УДК 003.26.09

ПОБУДОВА АТАКИ ПІДМІНИ НА КРИПТОСИСТЕМУ AJPS-2 З ВИКОРИСТАННЯМ МОДЕЛІ АКТИВНОГО ЗЛОВМИСНИКА

Ядуха Дарія, Фесенко Андрій

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

Анотація

У роботі досліджується криптосистема AJPS-2, яка є учасником конкурсу постквантових криптографічних примітивів NIST. Доводиться властивість арифметики за модулем числа Мерсенна. Також описується побудована атака підміни на AJPS-2 з використанням моделі активного зловмисника, яка базується на доведеній властивості арифметики за модулем числа Мерсенна.

Abstract

In this paper we analyze the AJPS-2 cryptosystem, which participates in the NIST quantum-resistant cryptographic primitives competition. We prove the arithmetic property modulo Mersenne number. Also we describe constructed substitution attack by active attacker on AJPS-2, which is based on the proven arithmetic property modulo Mersenne number.

Вступ

У листопаді 2017 року Національний інститут стандартів та технологій США (NIST) розпочав конкурс постквантових асиметричних криптопримітивів, які б реалізовували схему шифрування, механізм інкапсуляції ключів або схему цифрового підпису [1]. Одним з учасників першого раунду конкурсу є механізм інкапсуляції ключів Mersenne-756839 [2], який оснований на криптосистемі AJPS [3]. Криптосистема AJPS має дві версії – для шифрування біту повідомлення (AJPS-1) та для шифрування блоку повідомлення (AJPS-2).

Опис криптосистеми AJPS-2

Криптосистема AJPS-2 [3] дозволяє зашифрувати блок повідомлення довжиною λ, де λ – параметр захищеності, який задається при побудові криптосистеми, тобто відкритим текстом є $m \in \{0,1\}^{\lambda}$. Відкритими параметрами системи є числа M_n та h, де h – фіксоване число, яке задовольняє умовам $h = \lambda$ та $10h^2 < n \le 16h^2$, а також функції $E : \{0,1\}^{\lambda} \to \{0,1\}^n$ та $D : \{0,1\}^n \to \{0,1\}^{\lambda}$ – функції шифрування та розшифрування завадостійкого коду, які обираються відповідно до умови: для забезпечення рівня правдоподібності $(1-\delta)$, де δ – ймовірність помилки, необхідне виконання такої умови:

$$\forall m : \Pr\{D((F \cdot C_1) \oplus C_2) = m\} \ge 1 - \delta.$$

Позначимо $HM_{n,h}$ множину n-бітових чисел, які мають вагу Хеммінга h. Слід зауважити, що тут і надалі для спрощення запису ототожнюємо числа за модулем числа Мерсенна M_n та бітові рядки довжини n. Це можливо, оскільки між множинами, які задають дані значення, існує взаємно однозначне відображення.

- Генерація ключів криптосистеми відбувається наступним чином.
  1. Числа F та G обираються випадково та незалежно з множини $HM_{n,h}$, а число R обирається випадково з усіх можливих n-бітових чисел.
  2. Особистим ключем є число F, а відкритим ключем – пара чисел (R,T), де R – випадкове n-бітове число та $T = F \cdot R + G \bmod M_n$.

- Для шифрування блоку повідомлення $m \in \{0,1\}^{\lambda}$ незалежно і рівноймовірно обираються числа A, B_1 та B_2 з множини $HM_{n,h}$. Блок m шифрується наступним чином:

$$(C_1, C_2) = (A \cdot R + B_1 \bmod M_n, (A \cdot T + B_2 \bmod M_n) \oplus E(m)).$$

- При розшифруванні шифротексту (C_1, C_2) обчислюється значення

$$D((F \cdot C_1 \bmod M_n) \oplus C_2).$$

Щоб переконатись у правильності розшифрування, позначимо $C_2^* = C_1 \cdot F$ та помітимо, що $C_2^* = (A \cdot T + B_2) - A \cdot G - B_2 + B_1 \cdot F$. Оскільки за умовами побудови криптосистеми $A, B_1, B_2, F, G \in HM_{n,h}$, то відстань Хеммінга з великою ймовірністю буде малою. Тоді при обчисленні $D\left(C_2 \oplus C_2^*\right)$, з великою ймовірністю отримаємо *m*.

Побудова атаки підміни на криптосистему AJPS-2 з використанням моделі активного зловмисника

За теорією Джеймса Сіммонса атакою підміни називається атака, при якій криптоаналітик перехоплює справжній шифротекст від відправника, формує помилковий шифротекст та передає його отримувачу [4]. Атака вважається успішною, якщо отримувач прийняв отримане повідомлення за допустиме.

Активний зловмисник при здійсненні атаки може не лише зчитувати усі шифротексти, які передаються відкритим каналом зв'язку, а також може змінювати шифротексти у каналі зв'язку непомітно для отримувача [5].

Для побудови атаки підміни з використанням моделі активного зловмисника на криптосистему AJPS-2 використовується властивість арифметики за модулем числа Мерсенна, що описується у наступній лемі.

Лема 1. *Для довільних чисел* $A, B \in \{0,1\}^n$, *числа Мерсенна* $M_n = 2^n - 1$ *та довільного натурального числа* r *такого, що* $r < n$, *виконується співвідношення:*

$$\overleftarrow{A + B \bmod M_n} = \overleftarrow{A} + \overleftarrow{B} \bmod M_n,$$

де $\overleftarrow{X}$ *– операція циклічного зсуву числа X на* r *позицій вліво.*

Доведення. Оскільки операція циклічного зсуву на r позицій за модулем числа Мерсенна є еквівалентом операції множення на 2^r [6], то маємо:

$$\overleftarrow{A + B \bmod M_n} = (A + B) \cdot 2^r \bmod M_n = (A \cdot 2^r \bmod M_n) + (B \cdot 2^r \bmod M_n) = \overleftarrow{A} + \overleftarrow{B} \bmod M_n,$$

що і потрібно було довести. *Лему доведено.*

Твердження 1. *Атака підміни з модифікованим відкритим текстом є успішною для криптосистеми* AJPS-2*: маючи пару* (C_1, C_2), *зловмисник може обчислити шифротексти* (C_1^*, C_2), *де* $C_1^* = \overleftarrow{C_1}$, *значення* $\overleftarrow{C_1}$ *– результат операції циклічного зсуву числа* C_1 *на* r *позицій вліво, при цьому значення* r *– довільне натуральне число менше за* n.

Доведення. Результатом алгоритму шифрування криптосистеми AJPS-2 є пара чисел (C_1, C_2), де $C_1 = A \cdot R + B_1 \bmod M_n$ та $C_2 = (A \cdot T + B_2 \bmod M_n) \oplus E(m)$. Виконуючи циклічний зсув числа C_1, відповідно до леми 1, маємо $\overleftarrow{C_1} = \overleftarrow{A \cdot R} + \overleftarrow{B_1}$. Оскільки число B_1 обиралось випадковим чином з множини $HM_{n,h}$ при процедурі шифрування і використовується одноразово при обчисленні значення C_1, то використання значення $\overleftarrow{B_1}$ замість B_1 при обрахунку C_1 не змінює значення повідомлення, яке буде отримане при розшифруванні, адже вага Хеммінга не змінюється

при циклічному зсуві числа, тобто $\overleftarrow{B_1} \in HM_{n,h}$. Однак використання значення $\overleftarrow{A \cdot R}$ замість $A \cdot R$ впливає на розшифроване повідомлення. R – відкритий ключ криптосистеми, тобто відоме зловмиснику значення, а число A обирається випадково з множини $HM_{n,h}$ при кожній процедурі шифрування. Якщо вважати, що при обчисленні операції циклічного зсуву до значення $A \cdot R$ число R залишається незмінним, то маємо $\overleftarrow{A \cdot R} = Y \cdot R,$ де Y – деяке *n*-бітове число, яке задовольняє заданій умові. Якщо число Y має вагу Хеммінга *h* (хоча ймовірність цієї події порівняно мала), то значення C_1^* буде відповідати коректному повідомленню. Проте навіть в такому випадку атака буде успішною, адже число A використовується не лише при обчисленні C_1, а і при обчисленні C_2. Таким чином, маємо:

$$(C_1^*, C_2) = (Y \cdot R + B_1, (A \cdot T + B_2) \oplus E(m)),$$

тобто при розшифруванні (C_1^*, C_2) буде отримано повідомлення m^*, $m \neq m^*$. *Твердження доведено.*

Отже, криптосистема AJPS-2 не є стійкою до атаки підміни з використанням моделі активного зловмисника.

Висновки

У даній роботі розглянуто криптосистему AJPS-2, яка є учасником конкурсу постквантових криптопримітивів NIST. Особливістю даної криптосистеми, у порівнянні з іншими учасниками конкурсу, є використання операцій у кільці лишків, а саме операцій за модулем числа Мерсенна. У роботі доведено властивість арифметики за модулем числа Мерсенна та, застосовуючи доведену властивість, побудовано атаку підміни на криптосистему AJPS-2 з використанням моделі активного зловмисника.

Список використаних джерел

1. Post-Quantum Cryptography Standardization [Електронний ресурс] // National Institute of Standards and Technology, Information Technology Laboratory. – 2017. – Режим доступу: https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization.

2. Round 1 Post-Quantum Cryptography [Електронний ресурс] // National Institute of Standards and Technology, Information Technology Laboratory. – 2017. – Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

3. A New Public-Key Cryptosystem via Mersenne Numbers [Електронний ресурс] / D.Aggarwal, A. Joux, A. Prakash, M. Santha // IACR Cryptology ePrint Archive, Report 2017/481. – 2017. – Режим доступу: https://eprint.iacr.org/2017/481.

4. Simmons G. Authentication Theory & Coding Theory / Gustavus J. Simmons // CRYPTO 1984: Advances in Cryptology / Gustavus J. Simmons. – Berlin: Springer, 1985. – (Lecture Notes in Computer Science; vol. 184). – С. 411-431. – ISBN 978-3-540-15658-1.

5. Wyner A. The wire-tap channel / A. D. Wyner. // The Bell System Technical Journal. – 1975. – №54. – С. 1355 – 1387. – ISBN 0005-8580.

6. Baktir S. Optimal Extension Field Inversion in the Frequency Domain / S. Baktir, B. Sunar // Arithmetic of Finite Fields / S. Baktir, B. Sunar. – Siena: Springer, 2008. – (Theoretical Computer Science and General Issues). – (Lecture Notes in Computer Science; т. 5130). – С. 47-61. – ISBN 978-3-540-69498-4.