

ПОБУДОВА МОДИФІКАЦІЙ ПРОТОКОЛІВ АВТЕНТИФІКАЦІЇ СТОРІН НА ОСНОВІ ЗАДАЧІ MLHCDP-U

Є. В. Фурутіна^{1,a}, Д. В. Ядуха¹

¹ Навчально-науковий Фізико-технічний інститут

Анотація

У цій роботі досліджуються постквантові протоколи автентифікації сторін, стійкість яких ґрунтується на складності задачі *MLHCDP-U*. Побудовано модифікації цих протоколів шляхом зміни модуля та виконано порівняльний аналіз побудованих модифікацій та оригінальних протоколів. Показано, що перевагою побудованих модифікацій є значне збільшення варіативності параметрів протоколів.

Ключові слова: постквантові задачі, протокол автентифікації, число Мерсенна, узагальнене число Мерсенна

Вступ

Стійкість переважної кількості асиметричних криптосистем, які використовуються сьогодні, ґрунтується на складності задач факторизації або дискретного логарифмування. Такі криптосистеми вважаються захищеними у класичній моделі обчислень, оскільки класичний комп'ютер не може вирішити ці задачі за поліноміальний час. Проте із створенням масштабованого квантового комп'ютера усі дані, що захищені такими методами, опиняться під загрозою, бо цьому комп'ютеру буде під силу вирішити обидві задачі за поліноміальний час. Тому протягом останніх років активно досліджуються інші типи криптосистем, які були б стійкими до атак як з використанням класичного, так і квантового комп'ютерів. Такі криптосистеми називаються *постквантовими* або *квантово-стійкими*.

З 2017 по 2024 роки тривав основний етап конкурсу постквантових криптографічних примітивів Національного інституту стандартів і технологій США (NIST) [1], який мав на меті зібрати якомога більше ідей та підходів для побудови постквантових криптосистем, щоб розробити нові стандарти цифрового підпису, асиметричного шифрування та встановлення ключів, зокрема інкапсуляції ключів.

Усього проведено 3 основні раунди та ініційовано додатковий раунд, який триває дотепер. Основними критеріями відбору на всіх етапах конкурсу були рівень захищеності та стійкості, дослідженість підходу побудови, а також ефективність реалізації.

В результаті третього раунду конкурсу переможцями обрано один криптопримітив у категорії «Криптопримітиви для шифрування та встановлення ключа» під назвою *CRYSTALS-KYBER* та три в категорії «Криптопримітиви для цифрового підпису»:

CRYSTALS-DILITHIUM, *FALCON* та *SPHINCS+*. Список переможців опублікували у 2022 році, а вже у 2024 у відкритому доступі з'явилися розроблені стандарти: *FIPS 203* (Стандарт механізму інкапсуляції ключів на основі модульної решітки), *FIPS 204* (Стандарт цифрового підпису на основі модульної решітки) та *FIPS 205* (Стандарт цифрового підпису без збереження стану) [1].

Серед криптографічних примітивів, які були подані до участі у першому раунді конкурсу, був й механізм інкапсуляції ключів під назвою *Mersenne-756839*, що побудований на основі криптосистеми *AJPS*. Назва *AJPS* була сформована з перших літер прізвищ розробників — Дівеша Аггарвала (*Divesh Aggarwal*), Антуана Жу (*Antoine Joux*), Анупама Пракаша (*Anupam Prakash*) та Мікоса Сантхи (*Mikos Santha*).

1. Задача MLHCSP та її модифікації

Криптосистема *AJPS* основана на арифметиці за модулем чисел Мерсенна. Усього було дві версії цієї криптосистеми. Перша має назву *AJPS-1*, її стійкість ґрунтується на складності задачі *MLHRSP* (англ. *Mersenne Low Hamming Ratio Search Problem*) [2].

Тут і далі будемо використовувати наступні позначення:

- $M_n = 2^n - 1$, де $n \in \mathbb{N}$ — число Мерсенна;
- $Ham(x)$ — вага Геммінга (кількість 1 в бітовому представленні числа x);
- $HM_{n,h} = \{x \in \mathbb{Z}_{M_n} : Ham(x) = h\}$ — множина лишків за модулем M_n з вагою Геммінга h .

Наведемо означення задачі *MLHRSP*.

Означення 1. Задача ділення чисел з малою вагою Геммінга за модулем числа Мерсенна (*MLHRSP*) формулюється так: нехай M_n — число Мерсенна та h — ціле число; $F, G \in HM_{n,h}$. Тоді за заданим

^afurutina@gmail.com

$H = F \cdot G^{-1} \pmod{M_n}$ потрібно відновити F, G .

AJPS-1 дозволяє шифрувати лише один біт за одне застосування процедури шифрування, тож вона виявилася не дуже ефективною. Пізніше автори описали *AJPS-2*, яка дозволяє шифрувати блок бітів за одне застосування процедури шифрування і має більші параметри безпеки, що підвищує її захищеність, зокрема до атак на основі алгоритмів на решітках. Її стійкість ґрунтується на складності задачі *MLHCSP* (англ. *Mersenne Low Hamming Combination Search Problem*).

Означення 2. *Задача лінійної комбінації чисел з малою вагою Геммінга за модулем числа Мерсенна (MLHCSP)* полягає в наступному: нехай M_n — число Мерсенна та h — ціле число та нехай $R \in Z_{M_n}$ та $F, G \in HM_{n,h}$. Тоді, маючи кортеж $(R, F \cdot R + G \pmod{M_n})$, треба знайти F, G [2].

З часом ця задача була модифікована у задачу *MLHCSP-U* (*MLHCSP with uniform secret*); модифікація відрізняється тим, що значення F має довільну вагу Геммінга, тоді як у задачі *MLHCSP* $Ham(F) = h$.

Означення 3. *Задача MLHCSP-U* формується так: нехай M_n — число Мерсенна та h — ціле число та нехай $R, F \in Z_{M_n}$ та $G \in HM_{n,h}$. Тоді, маючи кортеж $(R, F \cdot R + G \pmod{M_n})$, треба знайти F, G [3].

Розглянемо модифікацію задачі *MLHCSP-U* — задачу розрізнення *MLHCDP-U* (англ. *Mersenne Low Hamming Combination Distinguishing Problem with Uniform Secret*) [3]. Позначимо як $\mathcal{O}_{S,n,h}$ — оракул, який за заданими числом Мерсенна M_n , цілим числом h ($n > h$) та S_1 , де $S_1 \in Z_{M_n}$ обирає число R_1 з Z_{M_n} (випадково та рівномірно) та G_1 з множини $HM_{n,h}$ і повертає пару (R_1, T_1) , де $T_1 = S_1 \cdot R_1 + G_1 \pmod{M_n}$; та $\mathcal{U}$ — оракул, який повертає довільну пару (A_1, B_1) з множини $Z_{M_n}^2$.

Означення 4. *Задача розрізнення MLHCDP-U* полягає в розрізненні пар (R_1, T_1) та (A_1, B_1) , які повертають оракули $\mathcal{O}_{S,n,h}$ і $\mathcal{U}$ відповідно.

2. Модифікація задачі MLHCDP-U та протоколів автентифікації шляхом зміни модуля

Для побудови модифікації задачі *MLHCDP-U* шляхом зміни класу чисел, що використовується як модуль, розглянемо клас узагальнених чисел Мерсенна виду $GM_{n,m} = 2^n - 2^m - 1$, де $n, m \in \mathbb{N}$ та $n > m$. На відміну від числа Мерсенна M_n , яке у двійковому представленні має вигляд послідовності з n одиниць, узагальнене число Мерсенна у двійковому представленні має рівно один нуль. Перехід на узагальнені числа Мерсенна є логічним, оскільки для них, так само як і для звичайних чисел Мерсенна, є алгоритми швидкого обчислення операцій за модулем; крім того, для узагальної форми числа Мерсенна простих значень більше, ніж для класичної.

Також опишемо множину лишків за модулем $GM_{n,m}$ з вагою Геммінга h .

$$HG_{n,m,h} = \{x \in Z_{GM_{n,m}} : Ham(x) = h\}.$$

Виначимо модифікацію задачі розрізнення *MLHCDP-U* з використанням арифметики за модулем узагальненого числа Мерсенна — задачу *GMLHCDP-U* (англ. *Generalized-Mersenne Low Hamming Combination Distinguishing Problem with Uniform Secret*).

Позначимо як $\tilde{\mathcal{O}}_{S,n,h}$ — оракул, який за заданими узагальненим числом Мерсенна $GM_{n,m}$, цілим числом h ($n > h$) та S_2 , де $S_2 \in Z_{GM_{n,m}}$ обирає число R_2 з $Z_{GM_{n,m}}$ (випадково та рівномірно) та G_2 з множини $HG_{n,m,h}$ і повертає пару (R_2, T_2) , де $T_2 = S_2 \cdot R_2 + G_2 \pmod{GM_{n,m}}$; та $\tilde{\mathcal{U}}$ — оракул, який повертає довільну пару (A_2, B_2) з множини $Z_{GM_{n,m}}^2$.

Означення 7. *Задача розрізнення GMLHCDP-U* полягає в розрізненні пар (R_2, T_2) та (A_2, B_2) , які повертають оракули $\tilde{\mathcal{O}}_{S,n,h}$ і $\tilde{\mathcal{U}}$ відповідно.

На основі задачі *MLHCDP-U* побудовано три протоколи автентифікації з різними рівнями захищеності:

- протокол, стійкий до атак з використанням моделі пасивного злоумисника;
- протокол, стійкий до атак з використанням моделі активного злоумисника;
- протокол, стійкий до атак типу MITM (англ. *Man-in-the-middle*),

а також MAC-код (англ. *Message Authentication Code*) [3].

Протокол односторонньої автентифікації — це процедура, за допомогою якої сторона, що доводить, підтверджує свою справжність стороні, що перевіряє. Позначимо V (англ. *verifier*) — сторона, що перевіряє, та P (англ. *prover*) — сторона, яка доводить.

Побудуємо модифікації протоколів на основі *GMLHCDP-U*, використовуючи клас узагальнених чисел Мерсенна. Ці модифікації будуються аналогічно оригінальним; відмінність в тому, що використовується інший модуль (M_n змінюється на $GM_{n,m}$) та інша множина лишків за модулем з вагою Геммінга h (замість $HM_{n,h}$ береться $HG_{n,m,h}$).

Протокол 1. Нехай $Z_{GM_{n,m}}$ — кільце лишків за модулем $GM_{n,m}$.

1. Обирається спільний для обох учасників ключ $sk = R$ з множини $Z_{GM_{n,m}}$ (випадково і рівномірно);
2. V обирає F з множини $Z_{GM_{n,m}}$ і передає його P ;
3. P обирає G з множини $HG_{n,m,h}$; обчислює

$$T = F \cdot R + G \pmod{GM_{n,m}}$$

і передає його V ;

4. V перевіряє, чи

$$Ham(T - F \cdot R \pmod{GM_{n,m}}) = h;$$

якщо так, то автентифікація пройшла успішно. Це виконується, оскільки

$$T - F \cdot R = G \pmod{GM_{n,m}},$$

а G обиралося з множини $HG_{n,m,h}$, тобто має вагу Геммінга h ; таким чином, у цьому випадку P обрав значення G правильно.

Таблиця 1. Порівняння кількості унікальних значень T та максимальної кількості повторень для T для кожного з протоколів із використанням різних модулів при 55000000 ітерацій.

	Кількість унікальних значень T		Кількість повторів значень T		Максимальна кількість повторень для одного T	
	$p = M_n$	$p = GM_{n,m}$	$p = M_n$	$p = GM_{n,m}$	$p = M_n$	$p = GM_{n,m}$
Протокол 1	54301546	54296446	698454	703554	4	4
Протокол 2	54301687	54295556	698313	704444	4	4
Протокол 3	54303259	54302658	696741	697342	4	5

Протокол 2. Нехай $Z_{GM_{n,m}}$ — кільце лишків за модулем $GM_{n,m}$.

1. Обирається спільний для обох учасників ключ $sk = (S_1, S_2)$ з множини $Z_{GM_{n,m}}^2$ (випадково і рівномірно);

2. V обирає F з множини $Z_{GM_{n,m}}$ і передає його P ;

3. P обирає G з множини $HG_{n,m,h}$ та деяке R з множини $Z_{GM_{n,m}}$; обчислює

$$T = R \cdot (S_1 \cdot F + S_2) + G \pmod{GM_{n,m}}$$

і передає V пару (R, T) ;

4. V перевіряє, чи $R \neq 0$ та чи

$$Ham(T - R \cdot (S_1 \cdot F + S_2) \pmod{GM_{n,m}}) = h;$$

якщо так, то автентифікація пройшла успішно. Це виконується, оскільки

$$T - R \cdot (S_1 \cdot F + S_2) = G \pmod{GM_{n,m}},$$

а G обиралося з множини $HG_{n,m,h}$, тобто має вагу Геммінга h ; таким чином, у цьому випадку P обрав значення G правильно.

Протокол 3. Нехай $Z_{GM_{n,m}}$ — кільце лишків за модулем $GM_{n,m}$.

1. Обирається спільний для обох учасників ключ $sk = (X_1, X_2, X_3, X_4)$ з множин $Z_{GM_{n,m}}^*$, $Z_{GM_{n,m}}$, $Z_{GM_{n,m}}^*$ та $Z_{GM_{n,m}}$ відповідно (випадково і рівномірно);

2. V обирає F з множини $Z_{GM_{n,m}}$ і передає його P ;

3. P обирає G з множини $HM_{n,h}$ та деяке R з множини $Z_{GM_{n,m}}$; обчислює

$$T = R \cdot (X_1 \cdot F + X_2) + X_3 \cdot G + X_4 \pmod{GM_{n,m}}$$

і передає V пару (R, T) ;

4. V перевіряє, чи $R \neq 0$ та чи

$$Ham(X_3^{-1} \cdot (T - R \cdot (S_1 \cdot F + S_2) - X_4) \pmod{GM_{n,m}}) = h;$$

якщо так, то автентифікація пройшла успішно. Це виконується, оскільки

$$T - R \cdot (S_1 \cdot F + S_2) - X_4 = X_3 \cdot G \pmod{GM_{n,m}}$$

і $X_3 \cdot G \cdot X_3^{-1} = G$, а G обиралося з множини $HG_{n,m,h}$, тобто має вагу Геммінга h ; таким чином, у цьому випадку P обрав значення G правильно.

Порівнюємо значення T для протоколів на основі MLHCDP-U та GMLHCDP-U.

3. Порівняння результатів

Для порівняння оригінальних протоколів автентифікації та побудованих модифікацій з використанням узагальнених чисел Мерсенна виконано аналіз кількості унікальних значень параметру T , за допомогою якого P проходить перевірку автентичності. Експериментальні результати, що описані у таблиці 1, отримані в результаті 55000000 застосувань кожного протоколу.

Проаналізувавши отримані результати, можна побачити, що кількість унікальних значень T для узагальненого числа Мерсенна дещо зменшилась, але не значно. Крім того, максимальна кількість повторень для кожного значення T не зросла, тобто, не дивлячись на зменшення простору значень для числа, розподіл залишився згладженим, і пікові значення параметру T не з'явилися.

Висновок

У роботі проведено дослідження протоколів автентифікації, що оснований на задачі MLHCDP-U. Побудовано модифікації таких протоколів шляхом зміни класу чисел, що використовуються як модуль — замість чисел Мерсенна у модифікаціях застосовуються узагальнені числа Мерсенна. Побудовані модифікації протоколів дозволили значно збільшити кількість використовуваних модулів, оскільки кількість простих узагальнених чисел Мерсенна значно більша за кількість простих чисел Мерсенна, і при цьому розподіл значень, які використовуються для автентифікації, не значно змінився, що підтверджено експериментально.

Перелік використаних джерел

1. Post-Quantum Cryptography, National Institute of Standards and Technology. — <https://www.nist.gov/pqc/crypto>.
2. A New Public-Key Cryptosystem via Mersenne Numbers / D. Aggarwal, A. Joux, A. Prakash, M. Santha. — 2017. — <https://eprint.iacr.org/2017/481.pdf>.
3. Ferradi H., Xagawa K. Post-Quantum Provably-Secure Authentication and MAC from Mersenne Primes // The Hong Kong Polytechnic University, Hong Kong; NTT Secure Platform Laboratories, Japan. — 2019. — <https://eprint.iacr.org/2019/409.pdf>.