УДК 004.056.5 **DOI:10.30837/rt.2022.3.210.05**

М.В. ЄСІНА, канд. техн. наук, Є.В. ОСТРЯНСЬКА, І.Д. ГОРБЕНКО, д-р техн. наук

СТАН ТРЕТЬОГО РАУНДУ ПРОЦЕСУ СТАНДАРТИЗАЦІЇ ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ NIST

Вступ

В останні роки спостерігається стійкий прогрес у створенні квантових комп'ютерів. У разі реалізації великомасштабних квантових комп'ютерів вони будуть загрожувати безпеці багатьох широко використовуваних криптосистем з відкритим ключем. Схеми встановлення ключів і цифрові підписи, що засновані на факторизації, дискретних логарифмах і криптографії на еліптичних кривих, найбільш сильно постраждають. Симетричні криптографічні примітиви, такі як блокові шифри і геш-функції, будуть порушені незначно. Внаслідок цього було активізовано дослідження щодо пошуку криптосистем на відкритих ключах, які були б захищені від криптоаналітиків як з квантовими, так і з класичними комп'ютерами. Цю область часто називають постквантовою криптографією (PQC), або іноді квантово-стійкою криптографією. Її мета полягає в розробці схем, які можна розгорнути в існуючих комунікаційних мережах та протоколах без суттєвих змін.

Національний інститут стандартів і технологій знаходиться в процесі вибору одного або декількох криптографічних алгоритмів з відкритим ключем за допомогою відкритого конкурсу. Нові стандарти криптографії з відкритим ключем визначатимуть одну або кілька додаткових цифрових підписів, шифрування з відкритим ключем і алгоритми встановлення ключів. Передбачається, що ці алгоритми будуть здатні добре захищати конфіденційну інформацію в недалекому майбутньому, в тому числі після появи квантових комп'ютерів.

Після багаторічного огляду кандидатів NIST вибрав 26 алгоритмів для переходу до 2-го раунду оцінки у січні 2019 року [1]. Ці алгоритми розглядалися як найбільш перспективні кандидати для можливої стандартизації і були обрані на основі як внутрішнього аналізу, так і відгуків спільноти. Під час 2-го раунду ці кандидати були піддані більш детальному аналізу з боку NIST і більш широкого криптографічного співтовариства. Після ретельного обговорення NIST вибрав сім фіналістів та вісім альтернативних варіантів, щоб перейти до 3-го раунду в липні 2020 року [2]. Намір NIST полягав у стандартизації невеликої кількості фіналістів наприкінці 3-го раунду, а також невеликої кількості альтернативних кандидатів після 4-го раунду.

3-й раунд розпочався в липні 2020 року і тривав приблизно 18 місяців. Під час 3-го раунду відбувся більш ретельний аналіз теоретичних та емпіричних доказів, що використовуються для обґрунтування безпеки кандидатів. Також проводилось ретельне оцінювання їх продуктивності, використовуючи оптимізовані реалізації на різних програмних та апаратних платформах.

Після трьох раундів оцінки та аналізу NIST вибрав перші алгоритми, які він стандартизує в результаті процесу стандартизації PQC.

Метою цієї статті є огляд та аналіз стану оцінювання та відбору процесу стандартизації постквантової криптографії NIST. У звіті узагальнено кожен із 15 алгоритмів-кандидатів 3-го раунду та визначено обрані для стандартизації, а також ті, які продовжуватимуть оцінюватись у 4-му раунді аналізу. Алгоритм шифрування на відкритому ключі та встановлення ключа, який буде стандартизовано, – Crystals-Kyber. Цифрові підписи, що будуть стандартизовані, – Crystals-Dilithium, Falcon та Sphincs+. Незважаючи на те, що обирається декілька алгоритмів підпису, NIST рекомендує Crystals-Dilithium як основний алгоритм, що повинен бути реалізований. Крім того, чотири альтернативні алгоритми-кандидати встановлення ключа проходять до 4-го раунду оцінювання: BIKE, Classic McEliece, HQC та SIKE. Ці кандидати все ще розглядаються для майбутньої стандартизації [3].

1. Критерії оцінювання та процес відбору кандидатів

NIST обрав 15 алгоритмів-кандидатів для 3-го раунду. Сім з п'ятнадцяти алгоритмів були обрані у якості алгоритмів-фіналістів, в той час як інші вісім були позначені як «альтернативні варіанти» [2]. Набір фіналістів включав алгоритми, які NIST вважав найбільш перспективними, такими, що відповідають більшості випадків використання, і найімовірніше, що будуть готові до стандартизації незабаром після закінчення 3-го раунду. Альтернативні кандидати вважалися потенційними кандидатами для майбутньої стандартизації, швидше за все, після чергового раунду оцінки. Деякі з альтернативних кандидатів мають гірші характеристики ефективності, ніж фіналісти, але можуть бути вибрані для стандартизації на основі високої впевненості NIST у їх безпеці. Інші мають прийнятну ефективність, але потребують додаткового аналізу чи іншої роботи, щоб забезпечити достатню гарантію їх безпеки для стандартизації NIST. Крім того, деякі альтернативні кандидати були обрані на основі прагнення NIST до різноманітності в майбутніх постквантових стандартах безпеки, або на їх потенціалі для подальшого вдосконалення.

Сім фіналістів включали у себе чотири механізми інкапсуляції ключів (KEM) та три механізми цифрового підпису. З восьми альтернативних варіантів п'ять – KEM та три – цифрові підписи. Командам подання було дозволено внести незначні модифікації та повторно подати свої пакети, які повинні були відповідати тим же вимогам, що і оригінальні подання. Повні оновлені технічні характеристики були розміщені на веб-сайті PQC NIST [3] 23 жовтня 2020 року для публічного огляду.

Таблиця 1

Фіналісти третього раунду

Шифрування на відкритому ключі/KEM	Цифрові підписи
Classic McEliece	Crystals-Dilithium
Crystals-Kyber	Falcon
NTRU	Rainbow
Saber	

Таблиця 2

Альтернативні кандидати третього раунду

Шифрування на відкритому ключі/KEM	Цифрові підписи
BIKE	GeMSS
FrodoKEM	Picnic
HQC	SPHINCS+
NTRU Prime	
SIKE	

1.1. Критерії оцінювання

У Call for Proposals NIST [4] визначено три широкі аспекти критеріїв оцінки, які будуть використовуватися для порівняння відповідних алгоритмів в процесі стандартизації PQC NIST: 1) безпека, 2) вартість і продуктивність та 3) характеристики алгоритму і реалізації. Ці критерії описані нижче разом з обговоренням того, як вони вплинули на оцінювання кандидатів у 2-му раунді.

Як і у випадку з минулими конкурсами Розширений стандарт шифрування (AES) і Безпечний алгоритм гешування 3 (SHA-3), безпека є найбільш важливим фактором, що NIST використовує при оцінці кандидатів на постквантові алгоритми. Нинішні стандарти з відкритим ключем NIST використовуються у самих різних додатках, включаючи Інтернет-протоколи, такі як TLS, SSH, IKE, IPsec і DNSSEC, а також для сертифікатів, підпису програмного коду і безпечних завантажувачів. Нові стандарти NIST на відкритому ключів забезпечать постквантову безпеку для кожного з цих додатків.

Для кількісної оцінки безпеки можливих алгоритмів NIST дав три можливі визначення безпеки – два для шифрування і одне для підпису. NIST також визначив п'ять категорій безпеки для класифікації обчислювальної складності атак, які порушують визначення безпеки (див. [5]).

NIST також згадував інші бажані властивості безпеки, такі як пряма безпечність, стійкість до атак бічними каналами та багатоключових атак, а також стійкість до неправильного використання. У деяких випадках NIST закликає представників внести незначні зміни, щоб забезпечити або вдосконалити ці додаткові бажані властивості безпеки (наприклад, додавання відкритої солі до шифртекстів, щоб уникнути багатоцільових атак на KEM).

Що стосується схем шифрування загального призначення і встановлення ключів, то у Call for Proposals [5] запрошувалися «семантично безпечні» схеми щодо атаки на основі адаптивно вибраного шифртексту (еквівалентно безпеці IND-CCA2). Для одноразових випадків використання NIST також приймав алгоритми, що забезпечують семантичну безпеку щодо атаки на основі вибраного відкритого тексту (безпека IND-CPA). IND-CCA2 безпека не потрібна в строго одноразових випадках використання, і спроба задовольнити більш суворі вимоги IND-CCA2 безпеки може спричинити за собою значні втрати продуктивності для деяких схем. Схеми цифрового підпису повинні були забезпечити екзистенційно непідробні підписи стосовно атаки на основі адаптивно вибраного повідомлення (EUF-CMA безпека). Автори заохочувалися, але не були зобов'язані надавати докази безпеки у відповідних моделях.

П'ять категорій безпеки, визначені у [5], були засновані на обчислювальних ресурсах, необхідних для виконання певних атак методом перебору проти існуючих стандартів NIST для AES і SHA в різних моделях вартості обчислень, як класичних, так і квантових.

1.2. Порівняльний аналіз кандидатів 3-го раунду

Що стосується вартості та продуктивності, то початковий запит пропозицій [5] визначав вартість як другий за важливістю критерій при оцінці алгоритмів-кандидатів. Вартість включає в себе обчислювальну ефективність генерації ключа і операцій з відкритим і особистим ключем, витрати на передачу відкритих ключів і підписів або шифртекстів, а також витрати на реалізацію в термінах RAM (оперативної пам'яті) або підрахунку гейтів.

При порівнянні загальної ефективності алгоритмів були розглянуті як обчислювальні витрати, так і витрати на передачу даних. Для використання загального призначення оцінка загальної ефективності розглядалася як витрати на передачу відкритого ключа на додаток до підпису або шифртексту під час кожної транзакції. Для KEM також враховували вартість генерації ключа, оскільки багато додатків використовують нову ключову пару KEM для кожної транзакції для забезпечення прямої секретності. Для алгоритмів підпису вартість генерації ключів вважалася менш важливою.

На рис. 1 показані числа обчислювальної продуктивності з [6] для процесора x86-64 з розширеннями AVX2 для Kyber, NTRU та Saber для категорій безпеки 1 та 3. На рис. 2 показані загальні витрати для Kyber, NTRU та Saber, коли додається вартість передачі даних. Рис. 2 було створено за допомогою орієнтовної вартості 2000 циклів/байт.

Інкапсуляція та декапсуляція є дуже швидкою з усіма трьома схемами. Незважаючи на те, що Saber має найнижчу загальну вартість завдяки меншим відкритим ключам та шифротекстам, різниця у вартості між Kyber та Saber не була достатньо великою, щоб вважатися значною.

Вартість генерації ключа для ntruhps2048677 або ntruhrss701 є приблизно в 11 разів більшою, ніж для KYBER512. Однак, як показано на рис. 2, загальна вартість використання цих схем, як правило, домінує у витратах передачі даних, і тому більша частина різниці в загальній вартості наборів параметрів NTRU порівняно з Kyber та Saber – через дещо більші відкриті ключі та шифротексти NTRU. Як результат, загальна вартість ntruhps2048677 менше, більш ніж на 30 %, ніж для KYBER512. Крім того, оскільки відкриті ключі та шифро-

тексти для наборів параметрів категорії 1 та 3 для всіх трьох схем, ймовірно, вписуються в один Інтернет-пакет, їхні числа продуктивності можуть вважатися порівнянними. Можна також зазначити, що, згідно з [6], вартість генерації ключів для ntruhps2048677 або ntruhrss701 порівнянна з витратами на генерацію ключа для криптографії на еліптичних кривих при кривій P-256, яка широко використовується для обміну тимчасовими ключами.

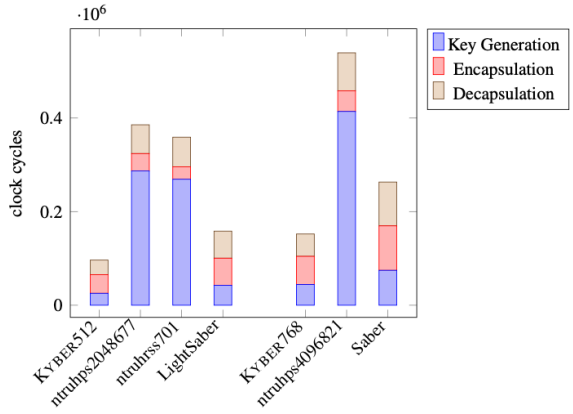

Рис. 1. Порівняльний аналіз KEM на процесорах x86-64 з розширеннями AVX2

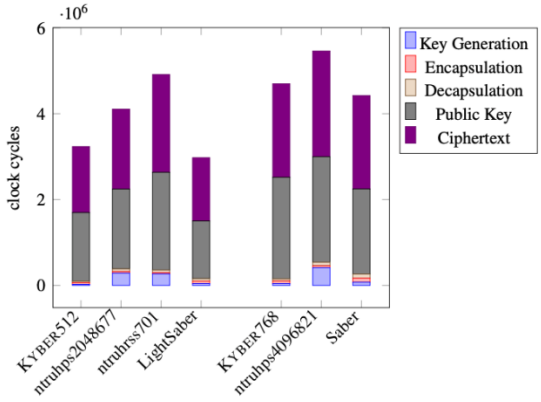

Рис. 2. Порівняльний аналіз KEM на процесорах x86-64
з розширеннями AVX2 з 2000 циклів/байт витратами на передачу

Звіт про стан 2-го раунду вибрав Dilithium і Falcon як фіналістів схеми підпису загального призначення та вказав на намір обрати щонайбільше одного з них [2]. Третій фіналіст, Rainbow, хоча й має привабливий профіль продуктивності для додатків, що вимагають малих підписів або швидкої перевірки, зазнав втрат безпеки, таким чином, показники ефективності Rainbow будуть далі опущені.

На рис. 3 показано показники обчислювальної продуктивності з [6] для процесора x86-64 з розширеннями AVX2 для Dilithium і Falcon. На відміну від рис.1, цей рисунок не включає вартість генерації ключів, оскільки ключі підпису не генеруються на основі кожної транзакції. На рис. 4 показані «загальні витрати» для Dilithium та Falcon з урахуванням вартості передачі відкритого ключа та підпису. При використанні процесора x86-64 генерація підпису за допомогою Dilithium відбувається трохи швидше, ніж за допомогою Falcon. Однак у загальних витратах на використання цих схем переважає передача даних, тому загальна вартість Falcon нижча через менший розмір відкритого ключа та підпису. Для більшості додатків, які використовують процесор x86-64 або подібний, показники продуктивності для Dilithium або Falcon мають бути прийнятними. Однак, на відміну від підписів Falcon, підписи Dilithium не можуть поміститися в один Інтернет-пакет, тому адаптація деяких додатків для використання Dilithium може виявитися складнішою, ніж їх адаптація для використання Falcon (наприклад, [7, 8]).

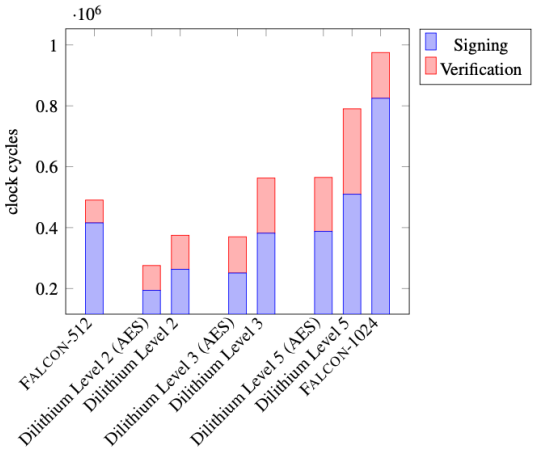

Рис. 3. Порівняльний аналіз підпису на процесорах x86-64
з розширеннями AVX2

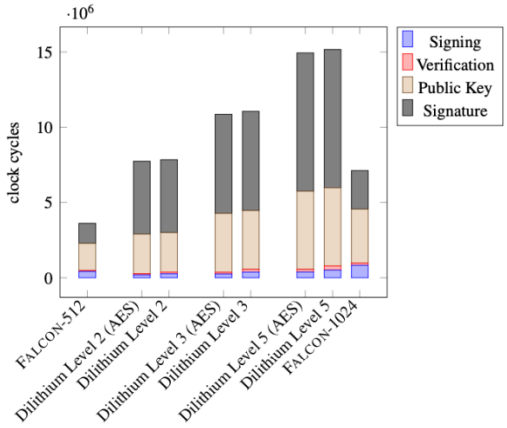

Рис. 4. Порівняльний аналіз підпису на процесорах x86-64
з розширеннями AVX2 з 2000 циклів/байт витратами на передачу

2. Попередня інформація щодо моделей та визначення безпеки

У цьому розділі представлені деякі складні обчислювальні проблеми, які є загальними для багатьох схем на основі кодів, багатовимірних схем або схем на решітках, досліджених у процесі стандартизації NIST PQC. Інші складні обчислювальні проблеми будуть згадані за потреби в описі окремих кандидатів у розд. 4.

2.1. На основі коду

Складність проблем загального та синдромного декодування (і деяких їх варіантів) є складовою аргументу безпеки для трьох KEM на основі коду, які проходять до 4-го раунду: BIKE, Classic McEliece і HQC. Усі три схеми забезпечують IND-CPA безпеку PKE з доказами, які залежать від однієї з цих двох обчислювальних проблем.

Нехай $C\_(n,k)$ двійковий лінійний код. Нехай $\mathbb{F}_2$ позначає скінченне поле двох елементів. Тоді набір із 2^k кодових слів C утворює k-вимірний підпростір $\mathbb{F}_2^n$. Для будь-якого вектора $v \in \mathbb{F}_2^m$, $m \in \mathbb{N}$ нехай $|v|$ позначатиме вагу Хеммінга v.

П р о б л е м а 1. (Проблема декодування синдрому (вирішення)). Дано $(n-k)\times n$ матрицю перевірки парності H для C, вектор $y \in \mathbb{F}_2^{n-k}$ і ціль $t \in \mathbb{N}$, визначити, чи існує $x \in \mathbb{F}_2^n$, що задовольняє $Hx^T = y$ і $|x| \le t$.

П р о б л е м а 2. (Проблема пошуку кодового слова (вирішення)). Дано $(n-k)\times n$ матрицю перевірки парності H для C і ціль $w\in\mathbb{N}$, визначити, чи існує $x\in\mathbb{F}_2^n$, який задовольняє $Hx^T=0$ і $|x|=w$.

Для загального двійкового лінійного коду C Berlekamp, McEliece та van Tilborg показали, що ці дві проблеми є NP-повними [9]. Це не гарантує, що будь-який даний криптографічний екземпляр проблеми є складним.

Найефективніші відомі атаки проти KEM на основі коду базуються на декодуванні набору інформації (ISD). Цей підхід ігнорує структуру двійкового коду та прагне відновити вектор помилки на основі його низької ваги Хеммінга. Ці методи виникли з алгоритму Прангe в 1962 році [10] і з тих пір зазнали низки вдосконалень. Також вивчалися квантові версії алгоритмів ISD [11 – 14]. Ці результати представляють загальне прискорення класичних алгоритмів ISD на основі Гровера та вказують на те, що ISD можна прискорити майже так само, як і пошук грубою силою.

2.2. На основі багатовимірних перетворень

Аргументи безпеки для двох багатовимірних схем підпису, GeMSS і Rainbow, залежать від складності проблеми *MQ* і проблеми MinRank.

П р о б л е м а 3. (Багатовимірна квадратична (*MQ*) поліноміальна проблема). Дано скінченне поле $\mathbb{F}$ і систему з m квадратичних поліномів з n змінними x_i:

$$f_k(x_1,\ldots,x_n)=\sum_{1\le i\le j\le n}a_{ij}^{(k)}x_ix_j+\sum_{1\le i\le n}b_i^{(k)}x_i+c^{(k)}=0, \tag{1}$$

для k від 1 до m, де $a_{ij}^{(k)}$, $b_i^{(k)}$, $c^{(k)}$ усі в $\mathbb{F}$, визначити, чи існує розв'язок у $\mathbb{F}^n$.

П р о б л е м а 4. (Проблема MinRank (вирішення)). Дано скінченне поле $\mathbb{F}$, k матриць M_i розміром $m\times n$ із записами в $\mathbb{F}$ та обмеження рангу r, визначити, чи існують значення $c_i\in\mathbb{F}$, які задовольняють наступне рівняння:

$$rank\left(\sum_{i=1}^{k}c_iM_i\right)\le r. \tag{2}$$

Проблема *MQ* була NP-складною в усіх полях [15]. У [16] показано, що проблема MinRank є NP-складною. Важливо відзначити, що коли цільовий ранг r фіксований, проблема MinRank має поліноміальну складність; таким чином, багатовимірні криптосистеми зазвичай вимагають великого значення r для будь-якого пов'язаного екземпляра MinRank. Відомо, що жодна проблема не є складною в середньому випадку, а також NP-складність не означає, що випадки, які виникають із криптографічних схем, нерозв'язні.

Найефективніші відомі загальні атаки на проблему *MQ* включають алгоритми базису Гробнера, такі як F4/F5, див. [17, 18], і алгоритми лінеаризації, такі як XL, див. [19]. Найефективніші атаки для MinRank відрізняються залежно від розміру та кількості матриць і цільового рангу. Основні методи включають комбінаторні методи пошуку, вперше введені в [20], і метод опорних міноpів, див. [21].

2.3. На основі алгебраїчних решіток

7 із 15 кандидатів 3-го раунду є криптосистемами на основі решітки. Ці криптосистеми пов'язані з великою кількістю академічних досліджень, які наголошують на (асимптотичній) доказовій безпеці, заснованій на найгіршому сценарії складності проблем решітки. Ранньою віхою в цьому напрямку досліджень стала стаття 1996 року Ajtai [22], яка визначила проблему короткого цілого розв'язку (SIS) і пов'язала її середню складність із найгіршою складніс-

тю пошуку коротких векторів у кожній цілочисельній решітці, даючи односторонні функції на основі решітки та односторонні функції з секретом на основі решітки.

Нижче коротко описано різні базові проблеми безпеки для кожної з цих систем:

П р о б л е м а 5. (Проблема короткого цілого розв'язку ($SIS_{n,m,q,\beta}$)). Нехай n, m, q – додатні цілі числа, і нехай β є позитивним дійсним числом. Дано матрицю $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, вибрану рівномірно навмання, необхідно знайти ненульовий цілий вектор $\mathbf{z} \in \mathbb{Z}^m$ з евклідовою нормою $\|\mathbf{z}\| \le \beta$, такий що $\mathbf{Az} = \mathbf{0} \in \mathbb{Z}_q^n$.

П р о б л е м а 6. (Проблема пошуку – $NTRU_{R,q,\mathcal{D},\gamma}$). Нехай q – додатне ціле число, γ – додатне дійсне число, а R – кільце форми $R = \mathbb{Z}_q[x]/\Phi$ (де Φ – монічний поліном). Дано елемент $h \in R$, взятий з деякого розподілу $\mathcal{D}$, такий, що існує ненульовий $(f, g) \in R^2$, який задовольняє $h \cdot f = g \bmod q$ і має малі евклідові норми $\|f\|$, $\|g\| \le \sqrt{q}/\gamma$, необхідно знайти таку пару (f, g).

Наступні кілька проблем – це всі типи проблем з навчанням з помилками (LWE). Для вектору $\mathbf{s} \in \mathbb{Z}_q^n$ і розподілу помилок χ необхідно визначити розподіл $A_{\mathbf{s},\chi}$ навчання з помилками (LWE) над $\mathbb{Z}_q^n \times \mathbb{Z}_q$, вибравши $\mathbf{a} \in \mathbb{Z}_q^n$ рівномірно навмання, вибравши $e \leftarrow \chi$ над $\mathbb{Z}$ і вивівши пару $(\mathbf{a}, b)$ де $b = \langle \mathbf{s}, \mathbf{a} \rangle + e \bmod q$.

П р о б л е м а 7. (Проблема пошуку – $LWE_{n,m,q,\mathcal{B},\chi}$). Нехай $\mathbf{s} \in \mathbb{Z}_q^n$ вибрано з деякого розподілу $\mathcal{B}$. Дано m вибірок $(\mathbf{a}_1, b_1), \ldots, (\mathbf{a}_m, b_m) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, що взяті незалежно випадковим чином із розподілу $A_{\mathbf{s},\chi}$, необхідно знайти $\mathbf{s}$.

П р о б л е м а 8. (Проблема прийняття рішень – $LWE_{n,m,q,\mathcal{B},\chi}$). Нехай $\mathbf{s} \in \mathbb{Z}_q^n$ вибрано з деякого розподілу $\mathcal{B}$. Не знаючи $\mathbf{s}$, дано m вибірок $(\mathbf{a}_1, b_1), \ldots, (\mathbf{a}_m, b_m) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, розрізнити наступні два випадки: (i) вибірки беруться незалежно від розподілу $A_{\mathbf{s},\chi}$, або (ii) вибірки беруться незалежно від рівномірного розподілу над $\mathbb{Z}_q^n \times \mathbb{Z}_q$.

Далі визначаємо деякі алгебраїчно структуровані проблеми SIS/LWE. Як правило, у цих алгебраїчно структурованих варіантах кільце R вважається поліноміальним кільцем ступеня n у формі $R = R_q = \mathbb{Z}_q[X]/(f(X))$ для деякого натурального числа q. Варіанти $f(X)$, які розглядаються в третьому раунді, мають вигляд $f(X) = X^{2d} + 1$, як у KYBER, Saber, Dilithium і FALCON. Окремо $f(X) = X^n - 1$ і $f(X) = X^{n-1} + X^{n-2} + \ldots + X + 1$ використовуються NTRU, а $f(X) = X^p - X - 1$ для простого числа p вибирається NTRU LPrime і sNTRU Prime. У третьому раунді використання алгебраїчних-SIS/LWE здебільшого набуло формулювання на основі модулів, як показано нижче.

П р о б л е м а 9. (Задача Module – $SIS_{R,m,k,q,\beta}$). Дано $\mathbf{a}_1, \ldots, \mathbf{a}_m \in R_q^k$ векторів поліномів $\mathbf{a}_m \in R_q^k$, вибраних рівномірно навмання, розглянемо їх як рядки матриці $\mathbf{A} \in R_q^{m \times k}$. Потім необхідно знайти ненульовий поліноміальний вектор $\mathbf{z} \in R_q^k$ з нормою $\|\mathbf{z}\| \le \beta$ так, що $\mathbf{Az} = 0$.

П р о б л е м а 10. (Проблема прийняття рішення – $LWE_{R,m,q,\mathcal{B},\chi}$). Нехай $\mathbf{s} \in R_q^k$ вибрано з деякого розподілу $\mathcal{B}$. При невідомому $\mathbf{s}$ дано m вибірок $(\mathbf{a}_1, b_1), \ldots, (\mathbf{a}_m, b_m) \in R_q^n \times R_q$, ро-

зрізнити наступні два випадки: (i) кожна вибірка складається незалежно від розподілу $A_{R,\mathbf{s},\chi}$ (аналог розподілу LWE $A_{\mathbf{s},\chi}$, але над R_q), або (ii) кожна вибірка складається незалежно від рівномірного розподілу над $R_q^k \times R_q$.

Нарешті, представляємо сімейство проблем навчання з округленням (LWR). Різниця між LWE і LWR полягає в тому, що вибірки формуються як округлені внутрішні продукти, а не незалежно від вибірки розподілу помилок χ. Тобто, зразки LWR приймають форму $(\mathbf{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, де $b_i = \lfloor \langle \mathbf{s}, \mathbf{a}_i \rangle \rceil_p$, а $\lfloor \cdot \rceil_p : \mathbb{Z}_q \to \mathbb{Z}_p$ (для $p < q$) є модульною функцією округлення, визначеною як $\lfloor x + q\mathbb{Z} \rceil_p := \lfloor x \cdot (p/q) \rceil + p\mathbb{Z}$.

Оцінка вартості вирішення цих критичних проблем безпеки на примірниках решітки реального світу є дуже нетривіальною, оскільки передбачає вибір найкращого типу атаки та оптимізацію параметрів атаки, щоб знайти найкраще можливе рішення із заданою кількістю обчислювальних ресурсів. Теоретичні межі та комп'ютерне моделювання використовуються для того, щоб оцінити вартість вирішення надзвичайно великих випадків цих проблем. Останніми роками це було предметом інтенсивних досліджень, які призвели до надійних оцінок конкретної безпеки криптосистем на основі решітки.

2.4. Моделі безпеки IND-CPA, IND-CCA2 та EUF-CMA

У оригінальному CFP [5] NIST дав визначення безпеки, які слід було сприймати як твердження того, що NIST вважав відповідною моделлю атаки. NIST планував стандартизувати KEM, які дозволили б «семантично безпечне» шифрування або інкапсуляцію ключів для загального використання – зокрема, схему, яка забезпечує нерозрізнення зашифрованих текстів під адаптованою атакою зашифрованого тексту. Грубо кажучи, схема є безпечною в цьому визначенні, якщо жоден зловмисник не може розрізнити «шифрування виклику» двох повідомлень на свій вибір, незважаючи на те, що він має доступ оракула до шифрування та розшифрування (останнє не можна використовувати під час виклику). Ця властивість позначається як IND-CCA2 безпека у науковій літературі [23]. Також для позначення цієї властивості використовуються терміни IND-CCA або CCA безпека.

Майже всі кандидати KEM, представлені NIST, досягли цієї функції, спочатку вказавши схему шифрування з відкритим ключем IND-CPA. Схема шифрування IND-CPA забезпечує нерозрізнення зашифрованих текстів під час обраної атаки відкритого тексту; це те саме визначення, що й вище, за винятком того, що криптоаналітик не має доступу оракула до розшифрування. Потім були створені повні KEM IND-CCA2 шляхом поєднання схем шифрування IND-CPA з певним типом перетворення Фудзісакі – Окамото (FO).

Для схем підписів відповідним визначенням безпеки була екзистенційна непідроблюваність під адаптованою атакою на повідомлення. Грубо кажучи, у цьому визначенні криптоаналітик отримує доступ оракула до функції підпису та повинен створити дійсний підпис для повідомлення, яке раніше не було підписано оракулом. У науковій літературі ця властивість позначається EUF-CMA безпека [23].

На додаток до цих визначень безпеки існують додаткові властивості безпеки. Хоча такі властивості не є обов'язковими для подання, вони можуть бути бажаними.

3. Стандартизація постквантової криптографії

Під час 3-го раунду було отримано деякі криптоаналітичні результати, які мали значний вплив на вибір NIST. Атака на GeMSS [24] різко знизила його безпеку та підірвала впевненість NIST у його стійкості. Цей результат призвів до виключення GeMSS з розгляду для стандартизації NIST.

Алгоритм Rainbow також зазнав значних атак під час 3-го раунду [25, 26]. Перша атака на початку 3-го раунду спричинила втрату наборів параметрів від 20 до 55 біт безпеки в моделі RAM, причому набори параметрів з вищим рівнем безпеки втрачали більше бітів

безпеки. За цим слідувала більш серйозна атака наприкінці 3-го раунду, що призвело до відновлення особистого ключа для параметрів категорії безпеки 1 трохи більше, ніж за два дні обчислень на одному ноутбуці. Через брак впевненості в безпеці NIST не вибрав Rainbow для стандартизації.

NIST також вирішив вилучити FrodoKEM, NTRU Prime та Picnic з розгляду для стандартизації. FrodoKEM – це кандидат, заснований на решітці, якого було обрано як альтернативний варіант під час 2-го туру. FrodoKEM в основному вирізняється тим, що він не покладається на структуровані решітки (на відміну від фіналістів Kyber, NTRU та Saber). У той час як NIST має намір вибрати принаймні один додатковий KEM, не заснований на структурованих решітках, для стандартизації після 4-го раунду, три інші альтернативи KEM (BIKE, HQC і SIKE) краще підходять для цієї ролі, ніж FrodoKEM.

FrodoKEM загалом має гіршу продуктивність, ніж ці три, тому не розглядатиметься надалі для стандартизації. NTRU Prime також було висунуто як альтернативний варіант, оскільки він вважався менш перспективним порівняно з фіналістами. Під час 3-го раунду не було результатів, які б суттєво змінили цю точку зору. Оскільки NIST буде стандартизувати один із (на основі структурованих решіток) фіналістів KEM, NTRU Prime не було обрано для продовження процесу. Схожа ситуація була і з підписами. Picnic не було обрано, оскільки NIST вирішив стандартизувати Sphincs+. Picnic та Sphincs+ мають подібні профілі ефективності (невеликі відкриті ключі та великі підписи) і підходять для тих же випадків використання. Sphincs+ і Picnic мають кілька версій, що робить пряме порівняння витрат та ефективності більш складним. Однак у кожного з них є набагато більша вартість та набагато гірша продуктивність порівняно з Dilithium та Falcon, що робить ці критерії менш важливими. Безпека Picnic не краща, ніж у Sphincs+, і NIST вважає, що, хоча Sphincs+ є зрілою конструкцією, Picnic та пов'язані з ним схеми продовжуватимуть отримувати користь від майбутніх досліджень та вдосконалень.

Вибираючи між подібними алгоритмами KEM, вартість та ефективність були значними критеріями відбору. NIST розглядав результати тестування продуктивності, надані спільнотою [6, 27] на декількох платформах при визначенні ефективності обчислень.

Одним із важких виборів, з якими стикнувся NIST, було прийняття рішення між Kyber, NTRU та Saber. Усі троє були обрані фіналістами і були дуже порівнянні один з одним. NIST впевнений у безпеці, яку забезпечує кожен. Більшість додатків зможуть використовувати будь-яку з них без суттєвих штрафів на продуктивність. Як зазначається, на завершення 2-го раунду NIST мав намір стандартизувати лише один із цих фіналістів, оскільки всі троє базувалися на структурованих решітках. Проблеми, пов'язані з патентами, були фактором рішення NIST протягом 3-го раунду, оскільки NIST дізнався про різні сторонні патенти. Однією з відмінностей між Kyber, Saber та NTRU є конкретне припущення щодо безпеки, що кожен покладається на безпеку. NIST вважає проблему MLWE, від якої залежить Kyber, трохи переконливішою, ніж інші припущення, такі як MLWR або проблема NTRU. NIST також високо оцінив специфікацію команди Kyber, яка включала ретельний і детальний аналіз безпеки. Що стосується продуктивності, то Kyber був майже найкращим (якщо не найкращим) у більшості тестів.

Решту обраних кандидатів KEM (BIKE, Classic McEliece, HQC, SIKE) продовжуватимуть оцінювати у 4-му раунді. І BIKE, і HQC засновані на структурованих кодах і будуть придатними як KEM загального призначення, що не ґрунтується на решітках. NIST може вибрати максимум одного з цих двох кандидатів для стандартизації по завершенню 4-го раунду. SIKE залишається привабливим кандидатом для стандартизації через його невеликі розміри ключа та шифротексту. NIST сподівається, що подальше вивчення SIKE триватиме протягом 4-го раунду. Classic McEliece був фіналістом, але наразі не стандартизується NIST. Хоча він вважається захищеним, NIST ще не передбачає, що він буде широко використовуватись через великий розмір відкритого ключа. Таким чином, ще немає терміновості для стандартизації Classic McEliece.

У [2] NIST вказав на намір вибрати щонайменше одного з Dilithium та Falcon, оскільки обидва базуються на структурованих решітках і можуть використовуватися в більшості додатків. Зрештою, NIST вирішив вибрати обидві схеми для стандартизації. Генерація ключа та підпису для Falcon, схоже, потребує більшої кількості ресурсів (гейтів та RAM), ніж Dilithium, що може зробити Falcon непридатним для впровадження на обмежених пристроях, особливо у випадках, коли вимагається захист від атак бічними каналами. Крім того, NIST визнає, що простіша конструкція ключа та генерації підписів Dilithium допоможе забезпечити безпечні реалізації. З цих причин NIST вибрав Dilithium як основний алгоритм підпису, який він рекомендує для загального використання, і надасть пріоритет його стандартизації.

NIST розуміє, що деякі додатки не працюватимуть так, як вони були розроблені, якщо підпис та дані, що підписуються, не будуть вписуватися в один Інтернет-пакет. Для цих додатків складність реалізації генерації підпису Falcon може не викликати занепокоєння, але труднощі з модифікацією додатків для роботи з більшим розміром підпису Dilithium можуть створити бар'єр для переходу до постквантових схем підпису. З цієї причини NIST вирішив також стандартизувати Falcon. Враховуючи загальну кращу продуктивність Falcon, коли генерацію підписів не потрібно виконувати на обмежених пристроях, багато додатків можуть вважати за краще використовувати Falcon, ніж Dilithium, навіть у випадках, коли розмір підпису Dilithium не буде перешкодою для реалізації.

Для того щоб не покладатися повністю на безпеку решіток, NIST також стандартизує Sphincs+. Безпека алгоритму підпису Sphincs+ добре зрозуміла, хоча він набагато більший та повільніший, ніж алгоритми підпису на решітках.

Підводячи підсумок, NIST обрав чотири алгоритми з 3-го раунду для стандартизації та чотири алгоритми для просування до 4-го раунду для подальшої оцінки та вивчення (див. табл. 3 та 4 для списку цих алгоритмів).

Таблиця 3

Алгоритми, які слід стандартизувати

Шифрування на відкритому ключі/KEM	Цифрові підписи
Crystals–Kyber	Crystals-Dilithium
	Falcon
	Sphincs+

Таблиця 4

Кандидати, що переходять до четвертого раунду

Шифрування на відкритому ключі/KEM	Цифрові підписи
BIKE	
Classic McEliece	
HQC	

Висновки

1. Основними алгоритмами, рекомендованими NIST для більшості випадків використання, є Crystals-Kyber (встановлення ключа) і Crystals-Dilithium (цифрові підписи). Крім того, схеми підпису Falcon і Sphincs+ також будуть стандартизовані. Кандидати BIKE, Classic McEliece, HQC, SIKE перейшли для подальшого вивчення до 4-го раунда оцінювання.

2. NIST створить нові проєкти стандартів для цих алгоритмів, координуючи команди подання, щоб гарантувати, що стандарти узгоджуються зі специфікаціями. У рамках процесу розробки NIST шукатиме інформацію про те, які конкретні набори параметрів слід включити, зокрема для будь-якої категорії безпеки 1. Після завершення стандарти будуть опубліковані для громадського обговорення. Після завершення періоду коментарів NIST перегляне проєкти стандартів, якщо це необхідно, на основі отриманих відгуків. Потім відбудеться остаточний розгляд, затвердження та процес оприлюднення. NIST сподівається опублікувати готовий стандарт до 2024 року.

3. NIST продовжує розглядати різноманітність обчислювальних припущень щодо складності як важливу довгострокову мету безпеки для своїх стандартів. NIST стандартизує практично ефективні схеми різних сімей криптосистем, щоб зменшити ризик того, що єдиний прорив у криптоаналізі залишить світ без життєздатного стандарту як для встановлення ключів, так і для цифрових підписів. Тим не менш, NIST не відчуває необхідності встановлювати ці стандарти відразу, а скоріше надасть пріоритет тим схемам, які здаються найближчими до того, щоб бути готовими до стандартизації та широкого прийняття. NIST вважає, що ця стратегія врівноважує прагнення до різноманітності з необхідністю ретельно перевіряти всі стандарти, перш ніж вони будуть видані.

4. Четвертий раунд оцінювання та аналізу відбуватиметься подібно до попередніх раундів. Як і раніше, чотирьом алгоритмам-кандидатам буде дозволено вносити відносно незначні модифікації у свої матеріали, які повинні бути подані до NIST і повинні відповідати тим же вимогам, що визначені в [5]. Подальші відомості та інструкції будуть надані на форумі PQC. Після завершення 4-го раунду NIST може вирішити вибрати деяких із кандидатів 4-го раунду для стандартизації.

5. Незважаючи на те, що 3-й раунд завершується і NIST почне розробляти перші стандарти PQC, зусилля зі стандартизації в цій галузі триватимуть ще деякий час. Це не слід інтерпретувати як те, що користувачі повинні чекати, щоб прийняти постквантові алгоритми. NIST сподівається на швидке впровадження цих перших стандартизованих алгоритмів і видасть майбутні вказівки щодо переходу. Перехід, безсумнівно, матиме багато складнощів, і виникнуть проблеми для деяких випадків використання, таких як пристрої IoT або прозорість сертифікатів.

Список літератури:

1. Alagic G., Alperin-Sheriff J., et al. (2019) Status report on the first round of the NIST post-quantum cryptography standardization process (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8240. – Режим доступу: https://doi.org/10.6028/NIST.IR.8240.
2. Alagic G., Alperin-Sheriff J., et al. (2020) Status report on the second round of the NIST post-quantum cryptography standardization process (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8309. Режим доступу: https://doi.org/10.6028/NIST.IR.8309.
3. NIST PQC. [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.
4. Schank J. (2021) Category 5 NTRU parameters. [Електронний ресурс]. Режим доступу: https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/t1JCgzSS-uk/m/VXXQaJgFCQAJ.
5. National Institute of Standards and Technology (2016) Submission requirements and evaluation criteria for the post-quantum cryptography standardization process. Режим доступу: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.
6. Bernstein D., Lange T. (eds.), eBACS: ECRYPT Benchmarking of Cryptographic Systems – SUPERCOP (2020). [Електронний ресурс]. Режим доступу: https://bench.cr.yp.to/supercop.html.
7. Shulman H., Goodman J., et al. (2021) PANEL: PQC considerations for DNSSEC, Third PQC Standardization Conference. [Електронний ресурс]. Режим доступу: https://www.nist.gov/video/third-pqc-standardization-conference-session-v-applications.
8. Bindel N. (2021) Suitability of 3rd round signature candidates for vehicle-to-vehicle communication // Workshop Record of the Third PQC Standardization Conference. [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/Presentations/2021/suitability-of-3rd-round-signature-candidates-for.
9. Berlekamp E., McEliece R,, van Tilborg H. (1978) On the inherent intractability of certain coding problems (corresp.) // IEEE Transactions on Information Theory 24(3): 384-386. Режим доступу: https://doi.org/10.1109/TIT.1978.1055873.
10. Prange E. (1962) The use of information sets in decoding cyclic codes // IRE Transactions on Information Theory 8(5): 5-9. Режим доступу: https://doi.org/10.1109/TIT.1962.1057777.
11. Bernstein D. J. (2010) Grovervs. McEliece. Post-Quantum Cryptography, ed Kachigar G., Tillich J. P. (2017) Quantum information set decoding algorithms. Post-Quantum Cryptography, eds Lange T., Takagi T. (Springer International Publishing, Cham), pp. 69-89.
12. Kachigar G., Tillich J. P. (2017) Quantum information set decoding algorithms. Post-Quantum Cryptography, eds Lange T., Takagi T. (Springer International Publishing, Cham), pp. 69-89.

13. Kirshanova E. (2018) Improved quantum information set decoding. Post-Quantum Cryptography, eds Lange T., Steinwandt R. (Springer International Publishing, Cham), pp. 507-527.
14. Esser A., Ramos-Calderer S., et al. (2021) An optimized quantum implementation of ISD on scalable quantum resources, Cryptology ePrint Archive, Report 2021/1608. Режим доступу: https://ia.cr/2021/1608.
15. Patarin J., Goubin L. (1997) Trapdoor one-way permutations and multivariate polynominals // Proceedings of the First International Conference on Information and Communication Security ICICS'97 (Springer-Verlag, Berlin, Heidelberg), p. 356-368.
16. Buss J. F., Frandsen G. S., Shallit J. O. (1996) The computational complexity of some problems of linear algebra. BRICS Report Series 3(33). Режим доступу: https://doi.org/10.7146/brics.v3i33.20013.
17. Faugere J. C. (1999) A new efficient algorithm for computing Grobner bases (F_4). Journal of Pure and Applied Algebra 139(1): 61-88. Режим доступу: https://doi.org/https://doi.org/10.1016/S0022-4049(99)00005-5.
18. Faugere J. C. (2002) A new efficient algorithm for computing Grobner bases without reduction to zero (F_5) // Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation ISSAC'02 (Association for Computing Machinery, New York, NY, USA), p. 75-83. Режим доступу: https://doi.org/10.1145/780506.780516.
19. Courtois N., Klimov A., Patarin J,, Shamir A. (2000) Efficient algorithms for solving overdefined systems of multivariate polynomial equations. Advances in Cryptology – EUROCRYPT 2000, ed Preneel B. (Springer Berlin Heidelberg, Berlin, Heidel- berg), pp. 392-407.
20. Goubin L., Courtois N. T. (2000) Cryptanalysis of the TTM cryptosystem. Advances in Cryptology – ASIACRYPT 2000, ed Okamoto T. (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 44-57.
21. Bardet M., Bros M., et al. (2020) Improvements of algebraic attacks for solving the rank decoding and MinRank problems. Advances in Cryptology – ASIACRYPT 2020, eds Moriai S., Wang H. (Springer International Publishing, Cham), pp. 507-536.
22. Ajtai M. (1996) Generating hard instances of lattice problems (extended abstract). Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing STOC'96 (Association for Computing Machinery, New York, NY, USA), p. 99-108. Режим доступу: https://doi.org/10.1145/237814.237838.
23. Katz J., Lindell Y. (2020) Introduction to Modern Cryptography (Chapman & Hall/CRC), 3rd Ed.
24. Tao C., Petzoldt A., Ding J. (2020) Improved key recovery of the HFEv- signature scheme // Cryptology ePrint Archive, Report 2020/1424. Режим доступу: https://ia.cr/2020/1424.
25. Beullens W. (2021) Improved cryptanalysis of UOV and Rainbow. Advances in Cryptology – EUROCRYPT 2021, eds Canteaut A., Standaert F. X. (Springer International Publishing, Cham), pp. 348-373.
26. Beullens W. (2022) Breaking Rainbow takes a weekend on a laptop, Cryptology ePrint Archive, Report 2022/214. Режим доступу: https://ia.cr/2022/214.
27. pqm4: Post-quantum crypto library for the ARM Cortex-M4 (2020). [Електронний ресурс]. Режим доступу: https://github.com/mupq/pqm4.

Надійшла до редколегії 03.09.2022

Відомості про авторів:

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; науковий співробітник-консультант АТ «Інститут Інформаційних технологій»; Україна; e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1252-7606

Острянська Єлизавета Вадимівна – аналітик з систем захисту інформації, АТ «Інститут Інформаційних технологій», Україна; e-mail: antelizza@gmail.com

Горбенко Іван Дмитрович – д-р техн. наук, професор, Харківський національний університет імені В. Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, АТ "Інститут Інформаційних Технологій", головний конструктор, Україна; e-mail: gorbenkoi@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-4616-3449