множення, пошук оберненого тощо [3]. Криптосистема AJPS має дві версії – для шифрування біту повідомлення (AJPS-1) та для шифрування блоку бітів повідомлення (AJPS-2).

## 1. Опис криптосистеми AJPS-1

Криптосистема AJPS-1 [2] дозволяє зашифрувати один біт повідомлення $b \in \{0,1\}$. При побудові криптосистеми задається параметр захищеності $\lambda$. Відкритими параметрами криптосистеми є числа $M_n = 2^n - 1$, $n \in \aleph$ та $h \in \aleph$, де $h$ – фіксоване число, яке задовольняє умовам $C_n^h \geq 2^\lambda$ та $4h^2 < n \leq 16h^2$. Тут і надалі для спрощення запису ототожнюємо числа за модулем числа Мерсенна

та двійкові рядки довжини *n*. Це можливо, оскільки між множинами цих об'єктів існує взаємно однозначне відображення. Позначимо множину чисел, які за модулем числа Мерсенна $M_n$ мають вагу Геммінга *h*, як $HM_{n,h} = \{x : Ham(x \bmod M_n) = h\}$, де *Ham*(*x*) позначає вагу Геммінга числа *x*.

1) Створення ключів: числа *F* та *G* обираються випадково та незалежно з множини $HM_{n,h}$. Особистим ключем є число *G*, а відкритим ключем – число $H = F \cdot G^{-1} \bmod M_n$.

2) Шифротекст *C* обчислюється за формулою $C = (-1)^b (A \cdot H + B) \bmod M_n$, де *A* та *B* – незалежно і рівноймовірно обрані значення з множини $HM_{n,h}$.

3) Для розшифрування обчислюється значення $d = Ham(C \cdot G \bmod M_n)$, після чого біт *b* визначається таким чином:

$$b = \begin{cases} 0, & якщо \quad d \le 2h^2 \\ 1, & якщо \quad d \ge n - 2h^2 \\ \perp, & інакше \quad (помилка\ розшифрування) \end{cases}.$$

Коректність розшифрування ґрунтується на Лемі 1.

**Лема 1.** [2] *Для довільних чисел* $A, B \in \{0,1\}^n$ *та числа Мерсенна* $M_n$ *виконуються співвідношення:*

1. $Ham(A + B \bmod M_n) \le Ham(A) + Ham(B)$;
2. $Ham(A \cdot B \bmod M_n) \le Ham(A) \cdot Ham(B)$;
3. Якщо $A \ne 0^n$, то $Ham(-A \bmod M_n) = n - Ham(A)$.

Стійкість криптосистеми AJPS-1 базується на складності задачі MLHRSP [2] – Задачі ділення чисел з малою вагою Геммінга за модулем числа Мерсенна (англ. *Mersenne Low Hamming Ratio Search Problem*).

**Означення 1** (MLHRSP)**.** *Маючи число Мерсенна* $M_n$, *n-бітове число H і ціле число h, знайти два n-бітових числа F, G, кожне ваги Геммінга щонайбільше h, таких, що* $H = F \cdot G^{-1} \bmod M_n$.

## 2. Умови на значення ключів криптосистеми AJPS-1

Одним з напрямків обґрунтування захищеності будь-якої криптосистеми є аналіз побудованих на криптосистему атак та оцінка їх успішності. Частину побудованих на AJPS-1 атак можливо застосувати лише за умови, що виконується певне припущення про вигляд чисел *F* та *G*.

1) Атака «*Слабкий ключ*» [4] є успішною, якщо усі одиниці у двійковому представленні чисел *F* та *G* знаходяться у правій частині двійкового представлення, тобто якщо кожне з чисел *F*, *G* менше за $\sqrt{M_n}$. Атака дозволяє визначити значення особистого ключа за допомогою методу раціональної реконструкції, тобто методу пошуку раціонального числа, використовуючи

результат редукції цього числа за деяким модулем. Складність атаки $2^{2h} \cdot n^{o(1)}$.

2) Атака «*Slice-and-Dice*» з використанням алгоритму LLL [5] побудована аналогічно до атаки «Слабкий ключ». В цій атаці на числа *F* та *G* накладається умова, щоб усі їхні ненульові значення бітів знаходились згруповано у одній частині бінарного запису числа. Атака використовує ідею розділення бінарного представлення числа на проміжки, які будуть використовуватись для побудови решітки. Якщо інтервали підібрані правильно, то найкоротшими векторами побудованої решітки будуть значення *F* та *G*. Складність такої атаки $(2+\delta+o(1))^{2h}$ для деякої малої константи $\delta > 0$. Також при реалізації цієї атаки можна використовувати SVP-оракули для пошуку *F* та *G*. Такий спосіб дозволяє збільшити ймовірність успіху атаки до $\left(\frac{1}{2}+o(1)\right)^{2h}$, однак також збільшує час виконання операції редукції решітки до $2^{(2+\delta)h+o(h)}$.

Слід зауважити, що, навіть якщо потрібні для атак умови виконуються, складність описаних атак є все одно досить великою, що унеможливлює їх використання на практиці. Однак, для підвищення стійкості криптосистеми AJPS-1, можна виконувати низку необхідних перевірок при застосуванні алгоритму створення ключів, і виконувати кроки алгоритму створення ключів повторно у випадку порушення однієї з вимог.

Також при визначенні умов на алгоритм створення ключів варто врахувати необхідні умови на значення відкритого ключа криптосистеми AJPS-1.

**Твердження 1.** У криптосистемі AJPS-1 при виконанні однієї з умов:

$$Ham(H) \le 1 \quad або \quad Ham(H^{-1} \bmod M_n) \le 1$$

можливе дешифрування шифротексту без використання особистого ключа.

***Доведення.*** Розглянемо випадки, коли можливе розшифрування без знання особистого ключа. Для розшифрування знаходять значення *d*:

$$d = Ham(C \cdot G \bmod M_n) = Ham((-1)^b (A \cdot H + B) \cdot G \bmod M_n).$$

Відповідно до значення біту *b*, можливі випадки:

1) Якщо *b* = 0, то, застосувавши Лему 1, маємо:

$$d = Ham((A \cdot H + B) \cdot G \bmod M_n) \le (Ham(A) \cdot Ham(H) + Ham(B)) \cdot Ham(G).$$

Оскільки за умовою криптосистеми числа *A, B* та *G* мають вагу Геммінга *h*, то отримаємо $d \le h^2 (Ham(H)+1)$. Для того, щоб при розшифруванні отримати біт 0, потрібно, щоб виконувалась нерівність $d \le 2h^2$. Отже, дешифрування біту 0 без використання особистого ключа можливе при $Ham(H) \le 1$.

2) Якщо ж *b* = 1, то, відповідно до Леми 1, маємо:

$$d = n - Ham((AH + B)G \bmod M_n) \ge n - ((Ham(A)Ham(H) + Ham(B))Ham(G).$$

Оскільки *Ham*(*A*) = *Ham*(*B*) = *Ham*(*G*) = *h*, то $d \ge n - h^2 (Ham(H)+1)$. Для того, щоб результатом розшифрування був біт 1, має виконуватись умова $d \ge n - 2h^2$, тобто отримаємо таку нерівність: $n - h^2 (Ham(H)+1) \ge n - 2h^2$.

Отже, розшифрування біту 1 без використання особистого ключа можливе при виконанні умови $Ham(H) \le 1$, як і у випадку розшифрування біту 0.

Умова $Ham(H^{-1} \bmod M_n) \le 1$ отримується аналогічно, врахувавши, що $G = H^{-1} \cdot F \bmod M_n$.

Узагальнюючи умови на значення *F* та *G* наведених атак, а також враховуючи обмеження на значення *H* криптосистеми AJPS-1, що описані у Твердженні 1, сформуємо рекомендації для алгоритмів створення ключів криптосистеми AJPS-1.

**Твердження 2** (*Рекомендації для алгоритму створення ключів криптосистеми AJPS-1*)**.** Нехай в результаті застосування алгоритму створення ключів AJPS-1 отримано *G* – особистий ключ, *F* – секретний параметр криптосистеми, $H = F \cdot G^{-1} \bmod M_n$ – відкритий ключ. Для забезпечення захищеності від описаних атак (а саме атак Слабкий ключ, *Slice-and-Dice* та атаки, що наведена у Твердженні 1) необхідно, щоб значення *F*, *G* та *H* задовольняли таким умовам:

1) Хоча б одне з чисел *F* та *G* має бути більшим або рівним $\sqrt{M_n}$, тобто має виконуватись така умова:

$$\left[\begin{array}{l} F \ge \sqrt{M_n}, \\ G \ge \sqrt{M_n}. \end{array}\right.$$

2) В бінарному записі хоча б одного з чисел *F* та *G* одиниці не згруповані разом (є хоча б один нуль між *h* одиницями), тобто виконується умова:

$$\left[\begin{array}{ll} F \ne 2^i \cdot M_h, & i = \overline{0, n-h}, \\ G \ne 2^j \cdot M_h & j = \overline{0, n-h}. \end{array}\right.$$

3) Число *H* задовольняє таким умовам:

$$Ham(H) \ne 1 \;\; та \;\; Ham(H^{-1} \bmod M_n) \ne 1.$$

Якщо хоча б одна з наведених умов не виконується, то необхідно повторно застосувати алгоритм створення ключів. Якщо усі умови виконуються, то *G* та *H* можна використовувати для подальшої роботи криптосистеми.

***Доведення.*** Пункт 1 отримано з умови атаки «Слабкий ключ». Розглянемо обґрунтування пункту 2. Умовою застосування атаки «Slice-and-Dice» є вимога, щоб усі одиниці у двійковому представленні чисел *F* та *G* знаходились згруповано. Оскільки числа *F* та *G* мають вагу Геммінга *h*, то *h* одиниць мають знаходитись поруч (без нулів між ними) у двійковому записі цих чисел. Розглянемо число Мерсенна $M_h = 2^h - 1$. У двійковому записі воно має вигляд 11…1, причому одиниць рівно *h*. Таким чином, число $M_h$ є одним з «слабких» значень для чисел *F*, *G*. При множенні на двійку отримаємо $2 \cdot M_h \bmod M_n = 11...10$, тобто ще одне «слабке» значення для чисел *F* та *G*. Оскільки числа *F*, *G* за умовою криптосистеми є *n*-бітовими, то максимальний степінь двійки, на який можна домножити $M_h$ для отримання «слабкого» значення, є (*n* – *h*), адже множення на степінь двійки за модулем числа Мерсенна є циклічним зсувом числа вліво [3]. Пункт 3 ґрунтується на Твердженні 1.

Іншим способом запобігти атакам, що використовують слабкі значення відкритого ключа *H*, які описано у Твердженні 1, є застосування схеми подвійного шифрування, у якій шифротекст, отриманий у результаті першого шифрування, використовуються як відкритий ключ при другому шифруванні.

**Лема 3.** *Якщо у криптосистемі AJPS-1 шифротекст буде обчислений як* $C = (-1)^b (A_2 \cdot H_C + B_2)$, *де* $H_C = (-1)^{b^*} (A_1 \cdot H + B_1)$, *біт* $b^* \in \{0,1\}$ *обирається випадково, та* $A_1, A_2, B_1, B_2 \in HM_{n,h}$, *то атака, що описана у Твердженні 1, не буде успішною при будь-яких значеннях відкритого ключа H.*

***Доведення.*** Слідує з Леми 1 та умови алгоритму створення ключів AJPS-1, розглядаємо 4 варіанти комбінацій можливих значень бітів *b та b**.

**Висновки.** У роботі виконано аналіз постквантової криптосистеми AJPS-1, здійснено огляд деяких відомих атак на AJPS-1, а саме атаки «Слабкий ключ» та «Slice-and-Dice» з використанням алгоритму LLL. Також у роботі визначено обмеження на значення відкритого ключа криптосистеми AJPS-1. Узагальнюючи вимоги для можливого застосування наведених атак та знайдені обмеження на значення відкритого ключа, сформовано рекомендації для алгоритмів створення ключів AJPS-1, які дозволяють підвищити захищеність криптосистеми. Також доведено, що застосування підходу подвійного шифрування у AJPS-1 дозволяє уникнути виникнення слабких значень відкритого ключа.

### Література

[1] Post-Quantum Cryptography Standardization. *National Institute of Standards and Technology, Available:https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization.*

[2] *D. Aggarwal, A. Joux, A. Prakash, M. Santha*. A New Public-Key Cryptosystem via Mersenne Numbers. *IACR Cryptology ePrint Archive. – Available: https://eprint.iacr.org/2017/481*.

[3] *S. Baktir, B. Sunar*. Optimal Extension Field Inversion in the Frequency Domain. Arithmetic of Finite Fields. Siena: Springer, 2008.

[4] *M. Beunardeau, A. Connolly, R. Geraud, D. Naccache*. On the Hardness of the Mersenne Low Hamming Ratio Assumption. *Available: https://eprint.iacr.org/2017/522.*

[5] *M. Tiepelt, A. Szepieniec.* Quantum LLL with an Application to Mersenne Number Cryptosystems. *Progress in Cryptology – LATINCRYPT 2019.*

## The necessary conditions for the key generation of the quantum-resistant AJPS-1 cryptosystem

Dariya Yadukha

*The paper analyzes the post-quantum AJPS-1 cryptosystem, which participated in the first round of the NIST post-quantum crypto primitives competition. The weak values of the public key of the cryptosystem are found and the necessary conditions for the public key to ensure the security of the cryptosystem are given. By generalizing other known attacks on AJPS-1, recommendations for choice of secret and public keys are given. The double encryption approach has been applied to the AJPS-1 cryptosystem, and it has been proved that there are no restrictions on the public key in this case.*

Отримано 12.03. 23