УДК 003.26.09

# ПОБУДОВА АТАК НА КРИПТОСИСТЕМУ AJPS З ВИКОРИСТАННЯМ МОДЕЛІ АКТИВНОГО ЗЛОВМИСНИКА

*Ядуха Дарія, Фесенко Андрій*

Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського», Фізико-технічний інститут

## Анотація

*Д. Агарвал та інші нещодавно запропонували нову потенційно постквантову асиметричну криптосистему AJPS, яка використовує операції за модулем числа Мерсенна. У даній роботі побудовано атаки на криптосистему AJPS, а саме атаки підміни та імітації активним криптоаналітиком.*

## Abstract

*D. Aggarwal and other recently introduced a new potentially postquantum public-key cryptosystem based on operations by modulus of the Mersenne number. This paper describes the attacks on AJPS cryptosystem, namely the attacks of substitution and simulation by an active cryptanalyst.*

## Вступ

Асиметричні криптосистеми або криптосистеми з відкритим ключем - це ефективні системи криптографічного захисту даних, у яких для зашифрування даних використовують один ключ - відкритий (публічний), а для розшифрування - інший (особистий). Оскільки стійкість більшості асиметричних криптосистем ґрунтується на складності задач, розв'язування яких може значно швидше виконати квантовий комп'ютер, то є мотивація створювати криптосистеми з відкритим ключем, які будуть стійкими до атак з використанням квантового комп'ютера. Національний інститут стандартів і технологій (NIST) оголосив конкурс постквантових криптографічних алгоритмів з відкритим ключем [4], заявки на участь у якому приймали до 30 листопада 2017 року. Одним із запропонованих примітивів і є криптосистема AJPS [1]. Основною задачею даної роботи є аналіз запропонованої криптосистеми та побудова атак на неї за моделі активного зловмисника.

## Опис криптосистеми AJPS

Розглянемо криптосистему AJPS [1]: нехай є відкриті параметри $M_n=2^n-1$ - число Мерсенна, $\alpha$ - параметр захищеності, заданий під час побудови криптосистеми, і $h$ - фіксоване значення, яке задовільняє умовам $4h^2 < n$ та $C_{n-1}^{h-1} \geq 2^{\alpha}$. Позначимо функцію знаходження ваги Хеммінга як $Ham$. Нехай $HM_{n,h} = \{x : Ham(x \bmod M_n) = h\}$, тобто $HM_{n,h}$ - множина чисел, які за модулем числа Мерсенна мають вагу Хеммінга $h$. Числа $F$ та $G$ обираються незалежно та рівноймовірно з множини $HM_{n,h}$. Значення $G$ є особистим ключем отримувача, $F$ - таємний параметр криптосистеми. Відкритий ключ $H$ обчислюється наступним чином: $H = \frac{F}{G} \bmod M_n$. Криптосистема дозволяє зашифрувати один біт, тобто відкритим текстом є число $b \in \{0,1\}$. Шифротекст $C$ обчислюється за формулою $C=(-1)^b(A \cdot H+B) \bmod M_n$, де $A, B$ - незалежно і рівноймовірно обрані значення з множини $HM_{n,h}$. Для розшифрування спочатку обчислюється значення $d=Ham(C \cdot G \bmod M_n)$, потім біт $b$ знаходиться наступним чином:

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

Правильність розшифрування випливає з леми [1]:

**Лема 1.** Нехай $M_n=2^n-1$ та $A,B \in \{0,1\}^n$, тоді виконуються наступні співвідношення:

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

Стійкість криптосистеми AJPS ґрунтується на складності задачі ділення чисел з малою вагою Хеммінга за модулем числа Мерсенна (задача MLHRSP) [1]. Також були спроби застосувати відомі види атак, наприклад, «зустріч посередині», «вгадай і виграй» [1] та інші побудовані атаки, наприклад, «розділи та спробуй» [2] – проведені атаки показали те, що криптосистема є стійкою за умови збільшення параметру захищеності [2].

## Побудова атак на криптосистему активним криптоаналітиком

Активний криптоаналітик може не лише переглядати усі шифротексти, які передаються відкритим каналом зв'язку, а також, при успішній атаці, може змінювати або підмінювати шифротекст так, що отримувач не помітить підміни. Далі розглянемо наступні атаки на криптосистему AJPS.

**Твердження 1.** *Атака підміни з незмінним відкритим текстом є успішною для криптосистеми AJPS: маючи у розпорядженні один шифротекст C, зловмисник може обчислити шифротексти, що будуть відповідати тому ж відкритому тексту наступним чином:* $C^*=C \cdot 2^z$ *для довільного значення* $z \in \mathrm{N}$.

**Доведення.** Дана атака полягає у тому, що криптоаналітик деяким чином перетворює перехвачений текст так, що при розшифруванні отримувач має той ж біт, який і мав отримати, навіть якби криптоаналітик не втрутився. Таким чином, криптоаналітик не знає відкритий текст і не отримує про нього ніякої інформації під час атаки. Така атака матиме наступний вигляд: нехай $C$ - справжній шифротекст і значення, яке мав би знаходити отримувач при розшифруванні: $d=Ham(C \cdot G\ mod\ M_n)$. Позначимо $C^*$ модифікований шифротекст, тоді значення, яке після успішної атаки буде знаходити отримувач для розшифрування: $d^*=Ham(C^* \cdot G\ mod\ M_n)$. Нехай криптоаналітик перехватив шифротекст $C$. Тоді він обчислює $C^*=C \cdot 2^z$, $z \in \mathrm{N}$ і відправляє його одержувачу. Одержувач обчислює наступне:

$$d^* = Ham(C^* \cdot G \bmod M_n) = Ham(C \cdot 2^z \cdot G \bmod M_n) = Ham((C \cdot G) \cdot 2^z \bmod M_n).$$

Далі використовуємо відому властивість для чисел Мерсенна - множення на степінь двійки за модулем числа Мерсенна є циклічним зсувом числа [3]. Тоді у даному випадку отримуємо значення зсуву $C \cdot G$ на $z$ позицій. А оскільки циклічний зсув ніяк не впливає на вагу Хеммінга числа, то маємо: $Ham((C \cdot G) \cdot 2^z\ mod\ M_n)=Ham(C \cdot G\ mod\ M_n)=d$. Таким чином, отримувач правильно розшифрує модифікований шифротекст.

Розглянута атака не надає можливості криптоаналітику отримати інформацію про відкритий текст або ключ та не спотворює повідомлення відправника, але якщо властивості шифротексту мають цінність, то описане твердження може бути використане із зловмисною метою.

**Твердження 2.** *Атака імітації з обраним криптоаналітиком фіксованим відкритим текстом успішна для криптосистеми AJPS: незалежно від особистого ключа, якщо криптоаналітик відправить повідомлення $C_1$ таке, що $Ham(C_1 \bmod M_n) \le 2h$, то отримувач розшифрує його як біт 0, та якщо відправить $C_2 = -C_1 \bmod M_n$, то отримувач при розшифруванні отримає біт 1.*

**Доведення.** Дана атака заключається у тому, що криптоаналітик може відправляти деякі шифротексти отримувачу, причому знаючи, що саме отримає при розшифруванні отримувач. Тобто криптоаналітик сам обирає шифротекст так, щоб отримувач при розшифруванні отримав вигідний для криптоаналітика відкритий текст. Розглянемо два випадки: коли криптоаналітику потрібно, щоб отримувач при розшифруванні отримав біт $b$=0 та коли $b$=1.

1. Випадок $b$=0: криптоаналітик обирає довільний такий шифротекст $C_1$, для якого виконується умова $Ham(C_1 \bmod M_n) \le 2h$ та відправляє його. Тоді при розшифруванні отримувач має $d = Ham(C_1 \cdot G \bmod M_n)$ і, використовуючи лему 1, маємо:

$$d = Ham(C_1 \cdot G \bmod M_n) \le Ham(C_1 \bmod M_n) \cdot Ham(G) = Ham(C_1 \bmod M_n) \cdot h \le 2h^2$$

.

Оскільки $d \le 2h^2$, то $b$=0.

2. Випадок $b$=1: криптоаналітик обирає шифротекст $C_2 = -C_1 \bmod M_n$, де $C_1$ - шифротекст з пункту 1, задовольняючий наведеним вище умовам, та відправляє його отримувачу. Тоді при розшифруванні маємо:

$$d = Ham(C_2 \cdot G \bmod M_n) = Ham(-C_1 \cdot G \bmod M_n) = n - Ham(C_1 \cdot G \bmod M_n) \ge n - 2h^2$$

.

Оскільки $d \ge n - 2h^2$, то $b$=1.

Отже, криптоаналітик, не знаючи особистий ключ, може відправляти шифротексти з обраним значенням біту.

## Висновки

У даній роботі розглянуто побудовану нещодавно асиметричну криптосистему AJPS, одного з учасників конкурсу NIST для постквантових криптопримітивів. На відміну від більшості постквантових криптографічних алгоритмів, система AJPS використовує обчислення в кільці лишків. У роботі побудовано ефективні атаки підміни та імітації, які можуть бути використані при активній моделі зловмисника.

## Список використаних джерел:

1. Divesh Aggarwal, Antoine Joux, Anupam Prakash, Miklos Santha. A New Public-Key Cryptosystem via Mersenne Numbers [Електронний ресурс]. — Режим доступу: https://eprint.iacr.org/2017/481.

2. Marc Beunardeau, Aisling Connolly, R´emi G´eraud, David Naccache. On the Hardness of the Mersenne Low Hamming Ratio Assumption. [Електронний ресурс]. — Режим доступу: https://eprint.iacr.org/2017/522.

3. Joppe W. Bos, Thorsten Kleinjung, Arjen K. Lenstra. Efficient SIMD arithmetic modulo a Mersenne number. [Електронний ресурс]. — Режим доступу: https://eprint.iacr.org/2010/338.

4. Post-Quantum cryptography standardization NIST [Електронний ресурс]. — Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization