УДК 004.056.55

Д. Новиков, В. Полторак

ТЕХНОЛОГІЇ ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ

Анотація: Об’єктом дослідження є сучасні квантовостійкі криптоалгоритми, які мають забезпечувати безпеку даних у комунікаційних каналах в умовах зростаючої загрози з боку квантових комп'ютерів, так як для них наразі не існує ефективних алгоритмів криптоаналізу, оскільки вони базуються на інших математичних проблемах ніж ті, що експлуатуються у поточний час. У статті зроблено огляд алгоритмів, які було подано на участь в процесі сертифікації від організації NIST, розподіллено за типами криптографічних схем, наведено відомості про те, на яких математичних задачах вони ґрунтуються, складність розв'язання цих задач, переваги та недоліки.

Метою роботи є порівняння постквантових криптографічних систем та їх аналіз. В роботі розглянуті та проаналізовані основні принципи застосування різних видів криптографії, яка є стійкою до атак з використанням як звичайних, так і квантових комп'ютерів та технологій. Оглянуто наступні криптографічні типи: криптографію на основі ґраток, мультиваріативну криптографію, криптографію на основі хеш-функцій, криптографію на основі кодів коригування помилок та криптографію на основі ізогенії; що дозволяє зробити висновок про те, який з підходів до криптографії є кращим для обрання в конкретній ситуації. Результатом є порівняльний аналіз алгоритмів за обраними критеріями та формування списку алгоритмів, які є прийнятними для використання у «пост квантову добу», коли звичайні алгоритми вже не зможуть забезпечувати конфіденційність, за умови відсутності специфічних вимог щодо їх роботи (таких як розмір відкритого та закритого ключів/швидкодія алгоритмів).

Ключові слова: криптографія, постквантові алгоритми, механізм інкапсуляції ключів, схема підпису.

Формулювання проблеми

Квантові алгоритми можуть зламати існуючі криптографічні алгоритми, які залежать від обчислювальної складності певних математичних задач. Наприклад, широко використовувана схема шифрування з відкритим ключем RSA спирається на складність розкладання великих цілих чисел на прості числа. Однак алгоритм Шора, квантовий алгоритм, може ефективно розкладати великі цілі числа і, потенційно, може зламати шифрування RSA [1]. При використанні достатньої кількості кубітів, алгоритм здатен знайти рішення за час, порівнянний з часом множення простих чисел.

Подібним чином, алгоритм Гровера, ще один квантовий алгоритм, може бути використаний для прискорення пошуку рішення в несортованій базі даних, що,

потенційно, може зламати криптографічні хеш-функції, такі як MD5, SHA-1, SHA-2 та SHA-3, які залежать від труднощів пошуку прообразу для даного хешу [2]. Наприклад, SHA-256, може бути скомпрометовано за допомогою алгоритму Гровера за 2^{128} операцій, що є можливим для потужного квантового комп'ютера.

Так само є алгоритми, які базуються на задачі дискретного логарифмування. Наприклад, алгоритм Ель-Гамаля може використовуватися для формування електронного підпису або шифрування даних. Він базується на складності обчислення дискретного логарифму, яка вважається складною для вирішення за прийнятний час. Проте і тут квантові алгоритми мають свій потенціал, наприклад, модифікація алгоритму Шора, яка пристосована для вирішення задачі дискретного логарифмування [3].

І хоча це все ще матиме реальне практичне значення у майбутньому (через недостатню обчислювальну потужність квантових комп'ютерів на теперішній час), вже зараз необхідно брати ці загрози до уваги під час проектування та розробки як нових систем, так і підтримки вже існуючих. Для вирішення цієї проблеми існує постквантова криптографія, яка стійка як для атак з використанням звичайних, так і квантових комп'ютерів.

Постквантові криптографічні системи

Квантові обчислення здатні вирішувати складні математичні проблеми, на яких базується велика кількість криптографічних алгоритмів. Для убезпечення комунікаційних систем від успішних квантових атак необхідно використовувати криптографічні системи, які є стійкими до таких атак, тобто квантово-стійкі. Ці системи використовують алгоритми, які ґрунтуються на математичних задачах, котрі, на відміну від класичних криптографічних методів, вважаються важкими для розв'язання як класичними, так і квантовими комп'ютерами.

Наразі існує декілька типів квантово-стійких алгоритмів, які можуть бути використані для розробки криптографічних систем [4]:

– Lattice-based cryptography – криптографія на основі ґраток;

– Multivariate Cryptography – мультиваріативна криптографія;

– Hash-based cryptography – криптографія на основі хеш-функцій;

– Code-based cryptography – криптографія на основі кодів коригування помилок;

– Isogeny-based cryptography – криптографія на основі ізогенії;

– Symmetric key cryptography – симетрична криптографія (за умовою використання ключа великого розміру стійка до квантових алгоритмів).

Критерії оцінки постквантових криптоалгоритмів і протоколів

Однією з відомих у світі організацій, що збирає пропозиції щодо постквантових криптосистем, акумулює коментарі та відомості про алгоритми, які є стійкими до атак з використанням як квантових, так і класичних комп’ютерів, виступає NIST у США (National Institute of Standards and Technology). Один із важливих проектів, які веде ця організація є підпроєкт PQC (Post-Quantum Cryptography). У межах проекту NIST проводить конкурси з аналізу раундів з відбору, дослідження та стандартизації квантовостійких алгоритмів. З метою вибору прийнятних криптосистем-кандидатів для стандартизації, NIST залучає і коментарі від громадськості в рамках процесу оцінки, планує і проводить кілька раундів оцінювання пропонованих алгоритмів. Криптографічна спільнота заохочується до оцінки зі свого боку, що створює неупередженість та підвищує кількість досліджень алгоритмів. NIST заохочує рецензентів продемонструвати практичні атаки на запропоновані алгоритми. На поточний час проведено три раунди відбору, наразі триває 4-й раунд. За рішенням NIST, у межах останнього, наразі завершеного, 3-го раунду, алгоритми позначатимуться як «Ф» - для фіналістів, та «АК» - для альтернативних кандидатів.

NIST визначає п’ять рівнів безпеки постквантових криптоалгоритмів наступним чином:

1. Алгоритм має бути настільки складно скомпрометувати, як і виконати пошук ключів у симетричного шифру з ключем довжиною 128 біти;
2. Має відповідати стійкості 256-бітної хеш-функції (наприклад, SHA256);
3. Має відповідати стійкості симетричного шифру з ключем довжиною 192 біти (наприклад, AES192);
4. Має відповідати стійкості 384-бітної хеш-функції (наприклад, SHA384);
5. Найвищий рівень, має забезпечувати захист еквівалентний до симетричного шифрування з ключем довжиною 256 бітів (наприклад, AES256).

Аналіз продуктивності квантово-стійких алгоритмів проводиться у рамках проекту Open Quantum Safe (OQS), який розробляє та прототипує такі алгоритми. Основна мета OQS — стандартизація постквантової криптографії NIST для механізму безпечної передачі ключа сеансу (KEM) і схем підпису.

У якості критеріїв оцінки постквантових алгоритмів були обрані широковідомі характеристики розміру ланцюга даних та продуктивності:

– Довжина відкритого/закритого ключів (байт) – необхідна для розуміння складності алгоритму, так як має прямий вплив (при ключі, довжиною n біт, в найгіршому випадку необхідно 2^n операцій для знаходження ключа). Також надає інформацію про те, яку кількість даних необхідно передати мережі (для відкритого ключа) та впливає на час, необхідний алгоритму для генерації пар ключів;

– Час генерації пари ключів (од/с) – визначає, скільки алгоритм здатен генерувати пар відкритого/закритого ключів за секунду часу. Критерій необхідний для розуміння частини швидкодії алгоритму;

– Перевірка підпису (од/с) – кількість підписів, яку алгоритм може перевірити за одну секунду. Цей критерій відображає частину загальної швидкості алгоритму схеми підпису;

– Підписування (од/с) – кількість операцій підписування, яку алгоритм може опрацювати за одну секунду. Цей критерій відображає частину загальної швидкості алгоритму схеми підпису;

– Encaps (од/с) – кількість ключів сеансу («K») та випадкового шифротексту («C»), які можуть бути отримані за допомогою відкритого ключа («PK») за секунду часу, використовуючи Encaps(PK) операцію. Критерій відображає частину загальної швидкодії KEM;

– Decaps (од/с) – кількість ключів сеансу («K»), які можуть бути отримані використовуючи шифротекст («C») та закритий ключ («SK») за допомогою Decap(SK, C) операції за секунду часу. Критерій відображає частину загальної швидкодії KEM.

Lattice-based cryptography

Криптографія на основі ґраток – це тип криптографічної схеми, що базується на математичній теорії ґраток, які є типом дискретної математичної структури, яка виникає в різних галузях математики, включаючи теорію чисел, алгебру та геометрію. Ґратка — це дискретний набір точок у n-вимірному просторі, які розташовані за регулярним шаблоном. Ці точки можна розглядати як сітку точок, яка нескінченно тягнеться в усіх напрямках.

Ґраткова криптографія заснована на обчислювальній складності ґратчастих задач, основою якої є задача найкоротшого вектора (SVP), яка вимагає знайти найкоротший ненульовий вектор у даній ґратці. Надано вхідну ґратку, представлену довільним базисом, і мета зловмисника полягає в тому, щоб знайти найкоротший вектор від початку координат, коли задано основу ґратки (нульовий вектор не працює як відповідь). Найвідоміші атаки на криптографію на основі ґраток покладаються на класичні алгоритми, які є неефективними та вимагають експоненціально великих ресурсів, а найвідоміший алгоритм має оцінку часу роботи $O(2n\,logn)$ для точного розв’язку SVP. Іншою важливою проблемою є проблема найближчого вектора (CVP), яка вимагає знайти точку ґратки, найближчу до даного цільового вектора і вирішується в найкращому алгоритмі за $O(2^{3.5n})$ [5].

Криптосистеми, засновані на ґратках, часто є алгоритмічно простими, ефективними та високо паралелізованими. Алгоритми, які використовуються в криптографії на основі ґраток, базуються на простих математичних операціях, таких як

множення матриць і модульна арифметика, які легко піддаються апаратній реалізації та оптимізації.

Потенційно квантово-безпечні алгоритми, засновані на ґратках:

CRYSTALS-KYBER («Ф») — KEM, безпека якого забезпечується складністю розв'язання задачі навчання з помилками на модульній ґратці (Module-LWE, або M-LWE [6]). Алгоритм обчислювально швидкий (здатен генерувати від 9 тисяч до 90 тисяч пар ключів за секунду в залежності від рівня безпеки алгоритму) і має невеликий відкритий ключ (від 800 до 1568 байтів – для відкритого ключа, від 1632 до 3168 байтів – для закритого). Він має різні параметри, відповідні до налаштувань рівнів безпеки NIST 1, 3 і 5;

NTRU («Ф») — заснований на складності розв'язання проблеми кільцевого навчання з помилками (Ring-LWE, або R-LWE [7]). Має ще коротший ключ, та співвідношення довжини відкрито/закритого ключа ~ 1.3;

SABER («Ф») — безпека алгоритму ґрунтується на складності вирішення проблеми модульного навчання з округленням (Module-LWR), є простим і ефективним алгоритмом [8]. Пропонує три рівні безпеки (LightSABER – відповідає 1-му рівню NIST, SABER – 3-му рівню, FireSABER – 5-му рівню);

FrodoKEM («АК») — KEM, який базується на алгебраїчно неструктурованій ґратці. Алгоритм менше обмежений параметрами, але має великий розмір ключа (відкритий ключ – від 9616 до 21520 байтів, приватний – від 19888 до 43088). Забезпечує три рівня безпеки (FrodoKEM-640 забезпечує 1й рівень NIST, FrodoKEM-976 – 3й рівень, та FrodoKEM-1344 – 5й рівень);

CRYSTALS-DILITHIUM («Ф») — базується на техніці «Fiat-Shamir with Aborts» Любашевського [9]. Має найменший відкритий ключ і розмір підпису серед будь-яких схем підпису на основі ґраток, яка використовує лише рівномірну вибірку, та показує гарну швидкодію (кількість цифрових підписів, які алгоритм може створювати за секунду, варіюються від 2 до 15 тисяч, та здатен перевірити від 3 до 45 тисяч підписів за секунду);

FALCON («Ф») — це схема підпису на основі ґратки. Безпека алгоритму базується на проблемі коротких інтегральних розв'язків (SIS) над ґратками NTRU, для якої в даний час не існує ефективного алгоритму [10].

Криптографічні алгоритми на основі ґраток здаються найбільш перспективними та квантовостійкими. Максимальна кількість алгоритмів, оголошених NIST у 3-му раунді, належить до сімейства криптографії на основі ґраток. Алгоритм CRYSTALS-KYBER також було оголошено переможцем в категорії KEM за результатами 2022 року, CRYSTALS-DILITHIUM та FALCON – в категорії цифрових підписів.

Multivariate Cryptography

Мультиваріативна криптографія (МС) — це тип криптографії з відкритим ключем, яка базується на складності розв’язування систем багатовимірних поліноміальних рівнянь над кінцевими полями. У деяких випадках ці поліноми можуть бути визначені як над основним, так і над полем розширення. Доведено, що розв’язування систем багатовимірних поліноміальних рівнянь є NP-трудоємною задачею. Однак МС також вразлива до алгебраїчних, диференціальних атак та атак на базис Грьобнера [11]. Як наслідок, МС не має широкого використання на практиці.

У МС відкритий ключ – це система рівнянь багатовимірного полінома, а закритий ключ – це знання коефіцієнтів цих поліномів. Щоб зашифрувати повідомлення, відправник перетворює відкритий текст на систему поліноміальних рівнянь і розв’язує їх за допомогою відкритого ключа. Щоб розшифрувати повідомлення, одержувач використовує свої знання закритого ключа, щоб розв’язати ту саму систему рівнянь.

Потенційні квантово-безпечні алгоритми на основі мультиваріативної криптографії:

Rainbow («Ф») — заснований на схемі підпису «UOV» (Unbalanced Oil and Vinegar), базується на тому факті, що розв’язування набору випадкових багатовимірних квадратичних систем є NP-трудоємною задачею. Може бути використано для цифрового підпису, а його параметри можна встановити для досягнення рівнів безпеки NIST 1, 3 і 5;

GeMSS («АК») — це схема підпису, що має дуже короткий приватний ключ (32 байти), базується на криптосистемі Hidden Field Equations (HFE) з використанням модифікаторів, наприклад HFEv- [12]. Алгоритм має середній/великий відкритий ключ і теоретично дуже швидкий процес перевірки.

Незважаючи на свої обмеження, МС було запропоновано як потенційний постквантовий криптоалгоритм через його стійкість до атак квантових комп’ютерів.

Hash-based cryptography

Криптографія на основі хешування — це тип постквантової криптографії, яка покладається на математичні властивості хеш-функцій для забезпечення безпеки. Основна ідея полягає у використанні односторонньої хеш-функції для створення дайджесту повідомлення або хеш-значення з вихідного повідомлення. Потім це хеш-значення використовується як цифровий підпис або ключ для шифрування та дешифрування.

Основна перевага криптографії на основі хешування полягає в тому, що це добре зрозуміла, вивчена і широко використовувана технологія, яка гарантує високу стійкість до квантових атак, що робить її кандидатом на довгострокову безпеку в постквантову еру (за умови використання достатньо довгого ключа).

Однак криптографія на основі хешування також має потенційні проблеми. По-перше, безпека хеш-функції може бути порушена, якщо зловмисники знайдуть колізії. По-друге, вимагає відносно великого розміру ключа для забезпечення безпеки (оскільки алгоритм Гровера можна використовувати для зламу хеш-функції за час $O(\sqrt{n})$ (де n – довжина ключа), коли звичайні алгоритмі мають експоненційну складність $O(2^{\frac{n}{2}})$, хоча і ефективний лише для коротких ключів), що може призвести до сповільнення часу обробки та збільшення вимог до пам’яті.

Підпис на основі хешу (HBS) це набір багатьох схем одноразового підпису, що використовує структуру даних дерева для ефективного об’єднання багатьох одноразових підписів. Щоб підписати повідомлення, HBS вибирає один із одноразових підписів зі своєї колекції та використовує його для підпису повідомлення (ніколи не повинен використовувати один і той самий одноразовий підпис двічі, інакше безпека буде порушена) [13].

Квантово-безпечні алгоритми на основі хешування:

SPHINCS+ («АК») — це схема підпису без збереження стану на основі хешу, спеціально спрямована на зменшення розміру підпису. Має співвідношення відкритого ключа до закритого 1: 2, має багато варіацій алгоритму і задовольняє рівням безпеки NIST 1, 3 і 5, пропонуючи три різні схеми підпису:

– SPHINCS+-SHA3 (з використанням хеш-функції SHAKE256);
– SPHINCS+-SHA2;
– SPHINCS+-Haraka.

Криптографія на основі хешування залишається багатообіцяючим методом для забезпечення безпечних цифрових підписів і автентифікації в різних програмах. Складність рішення та потенційні проблеми залежатимуть від конкретної реалізації та варіанту використання.

Code-based cryptography

Криптографія на основі кодів коригування помилок — покладається на складність задачі декодування лінійного коду з виправленням помилок, який, вибрано з певною структурою або в певному сімействі (наприклад, квазіциклічні коди або коди Гоппи [14]). Безпека базується на складності проблеми декодування, яка вимагає пошуку вектора помилки, який був введений під час передачі кодового слова. Вважається, що ця проблема складна з точки зору обчислень (складність рішення декодування залишається NP-трудоємною, проте точна складність є активною областю досліджень), що робить криптографію на основі коду перспективним кандидатом на постквантову криптографію.

Класичним представником даної системи вважається система McEliece — криптосистема з відкритим ключем на основі бінарного кода Гоппи. Classic McEliece

Згідно з ідеєю МакЕліса, відкритий ключ є продуктом коду Гоппи та лінійного перетворення. Щоб зашифрувати повідомлення, відправник повинен додати певну кількість випадкового «шуму», який можна видалити лише за допомогою коду Гоппи [15]. Відновити повідомлення, не знаючи, як врахувати відкритий ключ, для зловмисника є складною обчислювальною проблемою.

Одна з потенційних проблем криптографії на основі коду полягає в тому, що вона може бути вразливою до атак по бічному каналу, коли зловмисник може спостерігати за виконанням алгоритму шифрування або дешифрування та вилучати інформацію про секретний ключ [16]. Також слід зазначити, що криптографія на основі коду вимагає більшого розміру ключа. Це може призвести до довшого часу шифрування та дешифрування, а також може потребувати більше місця для зберігання. Крім того, криптографія на основі коду може бути дорогою з точки зору обчислень, оскільки операції кодування та декодування вимагають великих множень матриці, що може бути дорогим з точки зору обчислювальних ресурсів.

Квантово-безпечні алгоритми на основі кодів коригування помилок:

Classic McEliece («Ф») – KEM, що відповідає всім п’яти рівням безпеки NIST. Час обчислення алгоритму відносно швидкий, проте потребує використання дуже великого розміру відкритого ключа (від 260 до 1360 тисяч байтів);

BIKE («АК») — це механізм інкапсуляції ключів на квазициклічних кодах перевірки парності помірної щільності (QC-MDPC), які можуть бути декодовані за допомогою методів декодування з перевертанням бітів [17]. Має найкоротший відкритий ключ (від 1541 до 5122 байтів) та високу швидкість;

HQC («АК») — KEM на основі коду, має найкоротший відкритий ключ та співвідношення відкритого/закритого ключа майже 1 (закритий більше на кілька байтів). Алгоритм розроблений для досягнення 1, 3 і 5-го рівнів безпеки NIST;

Як і для будь-якого класу криптосистем, криптографія на основі коду є компромісом між безпекою та ефективністю. Загалом – є багатообіцяючою областю, але, як і інші системи, потребує подальших досліджень. На четвертий раунд NIST, де організація шукає альтернативи алгоритмам, заснованим на ґратках, наразі надійшло 4 заявки, 3 з яких відносяться до алгоритмів, заснованих на кодах, які були оглянуті вище.

Isogeny-based cryptography

Криптографія на основі ізогенії — відносно нова система, найвідоміший представник — протокол обміну ключами Supersingular Isogeny Diffie–Hellman (SIDH) [18]. Використовує відображення між еліптичними кривими для побудови криптосистем з відкритим ключем. Безпека базується на одній із небагатьох важких математичних задач, яка наразі протистоїть атакам квантових комп’ютерів — на так званих проблемах суперсингулярних ізогеній, або знаходженні відображення ізогенії

між двома суперсингулярними еліптичними кривими з однаковою кількістю точок [19]. Протоколи на основі ізогенії вимагають дуже маленького ключа порівняно з будь-яким іншим кандидатом пост-квантової криптографії (однак, все ще набагато більші, ніж для алгоритмів на звичайних еліптичних кривих), але продуктивність і придатність для більш просунутих криптографічних примітивів обмежені порівняно, наприклад, з системами на основі ґраток.

Однією з потенційних проблем є те, що це відносно нова та неперевірена криптосистема, а це означає, що можуть бути невиявлені вразливості або слабкі місця, якими можуть скористатися зловмисники. Крім того, хоча розміри ключів, необхідні для криптографії на основі ізогенії, невеликі, обчислювальна вартість генерації ключів все ще відносно висока, що може бути недоліком у деяких середовищах з обмеженими ресурсами.

Алгоритм на основі ізогенії зі списку кандидатів NIST:

SIKE («АК») — KEM на основі ізогенії, базується на псевдовипадкових блуканнях у суперсингулярних графах ізогенії. Має найменший розмір відкритого ключа (від 197 до 564 байтів для відкритого ключа, від 28 до 644 байтів – для закритого), але також найповільніший з оглянутих алгоритмів. Нещодавно був скомпрометований та вже не може бути рекомендованим до використання (алгоритм Magma порушує екземпляр SIKEp434, який націлений на 1-й рівень безпеки NIST, приблизно за одну годину на одному ядрі [20]). Був запропонований як кандидат на 4-й раунд NIST, проте через знаходження атаки з нотаткою, що алгоритм був скомпрометований, щоб остаточна версія пропозиції SIKE точно відображала поточний стан криптосистеми.

Загалом, криптосистеми на основі ізогенії демонструють великі перспективи для забезпечення безпечної та ефективної криптографії з відкритим ключем. А враховуючи що національний стандарт України для цифрових підписів ґрунтується на використанні еліптичних кривих (ДСТУ 4145-2002) [21], цей напрямок є дуже важливим та має перспективу для подальшого використання в Україні.

Порівняльний аналіз алгоритмів

За обраними критеріями оцінки, проведено порівняльний аналіз алгоритмів, з розподілом їх за алгоритмами механізму безпечної передачі ключа сеансу і на основі схеми підпису. Відомості у таблицях наведено відносно алгоритмів, які забезпечують найвищий доступний рівень безпеки NIST (якщо декілька модифікацій алгоритму забезпечують цей рівень захисту – обрано кращий). При порівнянні алгоритму 5го та нижчого рівня, слід розуміти, що чим вище рівень, тим вище складність обчислень. Для збору даних про поведінку алгоритмів та споживання пам'яті використовується хмарний сервіс Amazon, який працює на процесорі Intel Xeon Platinum 8259CL з тактовою частотою 2,50 ГГц:

Таблиця 1.

Порівняльні характеристики KEM-алгоритмів

Алгоритм і рівень безпеки NIST	**Відкритий ключ (байт)**	**Закритий ключ (байт)**	**Генерація пари ключів (од/с)**	**Encaps (од/с)**	**Decaps (од/с)**
CRYSTALS-KYBER (5)	1568	3168	71094	61995	96649.33
NTRU (5)	1230	1590	2437.33	47725.33	44142.33
SABER (5)	1312	3040	38432.1	30412.7	31734.6
FrodoKEM (5)	21520	43088	1025.22	773.33	795.07
Classic McEliece (5)	1047319	13908	2.28	19568	6900
BIKE (5)	5122	16494	559.48	4996.67	227.11
HQC (5)	7245	7258	5566	2982.67	1792.67
SIKE (5)	564	48	104.79	50.17	127.4

За результатом порівняння можна зробити висновок, що кращим кандидатом є CRYSTAL-KYBER, оскільки він має найкращу продуктивність та прийнятну довжину ключа. Також, якщо необхідно впровадити альтернативні алгоритми, можна рекомендувати використання алгоритмів SABER та NTRU, які демонструють гарні результати: SABER має гарну продуктивність, NTRU – найкращий розмір ключа (не беручи до уваги SIKE через компрометацію), середню продуктивність. Якщо розглядати алгоритми, які не базуються на ґратках, слід обрати HQC або BIKE. Алгоритм Classic McEliece демонструє середню продуктивність та має надзвичайно великі ключі (довжина публічного ключа більше одного мільйона байт, що створює додаткове навантаження на канал зв'язку та на час генерації пари ключів, проте не надає явної переваги, окрім захисту від атаки з використанням повного перебору ключів).

Таблиця 2.

Порівняльні характеристики алгоритмів на основі схеми підпису

Алгоритм і рівень безпеки NIST	**Відкритий ключ (байт)**	**Закритий ключ (байт)**	**Генерація пари ключів (од/с)**	**Перевірка підпису (од/с)**	**Підписування (од/с)**
CRYSTALS-DILITHIUM (5)	2592	4864	21586.33	21314.33	9008.67
FALCON (5)	1793	2305	42.09	8759.33	1542.82
Rainbow (5)	536136	1408736	0.18	24.48	23.82
GeMSS (5)	352180	32			
SPHINCS+ (5)	64	128	955.67	1815	44.22

 ISSN 1560-8956

У цій категорії кращим є CRYSTALS-DILITHIUM, алгоритм з прийнятною довжиною ключа, який демонструє найкращу продуктивність. У якості альтернативи може виступати FALCON – має коротший ключ, проте помітно гіршу продуктивність, та SPHINCS+ - має найкоротшу пару ключів та велику кількість реалізацій, проте й найповільніший (за операціями підписування/перевірки підпису) з трьох алгоритмів. GeMSS наразі не реалізовано у проекті OQS, тому точних даних щодо його продуктивності не існує.

Висновки

В статі проведено порівняльний аналіз криптографічних алгоритмів, які приймають участь у сертифікації від організації NIST. Ці алгоритми ґрунтуються на математичних задачах, які, на відміну від класичних криптографічних методів, вважаються важкими для розв'язання як класичними, так і квантовими комп'ютерами.

Використання пост-квантової криптографії стає більш актуальним через збільшення загрози зі сторони квантових комп'ютерів та досліджень у квантових обчисленнях. Для мінімізації ризику, який принесе впровадження та використання квантових систем вже зараз необхідно планувати перехід на квантовостійкі системи. Під час проектування та розробки найчастіше використовують криптографію на основі ґраток, на основі хешування або на основі кодів коригування помилок, проте конкретне рішення ґрунтується на вимогах до конкретної системи та має бути зроблене для кожного випадку окремо.

У загальному сенсі, при виборі механізму безпечного передавання ключа сеансу слід обирати CRYSTALS-KYBER, серед альтернативних кандидатів присутні SABER або NTRU (алгоритми на основі ґраток), HQC або BIKE (на основі кодів коригування помилок). Для електронного цифрового підпису наразі немає широкого вибору, кращим є CRYSTALS-DILITHIUM, а прийнятною альтернативою є або FALCON (на основі ґраток) або SPHINCS+ (на основі хешування).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Journal on Computing. 1997. № 26 (5). URL: https://doi.org/10.48550/arXiv.quant-ph/9508027;

2. Preston R. Applying Grover's Algorithm to Hash Functions: A Software Perspective // IEEE Transactions on Quantum Engineering. 2022. № 3. URL: https://doi.org/10.1109/TQE.2022.3233526;

3. Proos J., Zalka C. Shor's discrete logarithm quantum algorithm for elliptic curves // Quantum Information and Computation. 2003. № 3 (4). С.317-344 URL: https://doi.org/10.26421/QIC3.4-3;

4. Report on Post-Quantum Cryptography / L. Chen та ін. // NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD. 2016. URL: https://doi.org/10.6028/NIST.IR.8105;

5. Voulgaris P. Algorithms for the closest and shortest vector problems on general lattices // UC San Diego Electronic Theses and Dissertations. 2011. URL: https://escholarship.org/uc/item/4zt7x45z;

6. Towards Classical Hardness of Module-LWE: The Linear Rank Case / K. Boudgoust та ін. // Advances in Cryptology – ASIACRYPT 2020 / South Korea. Daejeon: Springer, Cham, 2020. С.289-317. URL: https://doi.org/10.1007/978-3-030-64834-3_10;

7. Lyubashevsky, V., Peikert, C., & Regev, O. (2013). A Toolkit for Ring-LWE Cryptography. Advances in Cryptology – EUROCRYPT 2013, (35-54). Athens: Springer Berlin, Heidelberg. Retrieved from https://doi.org/10.1007/978-3-642-38348-9_3;

8. Saber: Module-LWR Based Key Exchange, CPA-Secure Encryption and CCA-Secure KEM / J. D’Anvers та ін. // Progress in Cryptology – AFRICACRYPT 2018 / Africa, Morocco. Marrakesh: Springer, Cham, 2018. С.282-305. URL: https://doi.org/10.1007/978-3-319-89339-6_16;

9. Lyubashevsky V. Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures // Advances in Cryptology - ASIACRYPT 2009 / Japan. Tokyo: Springer, Berlin, Heidelberg, 2009. С.598-616. URL: https://doi.org/10.1007/978-3-642-10366-7_35;

10. Improved Reduction Between SIS Problems Over Structured Lattices / Z. Koo та ін. // IEEE. 2021. № 9. URL: https://doi.org/10.1109/ACCESS.2021.3128139;

11. Hashimoto Y., Takagi T., Sakurai K. General Fault Attacks on Multivariate Public Key Cryptosystems // Post-Quantum Cryptography / Taiwan. Taipei: Springer, Berlin, Heidelberg, 2011. С.1-18. URL: https://doi.org/10.1007/978-3-642-25405-5_1;

12. Wolf C., Preneel B. Asymmetric Cryptography: Hidden Field Equations // ECCOMAS 2004 / Finland. Jyväskylä, 2004. С.24-28. URL: https://eprint.iacr.org/2004/072;

13. Practical Fault Injection Attacks on SPHINCS / A. Genêt та ін. // Cryptology ePrint Archive. 2018. С.1-18 URL: https://eprint.iacr.org/2018/674;

14. Barreto P., Misoczki R., Lindner R. Decoding Square-Free Goppa Codes Over F-p // IEEE Transactions on Information Theory. 2013. № 59 (10). С.6851-6858 URL: http://doi.org/10.1109/TIT.2013.2270272;

15. Post-Quantum and Code-Based Cryptography—Some Prospective Research Directions / C. Balamurugan та ін. // Cryptography. 2021. № 5(4) (38). URL: https://doi.org/10.3390/cryptography5040038;

16. Novel Side-Channel Attacks on Quasi-Cyclic Code-Based Cryptography / B. Sim та ін. // IACR Transactions on Cryptographic Hardware and Embedded Systems. 2019. № 4. С.180-212 URL: https://doi.org/10.13154/tches.v2019.i4.180-212;

17. BIKE: Bit Flipping Key Encapsulation / N. Aragon та ін. // HAL open science. 2017. URL: https://hal.science/hal-01671903;

18. Jao D., De Feo L. Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies // Post-Quantum Cryptography / Taiwan. Taipei: Springer, Berlin, Heidelberg, 2011. С.19-34. URL: https://doi.org/10.1007/978-3-642-25405-5_2;

19. Galbraith S., Vercauteren F. Computational problems in supersingular elliptic curve isogenies // Quantum Inf Process 17. 2018. № 265. URL: https://doi.org/10.1007/s11128-018-2023-6;

20. Castryck W., Decru T. An efficient key recovery attack on SIDH // Cryptology ePrint Archive. 2022. URL: https://ia.cr/2022/975;

21. ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння [Чинний від 2003-07-01]. Вид. офіц. Київ : Державний комітет України з питань технічного регулювання та споживчої політики, 2002. 36 с.