УДК 003.26

ПОБУДОВА ОБМЕЖЕНЬ НА ЗНАЧЕННЯ ВІДКРИТОГО КЛЮЧА КРИПТОСИСТЕМИ AJPS

Д. В. Ядуха[1, a]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

Д. Агарвал та інші нещодавно запропонували нову постквантову асиметричну криптосистему AJPS [1], яка використовує операції за модулем числа Мерсенна. У даній роботі побудовано обмеження на значення відкритого ключа даної криптосистеми.

Ключові слова: число Мерсенна, вага Хеммінга, асиметрична криптосистема, криптосистема AJPS

Вступ

Асиметричні криптосистеми або криптосистеми з відкритим ключем – 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 такі криптосистеми, 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 алгоритмів і є криптосистема AJPS [1], яка використовує арифметику за модулем числа Мерсенна. Основною задачею даної роботи є аналіз запропонованої криптосистеми та побудова обмежень на значення відкритого ключа.

1. Числа Мерсенна та їх властивості

Числа спеціальної форми часто дозволяють швидше виконувати арифметичні операції за модулем. Це широко використовується для практичних цілей і пояснює велику кількість досліджень швидкої спеціальної арифметики.

Число Мерсенна M_n виду 2^n-1 є одним з найбільш відомих типів простих чисел, який досліджувався математиками ще з XVII століття. Числа Мерсенна мають багато переваг для застосування у криптографії або інших прикладних областях з використанням операцій у кільці лишків. Відомо, що такі числа дозволяють швидко реалізовувати обчислення редукції за даним модулем, оскільки трудомісткі операції (множення, ділення) за модулем числа Мерсенна можна замінити на звичайне додавання [5]. Наприклад, нехай x – деяке число, в такому випадку для знаходження $x \bmod M_n$ достатньо представити число x у вигляді $x = T \cdot 2^n + U$, тоді

$$x \equiv T + U (\bmod M_n).$$

Це випливає з властивостей чисел Мерсенна, а саме з факту, що множення на степінь двійки за модулем числа Мерсенна є циклічним зсувом (для будь-якого числа x і числа $y = 2^z$, де z – додатнє ціле, $x \cdot y \bmod M_n$ – це циклічний зсув числа x на z позицій [1]). Таким чином, вага Хеммінга числа x (кількість одиниць у двійковому записі числа) не змінюється при множенні на число, яке є степенем двійки. Позначимо функцію знаходження ваги Хеммінга як Ham. Відомі такі співвідношення для ваги Хеммінга за модулем числа Мерсенна [1].

Лема 1. Для деяких чисел $A, B \in \{0,1\}^n$ та модуля $M_n = 2^n - 1$ виконуються наступні співвідношення:

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

Ще однією перевагою даного типу чисел є те, що множення за модулем числа Мерсенна може бути виконане за допомогою циклічної згортки, обраної дискретним ваговим перетворенням [3]. Таким чином, множення за даним модулем приблизно вдвічі швидше, ніж множення за модулем інших цілих чисел.

Використовуючи арифметику за модулем числа Мерсенна, поняття ваги Хеммінга та описані вище співвідношення було створено задачу MLHRSP – задача ділення чисел з малою вагою Хеммінга за модулем числа Мерсенна [1], ґрунтуючись на якій, було побудовано криптосистему з відкритим ключем AJPS [1].

[a] dariya.yadukha@gmail.com

2. Опис криптосистеми AJPS

Нехай є відкриті параметри $M_n = 2^n - 1$ – число Мерсенна, α – параметр захищеності, заданий під час побудови криптосистеми і h – фіксоване значення, яке задовільняє умовам $4h^2 < n$ та $C_{n-1}^{h-1} \geq 2^\alpha$. 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 – секретний параметр криптосистеми.

Відкритий ключ H обчислюється за формулою

$$H = \frac{F}{G} \bmod M_n.$$

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:

$$b = \begin{cases} 0, & \text{якщо } d \leq 2h^2 \\ 1, & \text{якщо } d \geq n - 2h^2 \\ \text{помилка}, & \text{інакше} \end{cases}$$

Правильність розшифрування випливає з леми 1.

До криптосистеми AJPS 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, що криптосистема є стійкою при умові збільшення параметру захищенності до певного рівня.

3. Обмеження на відкритий ключ криптосистеми AJPS

Навіть відносно стійкі криптосистеми, які використовуються на практиці, часто мають вразливості при деяких значеннях параметрів, тим самим роблячи можливими ситуації, коли криптосистема є нестійкою. Така проблема вирішується накладанням обмежень на вибір відкритих та/або секретних параметрів. Зрозуміло, що кількість таких «вразливих» значень має бути невеликою задля того, щоб обмеження не могли значно зменшити кількість можливих варіантів, а тим самим, пришвидшити повний перебір.

Опишемо обмеження на вибір відкритого ключа H, тобто такі значення параметру H, щоб, знаючи H та C та не знаючи особистий ключ, можна було однозначно визначити відкритий текст (тобто біт b). Нагадаємо, що значення H та C загальновідомі, оскільки H – відкритий ключ, а C – шифротекст, передача якого відбувається відкритим зв'язком.

Твердження 1. У криптосистемі AJPS при значенні відкритого ключа H такому, що

$$Ham(H) \leq 1,$$

можна однозначно визначити повідомлення без знання особистого ключа.

Доведення. Розглянемо випадки, коли розшифрування буде однозначним, навіть без знання особистого ключа. Для розшифрування знаходять значення d:

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

Розглянемо два випадки, відповідно до значення b:

1) Якщо $b = 0$, то $d = Ham((A \cdot H + B) \cdot G \bmod M_n)$. Тоді, використовуючи лему 1 (пункти 1 та 2, який саме з них було використано, відображає позначка над знаком нерівності), маємо:

$$d = Ham((A \cdot H + B) \cdot G \bmod M_n) \overset{2}{\leq}$$
$$\overset{2}{\leq} Ham(A \cdot H + B) \cdot Ham(G) \overset{1}{\leq}$$
$$\overset{1}{\leq} (Ham(A \cdot H) + Ham(B)) \cdot Ham(G) \overset{2}{\leq}$$
$$\overset{2}{\leq} (Ham(A) \cdot Ham(H) + Ham(B)) \cdot Ham(G).$$

Оскільки за умовою криптосистеми числа A, B та G мають вагу Хеммінга h, то отримуємо наступне співвідношення:

$$d \leq (h \cdot Ham(H) + h) \cdot h = h^2 \cdot Ham(H) + h^2 =$$
$$= h^2(Ham(H) + 1).$$

Нагадаємо, що для того, щоб при розшифруванні отримати біт 0 необхідно виконання нерівності $d \leq 2h^2$. Таким чином, маємо наступне співвідношення: $h^2(Ham(H) + 1) \leq 2h^2$. Отже, однозначне розшифрування біту 0 при невідомому особистому ключі можливо при виконанні умови $Ham(H) \leq 1$.

2) Якщо ж $b = 1$, то для розшифрування потрібно обчислити $d = Ham(-(A \cdot H + B) \cdot G \bmod M_n)$. Використовуючи пункт 3 леми 1 маємо:

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

Аналогічно, використовуючи пункти 1 та 2 леми 1, отримуємо:

$$d = n - Ham((A \cdot H + B) \cdot G \bmod M_n) \overset{2}{\geq}$$
$$\overset{2}{\geq} n - (Ham(A \cdot H + B) \cdot Ham(G)) \overset{1}{\geq}$$
$$\overset{1}{\geq} n - ((Ham(A \cdot H) + Ham(B)) \cdot Ham(G)) \overset{2}{\geq}$$
$$\overset{2}{\geq} n - ((Ham(A) \cdot Ham(H) + Ham(B)) \cdot Ham(G)).$$

Враховуючи те, що $Ham(A) = Ham(B) = Ham(G) = h$, маємо $d \geq n - h^2(Ham(H) + 1)$. Оскільки для однозначного розшифрування біту 1 необхідно виконання умови $d \geq n - 2h^2$, то отримуємо співвідношення $n - h^2(Ham(H) + 1) \geq n - 2h^2$. Таким чином, однозначне розшифрування біту 1 при невідомому особистому ключі можливо при виконанні умови $Ham(H) \leq 1$.

Отже, при $Ham(H) \leq 1$ можна визначити значення біту b без знання особистого ключа.

Наслідок. Для запобігання атак, які використовують вразливість, що описана у твердженні 1, потрібно обирати відкритий ключ H криптосистеми AJPS так, щоб $Ham(H) \nleq 1$. Очевидно, що $Ham(H) \neq 0$, а, отже, обмеженням на значення H є:

$$Ham(H) \neq 1.$$

Також існує аналогічне обмеження на обернене відносно операції множення за модулем числа Мерсенна до значення H, яке використовує вразливість, описану далі.

Твердження 2. У криптосистемі AJPS при значенні відкритого ключа H такому, що

$$Ham(H^{-1} \bmod M_n) \leq 1,$$

можна однозначно визначити повідомлення без знання особистого ключа.

Доведення. Для доведення даного обмеження потрібно виразити особистий ключ через відкритий. Оскільки $H = \frac{F}{G} \bmod M_n$, то $H \cdot G = F \bmod M_n$, тоді $G = H^{-1} \cdot F \bmod M_n$. Тепер отримане співвідношення використовуємо у рівності для d:

$$\begin{gathered} d = Ham(C \cdot G \bmod M_n) = \\ = Ham((-1)^b(A \cdot H + B) \cdot G \bmod M_n) = \\ = Ham((-1)^b(A \cdot H + B) \cdot H^{-1} \cdot F \bmod M_n) = \\ = Ham((-1)^b(A \cdot H \cdot H^{-1} + B \cdot H^{-1}) \cdot F \bmod M_n) = \\ = Ham((-1)^b(A + B \cdot H^{-1}) \cdot F \bmod M_n). \end{gathered}$$

Аналогічно доведенню твердження 1, розглядаємо два випадки, використовуємо лему 1 та враховуємо те, що $Ham(A) = Ham(B) = Ham(F) = h$.

$$\begin{gathered} b = 0 : d = Ham((A + B \cdot H^{-1}) \cdot F \bmod M_n) \overset{2}{\leq} \\ \overset{2}{\leq} Ham(A + B \cdot H^{-1} \bmod M_n) \cdot Ham(F) \overset{1}{\leq} \\ \overset{1}{\leq} (Ham(A) + Ham(B \cdot H^{-1} \bmod M_n)) \times \\ \times Ham(F) \overset{2}{\leq} (Ham(A) + Ham(B) \times \\ \times Ham(H^{-1} \bmod M_n)) \cdot Ham(F) = \\ = (h + h \cdot Ham(H^{-1} \bmod M_n)) \cdot h = \\ = h^2(1 + Ham(H^{-1} \bmod M_n)). \end{gathered}$$

Таким чином, для однозначного розшифрування потрібно щоб $h^2(1 + Ham(H^{-1} \bmod M_n)) \leq 2h^2$, тобто $h^2(1 + Ham(H^{-1} \bmod M_n) - 2) \leq 0$. А, отже, отримуємо умову $Ham(H^{-1} \bmod M_n) \leq 1$.

$$\begin{gathered} b = 1 : d = Ham(-(A + B \cdot H^{-1}) \cdot F \bmod M_n) \overset{3}{=} \\ \overset{3}{=} n - Ham((A + B \cdot H^{-1}) \cdot F \bmod M_n) \overset{2}{\geq} \\ \overset{2}{\geq} n - (Ham(A + B \cdot H^{-1} \bmod M_n) \cdot Ham(F)) \overset{1}{\geq} \\ \overset{1}{\geq} n - ((Ham(A) + Ham(B \cdot H^{-1} \bmod M_n)) \times \\ \times Ham(F)) \overset{2}{\geq} n - ((Ham(A) + Ham(B) \times \\ \times Ham(H^{-1} \bmod M_n)) \cdot Ham(F)) = \\ = n - ((h + h \cdot Ham(H^{-1} \bmod M_n)) \cdot h) = \\ = n - h^2(1 + Ham(H^{-1} \bmod M_n)). \end{gathered}$$

Для однозначного розшифрування потрібно, щоб виконувалось $n - h^2(1 + Ham(H^{-1} \bmod M_n)) \geq n - 2h^2$, знову отримали умову $Ham(H^{-1} \bmod M_n) \leq 1$.

Отже, при $Ham(H^{-1} \bmod M_n) \leq 1$ можна однозначно визначити повідомлення без знання особистого ключа.

Наслідок. Для запобігання атак, які використовують вразливість, що описана у твердженні 2, потрібно обирати відкритий ключ H криптосистеми AJPS, враховуючи обмеження $Ham(H^{-1} \bmod M_n) \nleq 1$. Оскільки $Ham(H^{-1} \bmod M_n) \neq 0$, то обмеженням на значення відкритого ключа є

$$Ham(H^{-1} \bmod M_n) \neq 1.$$

Висновки

У даній роботі розглянуто запропоновану 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 обмеження на значення відкритого ключа криптосистеми, а саме обмеження на вагу Хеммінга відкритого ключа та на вагу Хеммінга оберненого відносно операції множення до відкритого ключа за модулем числа Мерсенна.

Перелік використаних джерел

1. D. Aggarwal, A. Joux, A. Prakash, M. Santha. A New Public-Key Cryptosystem via Mersenne Numbers — 2017. — Режим доступу: `https://eprint.iacr.org/2017/481`.
2. M. Beunardeau, A. Connolly, R. Géraud, D. Naccache. On the Hardness of the Mersenne Low Hamming Ratio Assumption — 2017. — Режим доступу: `https://eprint.iacr.org/2017/522`.
3. J. W. Bos, T. Kleinjung, A. K. Lenstra. Efficient SIMD arithmetic modulo a Mersenne number — 2010. — Режим доступу: `https://eprint.iacr.org/2010/338`.
4. Post-Quantum cryptography standardization NIST — Режим доступу: `https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization`.
5. Greg Zaverucha Generalized Mersenne Numbers in Pairing-Based Cryptography — 2006. — Режим доступу: `https://crysp.uwaterloo.ca/software/gmnt/gmz_mcs_thesis.pdf`.