УДК 519.9
DOI: 10.32626/2308-5916.2019-19.44-49

Ю. І. Горбенко*, канд. техн. наук,
О. С. Акользіна,**
В. О. Подгайко,** магістр

*АТ «Інститут інформаційних технологій», м. Харків,
**Національний університет імені В. Н. Каразіна, м. Харків

АНАЛІЗ АКТУАЛЬНИХ ПРОБЛЕМНИХ ПИТАНЬ ЩОДО ПЕРСПЕКТИВНОЇ АСИМЕТРИЧНОЇ КРИПТОГРАФІЇ

Наведений аналіз актуальних досліджень щодо криптографії на решітках. Аналіз відбувається відповідно до найбільш актуальних алгоритмів, що пройшли до другого етапу конкурсу NIST США. Деякі з них комбіновані — включають в себе декілька схожих алгоритмів з минулого етапу. Для детального їх розгляду приведено ряд актуальних тем дослідження для пост-квантових алгоритмів, що дозволяє описувати та класифікувати їх більш суттєво.

Ключові слова: *решітка, постквантовий алгоритм, LWE, кільце, інкапсуляція.*

Вступ. Нині на світовому рівні проводяться дослідження проблеми створення перспективних стандартів асиметричної криптографії — асиметричних шифрів (АСШ), протоколів інкапсуляціє ключів (ПІК) та електронного підпису (ЕП).

Попередні дослідження та перший етап їх суспільного обговорення показали, що певні переваги для реалізації стандартів щодо асиметричної криптографії має математичний апарат криптографічних перетворень у кільцях поліномів [1, 2]. Нині його називають крипто перетвореннями на алгебраїчних решітках, це пов'язане з тим, що доведення його стійкості ґрунтувалось на методах алгебраїчних решіток. На наш погляд, важливим є аналіз цього напрямку з токи зору створення перспективних стандартів асиметричної криптографії у кільцях поліномів з додатковими перетвореннями. Аналіз даних таблиці показує, що всього до 2 раунду конкурсу пройшло 17 кандидатів (із 40). Також, як видно із даних таблиці пройшли у 2 раунд 14 кандидатів, що ґрунтуються на математичних кодах та 4 на мультиваріативних перетвореннях. Серед інших необхідно виділити SIKE та SPHINCK+. Тому важливим завданням другого етапу конкурсу NIST США є подальше порівняння кандидатів.

Мета даної роботи — систематизація знань відносно процесу постквантової стандартизації, аналізу стану, основних властивостей кандидатів та конкретизація напрямку подальших досліджень із створення перспективних АСШ, ПІК та ЕП та їх порівняння.

Таблиця

Механізм	Математичні методи	Назви алгоритмів	Кіль-кість
Направлене шифрування	Решітки	CRYSTALS-KYBER, LAC, NTRU, Round5, SABER, Three Bears	7
	Коди	Classic McEliece, HQC, ROLLO, LEDAcrypt, RQC	6
	Інше	SIKE	1
	Усього кандидатів		14
Протоколи обміну ключами	Алгебраїчні решітки	CRYSTALS-KYBER, LAC, FrodoKEM, NewHope, NTRU, NTRU Prime, SABER, Three Bears	8
	Коди	BIKE, Classic McEliece, HQC, LEDAcrypt, NTS-KEM, ROLLO, RQC	8
	Інше	SIKE	1
	Усього кандидатів		17
Електронний підпис	Алгебраїчні решітки	CRYSTALS-DILITHIUM, FALCON, qTesla	3
	Мультиваріативні перетворення	GeMSS, LUOV, MQDSS, Rainbow	4
	Геш-перетворення	SPHINCK+	1
	Інше	Picnic	1
	Усього кандидатів		9

1. Аналіз стану створення стандартів асиметричної криптографії. Проведений аналіз показав, що до першого раунду конкурсу NIST США було допущено 69 кандидатів, 31 січня 2019 року інститутом NIST опубліковано перелік заявок, які пройшли до другого раунду конкурсу пост-квантової стандартизації [1]. Цей раунд, як повідомив представник NIST США Дастін Муді, буде тривати від 12 до 18 місяців. Деякі з них були об'єднані та автори об’єднаних проектів сформували комбіновані криптосистеми. Серед комбінованих заявок наступні [1]: LEDAcrypt (поєднання LEDAkem та LEDApkc), NTRU (поєднання NTRUEncrypt та NTRU-HRSS-KEM), ROLLO (поєднання LAKE, LOCKER та Ouroboros-R), Round5 (поєднання HILA5 та Round2). У таблиці наведена класифікація алгоритмів другого раунду за математикою та механізмами, що були застосованими.

Таким чином, із 69 проектів на другий етап рекомендовано 40 кандидатів на стандарти асиметричної криптографії — АСШ, ПІК та ЕП.

Попередні дослідження [3] дозволили визначити важливі та проблемні питання подальших досліджень. Основними з них є такі як:

- класичний та квантовий криптоаналіз кандидатів, включаючи криптоаналіз спрощених та демо-версій;

- аналіз відносної швидкодії або ресурсних вимог до кандидатів;
- оцінка класичної та квантової стійкості кандидатів;
- систематизація знань відносно процесу стандартизації NIST PQC;
- істотне покращення реалізації алгоритмів;
- вдосконалення аналізу або доведення властивостей кандидатів, навіть якщо це не призводить до якоїсь атаки;
- пропозиції критеріїв для вибору алгоритмів для стандартизації;
- вплив на існуючі додатки та протоколи. Наприклад, які зміни необхідні для впровадження конкретних кандидатів;
- підготовчі кроки або стратегії для організацій до майбутнього переходу на пост квантову криптографію.

2. Огляд та попередній аналіз деяких кандидатів на стандарти перспективних асиметричних крипто перетворень. Попередній аналіз та дослідження практичних реалізацій дозволили виділити такі проекти [1]: NTRU Prime, ThreeBears, Saber, Round5, CRYSTALS-Kyber та SPHINCS +. Розглянемо їх та проведемо попередній аналіз.

2.1. Проект NTRU Prime. Модернізований NTRU Prime [2] розроблений з метою забезпечити IND-CCA2 стійкості, тобто стійкості проти атак з адаптивно-підібраним шифртекстом. При реалізації такої моделі безпеки, сервер може повторно використовувати відкриті ключі будь-яку кількість разів, що спрощує вартість генерації та узгодження ключа. Для встановлення нового сеансового ключа, включаючи постквантовий сервер автентифікації, необхідне лише одне зашифрування для клієнта та одне розшифрування для серверу. Тому в модернізований NTRU Prime має важливі переваги у швидкодії при виконанні механізму обміну. Інші властивості NTRU Prime можна знайти в [2].

2.2. ThreeBears. Криптосистема ThreeBears [4] заснована на криптосистемах навчання з помилками у кільці (RLWE) Lyubashevsky-Peikert-Regev [5] та Ding [6]. Більш точно, вона заснована на NewHope [7] та Kyber [8], остання з яких використовує модульне навчання з помилками (MLWE). Автори ThreeBears замінили кільце поліномів, що лежить в основі цього модуля, на цілий модуль, узагальнене число Мерсена, за рахунок цього з'являється цілий модуль навчання з помилками (I-MLWE).

ThreeBears названа таким чином, через те, що її модуль має однакову форму «золотого співвідношення Солінас», та насправді деякий арифметичний код з її реалізації отриманий з арифметичного коду Goldilocks.

Одна з цілей ThreeBears — сприяти дослідженню потенційно бажаних, але менш традиційних систем. Через це ThreeBears використовує I-MLWE замість MLWE, через це особистий ключ є лише рядком, через це використовується явне відхилення, і через це відсутнє гешування Targhi-Unruh.

2.3. Saber. Saber представляє собою родину криптопримітивів, які засновані на складності Задачі Модульного навчання з округленням (Module Learning With Rounding problem — Mod-LWR) [9]. Спершу описується Saber.PKE — IND-CPA стійка схема шифрування, та її перетворення в Saber.KEM, IND-CCA стійкий механізм інкапсуляції ключа, з використанням перетворення Fujisaki-Okamoto. Цілями розробки були простота, швидкодія та гнучкість, які спричинили наступні рішення: усі цілі модулі є степенями 2, що дозволяє повністю уникнути зведення за модулем та вибірку з відхиленням; використання LWR зменшує вдвічі розмір необхідної випадковості у порівнянні з LWE-схемами та знижує пропускну здатність; модульна структура забезпечує гнучкість за рахунок повторного використання одного кореневого компоненту для багатьох рівнів стійкості.

2.4. Round5. Заявка Round5 складається з заявок Round2 та Hila5 [10]. Ключовою характеристикою Round2 є те, що він був розроблений, щоб визначити задачу навчання з округленням (Learning with Roundings — LWR) та Ring LWR задачу однаковим чином. Це досягається за рахунок Загальної LWR задачі, на якій заснований Round2, який може визначити LWR або RLWR в залежності від вхідних параметрів. Причини такого вибору наступні.

Round2 є адаптивним та може бути застосований до багатьох середовищ. З іншого боку, алгоритми на основі LWR є бажаними у тих середовищах, в яких швидкодія — найменша проблема, а стійкість — першочергова. В таких випадках бажано, щоб були відсутні додаткові кільцеві структури (як у ідеальних решітках [4, 5]). З іншого боку, алгоритми на основі RLWR забезпечують кращу швидкодію для пропускної здатності та обчислень, тож вони краще підходять для обмежених середовищ з вимогами обмеження пропускної здатності, наприклад, через складність фрагментації повідомлення.

Round2 зменшує аналіз коду та керування, так як єдине визначення для схем Round2.KEM та Round2.PKE визначають різні задачі, LWR та RLWR з одним кодом.

HILA5 використовує новий метод узгодження для Ring-LWE, який має значно меншу швидкість відмови, ніж попередні пропозиції, одночасно зменшуючи розмір шифртексту і кількість обов'язкової випадковості. Вона заснована на простому, детерміністичному варіанті погодження Peikert, який працює з нашим новим вибором «безпечних бітів» та методами корекції помилок постійного часу. Новий метод не потребує рандомізованого згладжування для досягнення необмежених секретів. Автори виконують аналіз комбінаторних відмов, використовуючи повні вірогідні згортки, що веде до точного розуміння умов відмови розшифрування на рівні бітів. Навіть із додатковими заходами безпеки та безпечності, нова схема, як і раніше, настільки ж швидко, як New Hope, але

має трохи коротші повідомлення. Нові методи були інсценировані та впроваджені як механізм інкапсуляції ключа (KEM) та схема шифрування відкритого ключа, розроблена для задоволення вимог постквантової криптографії NIST на найвищому рівні безпеки.

2.5. CRYSTALS-Kyber. Kyber — це IND-CCA2 безпечний механізм інкапсуляції ключів (KEM) [8]. Безпека Kyber заснована на складності вирішення проблеми навчання-з-помилками в модульних решітках (проблема MLWE). Побудова Kyber відбувається за двоетапним підходом: спочатку автори представляють схему шифрування загальнодоступного ключа INDCPA безпеки, що шифрує повідомлення фіксованої довжини 32 байтів, яка називається Kyber.CPAPKE. Потім використовується злегка змінене перетворення Fujisaki-Okamoto (FO), щоб побудувати IND-CCA2 безпечний KEM.

2.6. SPHINCS +. На високому рівні, SPHINCS + працює як SPHINCS [11]. Основна ідея полягає в автентифікації великої кількості ключових пар багаторазового підпису (FTS), використовуючи так зване гіпердерево. Схеми FTS — схеми підпису, які дозволяють парі ключів виготовити невелику кількість підписів, наприклад, порядку десяти для наших наборів параметрів.

Для кожного нового повідомлення ключова пара (псевдовипадкових) FTS підбирається для підпису повідомлення. Підпис складається, таким чином, з підпису FTS та інформації про автентифікацію для цієї ключової пари FTS. Інформація про автентифікацію приблизно є підписом гіпердерева, тобто підписом використовується дерево сертифікації підписів дерева Мерклі.

Висновки. 1. Попередній аналіз, результати якого наведені в таблиці, показав, що до 2 раунду конкурсу пройшло 17 кандидатів (із 40), що засновані та перетвореннях у кільцях поліномів. Також, як видно із даних таблиці, у другий раунд пройшли 14 кандидатів, що ґрунтуються на математичних кодах та 4 на мультиваріативних перетвореннях. Серед інших необхідно виділити SIKE та SPHINCK+.

2. Якщо розглядати АСШ як складову ПІК, то тоді до другого раунду процесу постквантової стандартизації пройшло усього 26 криптосистем (9 алгоритмів ЕП, 17 АСШ та ПІК).

3. Необхідно проводити подальші дослідження основних властивостей кандидатів та провести їх порівняння за прийнятими критеріями. На наш погляд для цього необхідно застосовувати обґрунтовану методику з відповідними критеріями.

4. В процесі попередніх досліджень визначені проблемні питання та пріоритетні напрямки досліджень, вони стосуються таких питань: оцінювання алгоритмів, формування критеріїв, класичний і квантовий криптоаналіз, вдосконалення аналізу та визначення необхідних змін для практичного впровадження постквантових алгоритмів.

Список використаних джерел:

1. URL: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.
2. URL: https://ntruprime.cr.yp.to.
3. URL: https://groups.google.com/a/list.nist.gov/forum/#!forum/pqc-forum.
4. URL: https://sourceforge.net/ projects/threebears/
5. URL: https://eprint.iacr.org/2012/230.pdf.
6. URL: https://eprint.iacr.org/2012/688.
7. URL: https://newhopecrypto.org.
8. URL: https://eprint.iacr.org/2017/634.pdf.
9. URL: https://eprint.iacr.org/2018/230.pdf.
10. URL: https://round5.org.
11. URL: https://cryptojedi.org/papers/sphincs-20141001.pdf.

ACTUAL ISSUES ANALYSIS REGARDING PERSPECTIVE PUBLIC-KEY CRYPTOGRAPHY

An analysis of current research on cryptography on lattices is given. The analysis takes place in accordance with the most relevant algorithms that have gone through the second stage of the US NIST competition. Some of them are combined — include several similar algorithms from the past stage. For a detailed consideration of them, a number of relevant topics for post-quantum algorithms are presented, which allows them to be described and categorized more substantially.

Key words: *lattice, post-quantum algorithm, LWE, ring, encapsulation.*

Одержано 02.12.2018

УДК 004.056.55
DOI: 10.32626/2308-5916.2019-19.49-55

М. В. Єсіна, канд. техн. наук

АТ «Інститут інформаційних технологій»,
Харківський національний університет імені В. Н. Каразіна, м. Харків

МОДЕЛІ БЕЗПЕКИ ПОСТКВАНТОВИХ КРИПТОГРАФІЧНИХ ПРИМІТИВІВ

У даній роботі розглядається сутність та досліджуються моделі безпеки щодо асиметричних постквантових криптографічних примітивів різного типу. За основу взяті моделі безпеки, які рекомендовані NIST США у вимогах конкурсу PQC до кандидатів на постквантові криптографічні примітиви. До таких алгоритмів відносяться асиметричні криптографічні перетворення типу асиметричне шифрування, цифровий підпис та механізм інкапсуляції ключів. Рекомендованими є наступні моделі безпеки, які стосуються: щодо асиметричного шифрування — IND-CCA2 (IND-CPA, IND-CCA); щодо цифрового підпису — EUF-CMA (та її варіації); щодо механізмів інкапсуляції ключів —