DOI 10.31891/2307-5732-2024-333-2-56
УДК 004.056.5

ЛАВРИК ІВАН
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут
https://orcid.org/0000-0002-3433-9083
e-mail: ivan.lavryk@viti.edu.ua

ДОСЛІДЖЕННЯ АЛГОРИТМІВ ПОСТКВАНТОВОГО ЦИФРОВОГО ПІДПИСУ

Стрімкий розвиток квантових обчислень зумовлює необхідність розробки криптографічних алгоритмів стійких до квантового криптоаналізу. В зв'язку з цим Національний інститут стандартів та технологій (NIST) проводить конкурс з метою стандартизації алгоритмів в постквантовий період, серед них алгритми для цифрових підписів такі як: Crystals-Dilithium, Falcon та Sphincs+. З метою визначення шляхів розвитку і способів вдосконалення існуючих методів криптографічного захисту та електронного цифрового підпису (ЕЦП) виникла актуальна задача оцінки ефективності існуючих алгоритмів ЕЦП. У роботі було проведено порівняльну оцінку ефективності алгоритмів ЕЦП за ключовими показниками. За результатами досліжень було визначено недоліки та переваги кожного алгоритму, з урахуванням важливості контекстно-специфічного використання. Було встановлено, що Dilithium має найменше навантаження на обчислювальні ресурси системи, Falcon виділяється швидкістю верифікації підписів, а Sphincs+ забезпечує необхідний рівень стійкості. Можливості існуючих алгоритмів криптоперетворень на основі еліптичних кривих не забезпечують зростаючої потреби у стійкості алгоритмів автентифікації до квантового криптоаналізу, а використання сучасних кандидатів на стандарт постквантової криптографії не дозволяє в короткостроковій перспективі здійснити перехід на використання нових криптоалгоритмів в інформаційних системах. Також в роботі зазначено про неможливість одночасного переходу до потенційно стійких до квантового криптоаналізу алгоритмів в існуючих інформаційних системах.

Напрямком подальших досліджень є розробка нових криптоалгоритмів і методів, що забезпечать цілісність та конфіденційність інформації під час її передачі незахищеними каналами в перехідний період до широкого використання та впровадження стандартів постквантової криптографії.

Ключові слова: асиметричні криптосистеми, цифровий підпис, NIST PQC, еліптична крива, автентифікація.

LAVRYK IVAN
Kruty Heroes Military Institute of Telecommunications and Information Technologies

RESEARCH OF POST-QUANTUM DIGITAL SIGNATURE ALGORITHMS

The continuous development of quantum computing requires the development of cryptographic algorithms resistant to quantum cryptanalysis. Therefore, the National Institute of Standards and Technology (NIST) is holding a competition to standardize algorithms in the post-quantum period, including Crystals-Dilithium, Falcon, and Sphincs+ for digital signatures. In order to determine the ways of development and ways to improve the existing methods of cryptographic protection and electronic digital signature (EDS), an urgent task arose to assess the effectiveness (stability and computational complexity) of existing EDS algorithms. In this paper, a comparative evaluation of EDS algorithms was carried out by key indicators. Research results show the disadvantages and advantages of each algorithm, taking into account the importance of context-specific use. The conclusions indicate that Dilithium has the lowest load on the system's computing resources, Falcon stands out for its signature verification speed, and Sphincs+ provides reliable security. The capabilities of existing cryptographic transformation algorithms based on elliptic curves do not meet the growing need of authentication algorithms resistance to quantum cryptanalysis, and the use of modern candidates for the post-quantum cryptography standard does not allow for a short-term transition to the usage of new cryptographic algorithms in information systems. The paper also points out the impossibility of simultaneous transition to potentially quantum cryptanalysis-resistant algorithms in existing information systems.

The direction of further research is the development of new cryptoalgorithms and methods that will ensure the integrity and confidentiality of information during its transmission over unprotected channels in the transition period to the widespread use and implementation of post-quantum cryptography standards.

Keywords: asymmetric cryptosystems, digital signature, NIST PQC, elliptic curve, authentication.

Постановка проблеми

Потенціал використання квантових комп'ютерів для здійснення криптоаналізу постійно зростає завдяки дослідженню алгоритмів, специфічних для квантових обчислень [1,2] та постійному зростанню обчислювальних спроможностей квантових комп'ютерів. Хронологія розвитку квантових обчислень, наведена в таблиці 1 показує, що існуючі спроможності квантових обчислень вже досягли результату в 1121 кубіт.

Таким чином, класичні криптографічні методи стикаються з можливими загрозами. Криптосистеми з відкритим ключем, які лежать в основі безпечного обміну інформацією, можуть стати застарілими, якщо будуть побудовані достатньо потужні квантові комп'ютери [3]. Проблема не є гіпотетичною; дослідники все більше схиляються до розгляду квантових обчислень як інженерного виклику, а не як нерозв'язної теоретичної проблеми. Прогнози вказують, що протягом декількох десятиліть квантові комп'ютери, здатні зламати сучасні стандартизовані криптоалгоритми з відкритим ключем, стануть реальністю.

Дата появи квантових комп'ютерів, здатних зламати сучасні криптографічні системи, все ще невизначена. У зв'язку з цим довгий час, необхідний для впровадження та стандартизації нових криптографічних алгоритмів, вимагає негайних дій. Зокрема, існуючі криптосистеми мають бути адаптовані або замінені, щоб протистояти як класичному криптоаналізу, так і атакам з використанням квантових комп'ютерів квантових комп'ютерів. Отже, невідкладність розробки та впровадження постквантових (або квантово-стійких) криптографічних алгоритмів є очевидною [3].

Табл.1

Хронологія розвитку квантових обчислень

Рік	Подія
1982	Річард Фейнман висунув ідею квантових обчислень.
1985	Девід Дойч розробив концепцію квантової машини Тьюрінга.
1994	Пітер Шор запропонував квантовий алгоритм факторизації, який був здатен значно швидше розкладати числа на прості множники порівняно з класичними алгоритмами.
1996	Лов Гровер запропонував квантовий алгоритм пошуку.
2001	IBM та Лос-Аламоська національна лабораторія вперше реалізували алгоритм Шора.
2007	D-Wave Systems анонсувала продаж першого комерційного квантового комп'ютера.
2011	IBM запустила проект «IBM Q» з метою розвитку комерційно доступних квантових комп'ютерів.
2016	IBM створила платформу IBM Quantum Experience, яка дозволяла користувачам експериментувати з квантовими алгоритмами в хмарі.
2019	Google оголосила про досягнення квантової переваги.
2020	Дослідники з Китаю заявили про досягнення квантової переваги за допомогою фотонної системи.
2021	IBM представила квантовий процесор «Eagle» з 127 кубітами.
2022	IBM представила квантовий процесор «Osprey» з 433 кубітами.
2023	IBM представила квантовий процесор «Condor» з 1121 кубітами.

NIST у 2016 році розпочав процес розробки та стандартизації одного або декількох криптоалгоритмів з відкритим ключем для вдосконалення існуючого стандарту цифрових підписів FIPS 186-4 (DSS) [4] NIST PQC. Як результат було проведено кілька раундів стандартизаційних процесів [5–7]. Третій раунд, проведений у липні 2022 року, завершив відбір постквантових алгоритмів шифрування з відкритим ключем та цифрових підписів (табл.2) [8].

Таблиця 2

Фіналісти третього раунду NIST PQC

Алгоритм інкапсуляції ключів	Цифровий підпис
CRYSTALS-KYBER	CRYSTALS-Dilithium
	FALCON
	SPHINCS+

Загалом, ці раунди мають на меті визначення алгоритму здатного захистити конфіденційну інформацію у передбачуваному майбутньому, включаючи постквантовий період. Crystals-Dilithium і Falcon ґрунтуються на проблемах з теорії та практики алгебраїчних решіток з особливостями, що залежать від контексту застосування. Алгоритм Dilithium легше впровадити, тоді як Falcon забезпечує коротші підписи [9]. Sphincs+ повільніший та більший за розміром, оскільки базується на іншому математичному підході, а саме на хеш-функціях.

Актульним напрямком досліджень є розробка методів генерації та верифікації цифрового підпису на основі перетворень над точками ізогенії еліптичної кривої. Адже розробка принципово нових криптоалгоритмів викликає потребу в додаткових витратах на впровадження в інформаційні системи, реалізацію нових програмно-апаратних засобів та систем. Тому актуальною науково-технічною задачею є вдосконалення існуючих криптоперетворень з підвищеними показниками стійкості до квантового криптоаналізу.

Метою роботи є: дослідження параметрів та характеристик алгоритмів постквантового цифрового підпису

Виклад основного матеріалу

Алгоритми Dilithium, Falcon та Sphincs+ були відібрані NIST для стандартизації в постквантовий період. Вони розвивалися протягом кількох ітерацій. Їх останні подані версії проаналізовані в цій статті, оскільки вони пропонують вдосконалені компроміси між безпекою та продуктивністю. Стандартизація Dilithium та Sphincs+ наразі знаходиться на стадії проекту [11,12]. Перший проект стандарту Falcon досі очікується [13].

Dilithium

Dilithium — представник криптографії на решітках. За основу взята схема Fiat-Shamir з перериваннями. Має хорошу продуктивність і може бути ефективно реалізована на пристроях з малими обчислювальними спроможностями [14].

ЕЦП Dilithium ґрунтується на підході, що отримав назву "Fiat-Shamir з перериваннями" [17]. Dilithium в певній мірі схожий на [16,17]. Розглянемо спрощену версію алгоритму , який складається з алгоритм генерації ключів, генерації та верифікації ЕЦП.

Генерація ключів

1 $A \leftarrow R_q^{k \times t}$

2 $(s_1, s_2) \leftarrow S_\eta^t \times S_\eta^k$

3 $t \coloneqq As_1, s_2$

4 $return\ (pk = (A, t), sk = (A, t, s_1, s_2))$

Генеріція підпису (sk,M)

5 $z \coloneqq \perp$

6 $while\ z = \perp$ do

7 $y \leftarrow S_{\gamma_1 - 1}^l$

8 $w_1 \coloneqq HighBits(A_y, 2_{\gamma_2})$

9 $c \in B_{60} \coloneqq H(M||w_1)$

10 $z \coloneqq y + cs_1$

11 $if\ ||z||_\infty \geq \gamma_1 - \beta\ or\ ||LowBits\ \left(A_y - cs_2, 2_{\gamma_2}\right)||_\infty \geq \gamma_2 - \beta, then\ z \coloneqq \perp$

12 $return\ \sigma = (z, c)$

Верифікація підпису$(pk, M, \sigma = (z, c))$

13 $w_1' \coloneqq HighBits(A_z - ct, 2_{\gamma_2})$

14 $if\ return\ \left[\ ||z||_\infty < \gamma_1 - \beta\right]\ and\ [c = H(M||w_1')]$

Рис.1 Механізм ЕП Dilithium

Таблиця 3 показує основні параметри Dilithium, які детальніше описані в [19]. Таблиця 4 та Рисунок 2 демонструє продуктивність Dilithium з точки зору швидкості виконання.

Таблиця 3

Параметри для версій Dilithium

Рівень безпеки:	128	192	256
Рівень безпеки згідно NIST	1	3	5
Розмір публічного ключа (байти):	1312	1952	2592
Розмір секретного ключа (байти):	2528	4000	4864
Розмір підпису (байти):	2420	3293	4595

Таблиця 4

Порівняння швидкодії версій алгоритму Dilithium

Алгоритм (x86_64)	Генерація ключів/с	Генерація ключів(циклів)	Підпис/с	Підпис (циклів)	Верифікація/с	Верифікація (циклів)
Dilithium2	27648.33	90 295	10656.33	234 475	28625.67	87 258
Dilithium3	16318	153 073	6566.67	380 593	17207.67	145 202
Dilithium5	10099.33	247 413	5247	476 342	10639	234 906

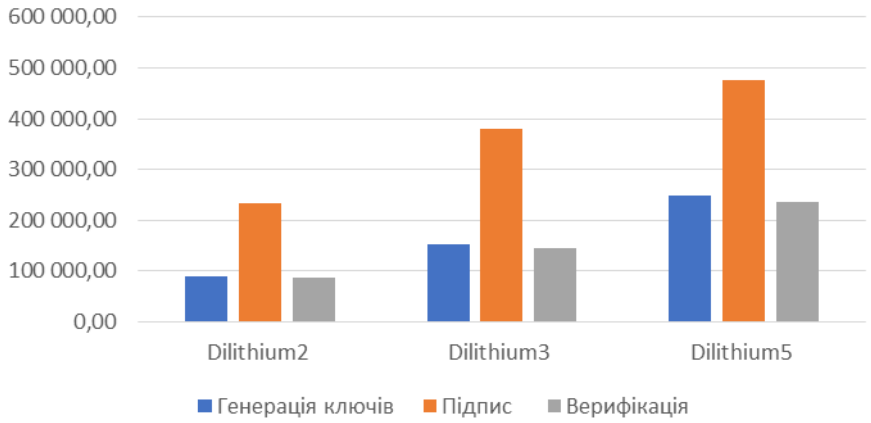

Рис.2 Порівняння швидкодії версій алгоритму Dilithium

В роботі [20] визначені наступні переваги Dilithium:

– вища швидкість і менший розмір порівняно з криптосистемами на основі хеш-функцій (наприклад, схемою Sphincs+);
– простота реалізації, оскільки реалізація розподілу Ґаусса не потрібна.

Dilithium і Falcon – це єдині дві схеми на основі решіток в третьому раунді відбору NIST, і NIST оголосила, що стандартизуватиме лише одну таку схему.

Також автори підкреслили, що розміри підпису та ключа Falcon приблизно в 2.3 рази менші, ніж у Dilithium (рис. 2), але вказали на його недоліки:

- використовує високоточний розподіл Ґаусса (точність 64 біти), що ускладнює виявлення помилок у реалізації (розподіл все одно буде виглядати нормальним, навіть якщо він не є задовільним), що може призвести до витоку секретного ключа;
- його складно замаскувати, і досі не було серйозних спроб це поліпшити. Однак, маскування може бути непотрібним для підписання невеликої кількості повідомлень (на рівні близько 100 повідомлень);
- Dilithium має перевагу використання лише рівномірного відбирання проб в межах діапазону ступенів двійки, що значно спрощує виявлення помилок у реалізації.

Хоча обидва алгоритми є конкурентоспроможними, автори [20] наголосили на застосовності Dilithium та Falcon для конкретних цілей. Наприклад, Dilithium може використовуватися як алгоритм "загального призначення", тоді як Falcon може бути застосований у додатках, що вимагають кількох підписів (на рівні 100–1000 підписів), оскільки Dilithium легше реалізувати, а Falcon забезпечує значно коротші підписи.

Falcon

Falcon – це схема підпису на основі решіток, розроблена на основі теоретичного плану, запропонованого Гентрі, Пейкертом та Вайкунтатананом у їхній статті 2008 року [22]. Безпека алгоритму базується на базовій складній проблемі короткого цілого розв'язку (SIS) над решітки NTRU, для якої в даний час не відомий ефективний алгоритм розв'язання в загальному випадку, навіть за допомогою квантових комп'ютерів.

Falcon слідує структурі, представленій у 2008 р.Гентрі, Пейкертом і Вайкунтатаном, яку називають фреймворком GPV. Алгоритм роботи виглядає наступним чином.

Алгоритм роботи Falcon

1)Відкритий ключ є довгою основою q -ї решітки.

2)Приватний ключ є короткою основою тієї ж решітки.

3)Під час процедури підписання підписувач:

- генерує випадкове значення v;
- обчислює ціль $c = H(m \| v)$, де H – функція, яка надсилає вхідні дані до випадкової точки (на сітці), m –повідомлення;
- використовує свої знання про короткий базис для обчислення точки решітки поблизу цілі с;
- на виході отримує (m, s), де $s = c - v$. .

4)Верифікатор приймає підпис (m, s) в тому випадку, якщо вектор v короткий, та $H(m \| v) - s$ є точкою на решітці, згенерованою його відкритим ключем.

Рекомендовані параметри та показники продуктивності для Falcon представлені в таблиці 5,6. Ці показники продуктивності базуються на реалізації на процесорі Intel Xeon Gold 63338 (з тактовою частотою 2 ГГц).

Таблиця 5

Параметри для версій Falcon

Набір параметрів	Рівень безпеки згідно NIST	Розмір публічного ключа (байти):	Розмір секретного ключа (байти):	Розмір підпису (байти):
Falcon-512	1	897	1281	752
Falcon-1024	5	1793	2305	1462

Таблиця 6

Порівняння швидкодії версій алгоритму Falcon

Алгоритм (x86_64)	Генерація ключів/с	Генерація ключів(циклів)	Підпис/с	Підпис (циклів)	Верифікація/с	Верифікація (циклів)
Falcon-1024	38.04	65 720 685	1390	1 798 694	8563.33	291 853
Falcon-512	112.52	22 220 578	2810	889 570	17368.33	143 857

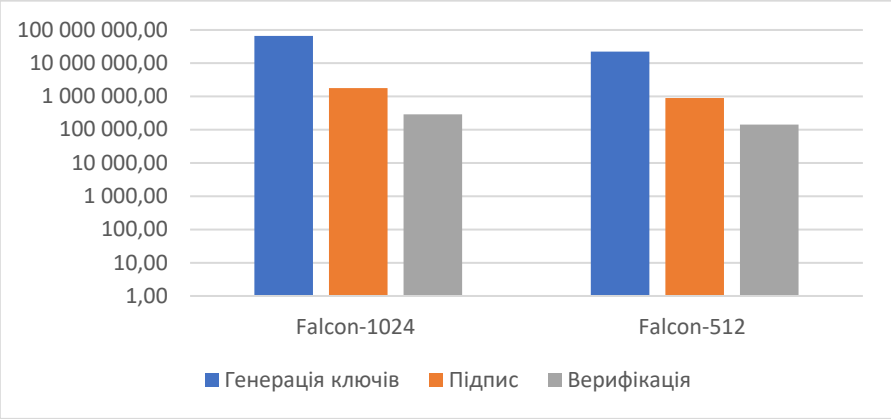

Рис.3 Порівняння швидкодії версій алгоритму Falcon

Переваги та недоліки алгоритму Falcon [24]:

- найбільш ефективний алгоритм з точки зору використання пропускної здатності каналу зв'язку, як показано на рисунку 4;
- для генерації ключів застосовується розподіл Гауса, що забезпечує неможливість визначення характеристик секретного ключа по відкритому ключу, відкритий ключ виглядає як випадковий;
- модульний дизайн; наприклад, NTRU решітки можуть бути замінені на інші типи решіток;
- завдяки використанню решіток NTRU підписи значно коротші, ніж у будь-якій схемі підпису на основі решіток з тими ж гарантіями безпеки, тоді як відкриті ключі мають приблизно однаковий розмір;
- Falcon використовує менше 30 кілобайт оперативної пам'яті, це значно менше, ніж у попередніх варіантах, наприклад, NTRUSign. Falcon сумісний з невеликими вбудованими пристроями з обмеженням пам'яті;
- швидка верифікація;
- краще вивчена безпека проти атак з використанням побічних каналів електромагнітного випромінювання.

Недоліки:

- складні процеси генерації ключів та підписів.

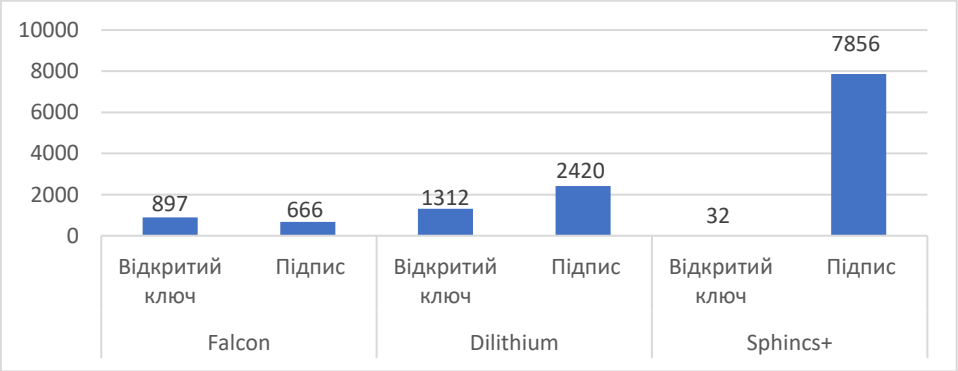

Рис.4 Порівняння розмірів параметрів

Sphincs+

Sphincs+ є алгоритмом постквантового цифрового підпису, розроблений для протидії атакам з використанням квантових комп'ютерів. Основу цього алгоритму складають хеш-функції, безпека схеми проста у оцінці та залежить виключно від характеристик використовуваної хеш-функції. Sphincs+ по суті базується на фундаментальній архітектурі Sphincs, але покращує її за рахунок оптимізації параметрів і впровадження нових методів, спрямованих на підвищення як швидкості алгоритму, так і його безпеки [25].

Таблиця 7,8 показує приклади наборів параметрів для Sphincs+, що націлені на різні рівні безпеки та різні компроміси між розміром і швидкістю [25].

Таблиця 7

Параметри для версій Sphincs+

Назва	Рівень безпеки (біт)	Рівень безпеки NIST	Розмір публічного ключа (байти):	Розмір секретного ключа (байти)	Розмір підпису (байти)
SPHINCS+-128s	133	1	32	64	7856
SPHINCS+-128f	128	1	32	64	17088
SPHINCS+-192s	193	3	48	96	16224
SPHINCS+-192f	194	3	48	96	35664
SPHINCS+-256s	255	5	64	128	29792
SPHINCS+-256f	255	5	64	128	49856

Таблиця 8

Порівняння швидкодії версій алгоритму Sphincs+

Набір параметрів SPHINCS+ (x86 64)	Генерація ключів/с	Генерація ключів(циклів)	Підпис/с	Підпис (циклів)	Верифікація/с	Верифікація (циклів)
SHA2-128f	2678.00	933 411	113.70	21 987 528	1281.33	1 951 192
SHA2-128s	42.51	58 800 222	5.59	447 564 588	3072.00	813 785
SHA2-192f	1777.67	1 406 276	65.29	38 290 480	935.33	2 673 110
SHA2-192s	28.03	89 219 475	2.90	860 908 617	2235.67	1 118 141
SHA2-256f	669.33	3 735 470	31.59	79 125 943	898.33	2 783 246
SHA2-256s	41.85	59 739 270	3.18	786 684 288	1656.00	1 509 614
SHAKE-128f	1360.88	1 836 656	58.12	43 012 220	809.67	3 087 791
SHAKE-128s	21.37	116 999 038	2.82	887 332 813	2148.33	1 163 669
SHAKE-192f	945.35	2 644 168	36.52	68 449 483	580.28	4 307 715
SHAKE-192s	14.75	169 430 099	1.64	1 525 224 718	1597.80	1 564 304
SHAKE-256f	353.88	7 063 679	17.68	141 454 125	549.97	4 545 046
SHAKE-256s	22.25	112 344 406	1.87	1 333 861 498	1069.00	2 338 817

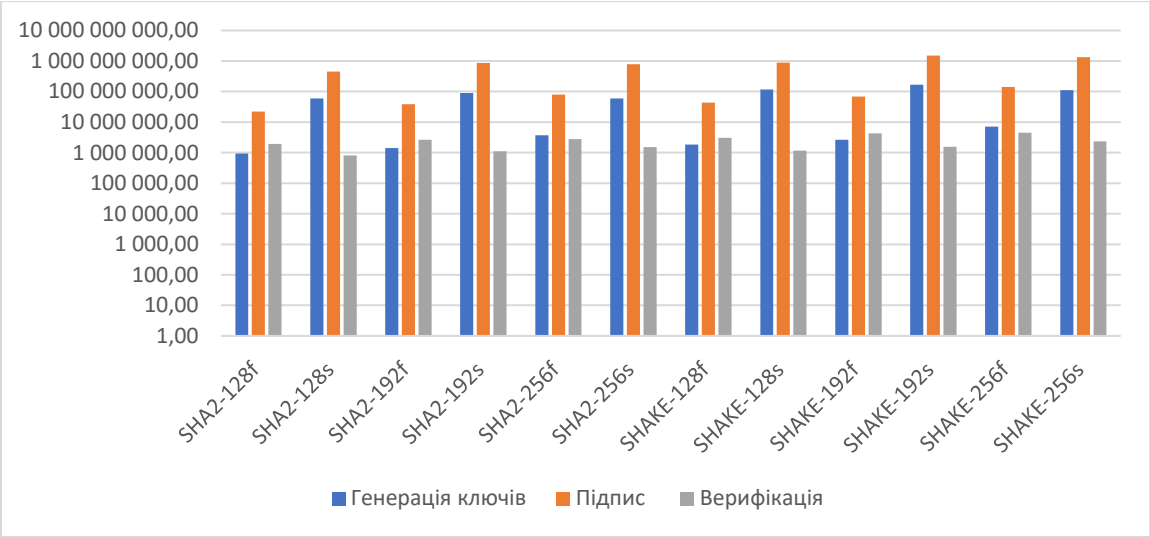

Рис. 5. Порівняння швидкодії версій алгоритму Sphincs+

Рисунок 5 показує показники продуктивності алгоритму при виконанні на процесорі Intel Xeon Gold 63338 (ядро, з тактовою частотою 2.3 ГГц). Також доступні оптимізовані реалізації для платформ, сумісних з набором інструкцій AVX2. Зокрема, для Haraka особливо важливою є наявність набору інструкцій AES-NI. Кожна з шести реалізацій має свою версію для:

- рівнів безпеки NIST один, три та п'ять;
- малих і швидких наборів параметрів.

У таблиці 5 вказані розміри публічних ключів, секретних ключів та цифрових підписів у байтах. Що стосується використання пам'яті, референтна реалізація, як правило, спрямована на мінімальне використання стеку.

Переваги та недоліки алгоритму Sphincs+.

Суть Sphincs+ полягає у її дихотомії. Хоча він, можливо, представляє найбезпечніший підхід до архітектури цифрового підпису постквантового періоду, він платить за це ефективністю: як з точки зору розміру підпису, так і обчислювальної швидкості.

Недоліки:

- Розмір та швидкість підпису: Sphincs+ не розроблений, щоб бути найшвидшим або найменшим, хоча він і пропонує компроміси між цими двома показниками.

Переваги:

- Безпека алгоритму ґрунтується на досліджених та проаналізованих хеш-функціях.
- Атаки, як класичні, так і квантові, можуть бути просто проаналізовані, що дозволяє точно оцінити безпеку.
- Sphincs+ має компактні публічні ключі, що є перевагою в сценаріях, де публічні ключі часто передаються.

Порівняння параметрів та продуктивності

Розмір ключа та підпису.

У аналізі алгоритмів порівнюються два важливі параметри: розмір ключа та розмір підпису, для яких менші значення є кращими. Дані про довжину ключа та підпису представлені на Рисунку 4 [19,23,26].

Два алгоритми на основі решіток (Crystals-Dilithium, Falcon) мають публічні ключі порівнянних розмірів, тоді як Sphincs+ має значно коротшу довжину публічного ключа, як це видно на Рисунку 5. З іншого боку, Sphincs+ має найбільшу довжину підпису.

Швидкість виконання.

Швидкість продуктивності алгоритму оцінюється на основі швидкості виконання трьох операцій: генерації ключів, підпису та верифікації підпису. Швидкість виконання залежить від платформи, на якій запущено алгоритм , а також від реалізації алгоритму. Наукове та професійне співтовариство постійно пропонує нові реалізації алгоритмів з метою їх оптимізації та досягнення кращої продуктивності.

Крім використаних у дослідженні, існують інші реалізації алгоритмів постквантової криптографії для інших платформ. Однак, це окремі реалізації, де порівняльний аналіз усіх трьох алгоритмів цифрового підпису неможливий. Наприклад, Dilithium було реалізовано та протестовано на різних платформах FPGA [28–31], на платформі Cortex M3 [21], на платформах ARMv8 (Cortex-A72 та Apple M1) [32], а також на комп'ютерах IBM Z [33]. Реалізація Falcon також була описана на платформах ARMv8 (CPU Jetson Xavier з 8 ядрами ARMv8.2) [34], а реалізація Sphincs+ була представлена на FPGA [35] та платформах ARM Cortex M3 [36].

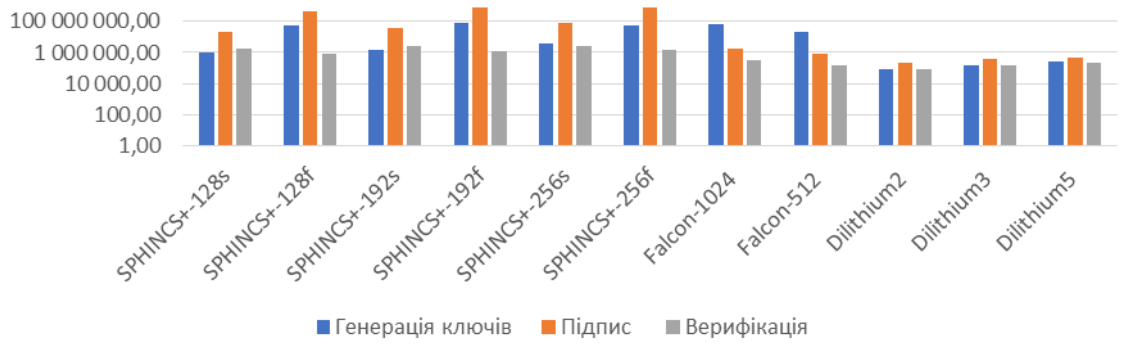

Рис.6 Порівняння швидкодії всіх кандидатів

Дані з рисунку 6 показують швидкість виконання на платформі x86/x64 з процесором Intel Xeon Gold 63338, а [27] надає дані про час виконання для процесора i7-1165G7 для Dilithium та Falcon. [37] і [38] надають дані про споживання енергії, роблячи висновок, що споживання енергії приблизно пропорційне швидкості, тобто часу виконання, оскільки витрати енергії мають набагато менші відхилення (максимум 20% у [37], максимум 50% у [38]) порівняно зі швидкістю виконання.

Підсумки аналізу

Dilithium та Falcon базуються на основі решіток, які мають теоретичне підґрунтя для стійкості проти квантового криптоаналізу. Sphincs+ обирає інший підхід, вибираючи механізми на основі хешів, надаючи змогу більш легко оцінити стійкість алгоритму.

Їхню обчислювальну швидкість було виміряно на платформі з процесором Intel Xeon Gold 63338, розкриваючи відмінні характеристики продуктивності. Falcon вирізнявся швидкістю верифікації підписів. Sphincs+ залишається найбільш вимогливим до обчислювальної потужності алгоритмом, проте він пропонує гнучкість у компромісі між обчислювальною ефективністю та параметрами безпеки.

Оцінки споживання енергії додатково підкреслюють перевагу Dilithium у сценаріях з низьким споживанням енергії, таких як IoT пристрої, тоді як Sphincs+ менш енергоефективний через більше навантаження на обчислювальні ресурси.

З точки зору розмірів ключів та підписів, Falcon добре впорався завдяки своєму компактному дизайну, тим самим оптимізуючи пропускну здатність. Dilithium має дещо більший розмір підписів, що впливає на його ефективність пропускної здатності. Використання Sphincs+ представляє значну проблему у сценаріях з обмеженою пропускною здатністю через його великі підписи.

Dilithium виокремлюється як універсальний та особливо привабливий для вбудованих систем та пристроїв інтернету речей (IoT) завдяки низькому споживанню енергії та обчислювальним вимогам. Falcon, незважаючи на більше навантаження під час генерації ключів, виявляється ідеальним вибором для середовищ з високими вимогами до пропускної здатності та низької затримки завдяки своїй перевазі у швидкій верифікації підписів.

Sphincs+ пропонує гнучкість налаштування рівня безпеки та обчислювальної швидкості. Хоча цей компроміс позиціонує його як реальний варіант для певних сценаріїв використання, його низька швидкість виконання операцій та великий розмір підпису значно обмежують його корисність.

У підсумку, порівняльна оцінка за ключовими метриками виявила такі особливості:

- Розміри публічних ключів та підписів показують, що Sphincs+ пропонує найменший розмір публічного ключа, що є корисним для пристроїв з обмеженим обсягом зберігання.

- Dilithium є лідером за швидкістю генерації ключів та підпису, тоді як Falcon є оптимальним для швидкої верифікації підписів.

Висновки

В роботі проведено детальний аналіз ефективності різних алгоритмів, що дає чітке уявлення про їхні сильні та слабкі сторони в контексті потенційної реалізації у сучасних інформаційних системах. За результатами досліжень було визначено недоліки та переваги кожного алгоритму, з урахуванням важливості

контекстно-специфічного використання. Було встановлено, що Dilithium має найменше навантаження на обчислювальні ресурси системи, Falcon виділяється швидкістю верифікації підписів, а Sphincs+ забезпечує необхідний рівень стійкості.

Запропоновані на сьогоднішній день кандидати на стандарт квантовостійкого електронного цифрового підпису, мають принципово нові структури, які не глибоко досліджені та надвеликі довжини ключів (рис.7), що створює суттєве навантаження на обчислювальні потужності в існуючих програмно-апаратних засобах, на основі яких побудовані сучасні інформаційні системи. Можливості існуючих алгоритмів криптоперетворень на основі еліптичних кривих не забезпечують зростаючої потреби у стійкості алгоритмів автентифікації до квантового криптоаналізу, а використання сучасних кандидатів на стандарт постквантової криптографії не дозволяє в короткостроковій перспективі здійснити перехід на використання нових криптоалгоритмів в інформаційних системах. Це потребує розробки методів що вдосконалюють алгоритми ЕЦП на основі еліптичних кривих з урахуванням стійкості до квантового криптоаналізу.

Напрямком подальших досліджень є розробка нових криптоалгоритмів і методів, що забезпечать цілісність та конфіденційність інформації під час її передачі незахищеними каналами в перехідний період до широкого використання та впровадження стандартів постквантової криптографії.

References

1. Quantum Computing Approaches for Mission Covering Optimization [Електронний ресурс] / [M. Cutugno, A. Giani, P. Alsing та ін.] // Algorithms 15(7). – 2022. – Режим доступу до ресурсу: https://www.mdpi.com/1999-4893/15/7/224..
2. Quantum Computing Approaches for Mission Covering Optimization [Електронний ресурс] / [M. Cutugno, A. Giani, P. Alsing та ін.] // 15(7). – 2022. – Режим доступу до ресурсу: https://www.mdpi.com/1999-4893/15/7/224.
3. NIST. Post-Quantum Cryptography [Електронний ресурс] – Режим доступу до ресурсу: https://csrc.nist.gov/Projects/post-quantum-cryptography` (дата звернення: 1.04.24).
4. NIST. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms [Електронний ресурс] – Режим доступу до ресурсу: https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms
5. NIST. Post-Quantum Cryptography—Call for Proposals. [Електронний ресурс] – Режим доступу до ресурсу: https://csrc.nist.gov/Projects/post-quantumcryptography/post-quantum-cryptography-standardization/Call-for-Proposals (дата звернення: 1.04.24).
6. NIST. Post-Quantum Cryptography—Round 1 Submissions. [ЕЛЕКТРОННИЙ РЕСУРС] – РЕЖИМ ДОСТУПУ ДО РЕСУРСУ: https://csrc.nist.gov/Projects/post-quantumcryptography/Round-1-Submissions (дата звернення: 1.04.24).
7. NIST. Post-Quantum Cryptography—Round 2 Submissions. [ЕЛЕКТРОННИЙ РЕСУРС] – РЕЖИМ ДОСТУПУ ДО РЕСУРСУ: https://csrc.nist.gov/Projects/post-quantumcryptography/round-2-submissions (дата звернення: 1.04.24).
8. NIST. Post-Quantum Cryptography—Round 3 Submissions. 11 September 2023. [Електронний ресурс] – Режим доступу до ресурсу: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions .
9. Pronin T. New Efficient, Constant-Time Implementations of Falcon [Електронний ресурс] / Pronin // Cryptology ePrint Archive. – 2019. – Режим доступу до ресурсу: https://eprint.iacr.org/2019/893. (дата звернення: 10.04.24).
10. NIST. Module-Lattice-Based Digital Signature Standard. 24 August 2023. [Електронний ресурс] – Режим доступу до ресурсу: https://csrc.nist.gov/pubs/fips/204/ipd (дата звернення: 1.04.24).
11. NIST. Stateless Hash-Based Digital Signature Standard. 24 August 2023. [Електронний ресурс] – режим доступу до ресурсу: https://csrc.nist.gov/pubs/fips/205/ipd (дата звернення: 1.04.24).
12. NIST. NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers. 24 August 2023. [Електронний ресурс] – Режим доступу до ресурсу: https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantumcomputers (дата звернення: 1.04.24).
13. CRYSTALS Team. CRYSTALS-Dilithium—Cryptographic Suite for Algebraic Lattices. [Електронний ресурс] – Режим доступу до ресурсу: https://pq-crystals.org/dilithium/index.shtml (дата звернення: 1.04.24).
14. Lyubashevsky V. Lattice Signatures Without Trapdoors [Електронний ресурс] / V. Lyubashevsky // Advances in Cryptology—EUROCRYPT 2012; Springer: Berlin, Heidelberg, 2012; Volume 7237. – 2012. – Режим доступу до ресурсу: https://link.springer.com/chapter/10.1007/978-3-642-29011-4_43.
15. Guneysu T. Practical lattice-based cryptography: A signature scheme for embedded systems [Електронний ресурс] / T. Guneysu, V. Lyubashevsky, T. Poppelmann // Cryptographic Hardware and Embedded Systems—CHES 2012; Springer: Berlin, Heidelberg, 2012; Volume 7428. – 2012. – Режим доступу до ресурсу: https://www.iacr.org/archive/ches2012/74280529/74280529.pdf.
16. Bai S. CRYSTALS-Dilithium–Algorithm Specifications and Supporting Documentation [Електронний ресурс] / S. Bai, L. Ducas, E. Kiltz. – 2020. – Режим доступу до ресурсу: https://csrc.nist.gov/CSRC/media/Projects/postquantum-cryptography/documents/round-3/submissions/Dilithium-Round3.zip. (дата звернення: 10.04.24).
17. Lyubashevsky V. Dilithium Presentation at Third PQC Standardization Conference—Session I

Welcome/Candidate Updates [Електронний ресурс] / V. Lyubashevsky // NIST. – 2021. – Режим доступу до ресурсу: https://csrc.nist.gov/presentations/2021/crystals-dilithium-round-3-presentation. (дата звернення: 10.04.24).

18. Greconici, D. Compact Dilithium Implementations on Cortex-M3 and Cortex-M4 [Електронний ресурс] / Greconici, D., Kannwischer, M., Sprenkels, D. // IACR Trans. Cryptogr. Hardw. Embed. Syst. – 2021. – Режим доступу до ресурсу: https://tches.iacr.org/index.php/TCHES/article/view/8725/8325.

19. Gentry C. Trapdoors for hard lattices and new cryptographic constructions [Електронний ресурс] / C. Gentry, C. Peikert, V. Vaikuntanathan // Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing. – 2008. – Режим доступу до ресурсу: https://eprint.iacr.org/2007/432.23. Fouque P. Falcon:Fast-Fourier Lattice-based Compact Signatures over NTRU [Електронний ресурс] / P. Fouque, J. Hoffstein, P. Kirchner. – 2020. – Режим доступу до ресурсу: https://csrc.nist.gov/CSRC/media/Projects/post-quantum-cryptography/documents/round-3/submissions/Falcon-Round3.zip.

20. Prest, T. Falcon Presentation at Third PQC Standardization Conference—Session I Welcome/Candidate Updates. 2021. [Електронний ресурс] – Режим доступу до ресурсу: https://www.nist.gov/video/third-pqc-standardization-conference-session-i-welcomecandidate-updates (дата звернення: 10.04.24).

21. Bernstein, D.J.; Hopwood, D.; Hülsing, A.; Lange, T.; Niederhagen, R.; Papachristodoulou, L.; Schneider, M.; Schwabe, P.; Wilcox-O'Hearn, Z. SPHINCS: Practical stateless hash-based signatures. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, 26–30 April 2015; Springer: Berlin/Heidelberg, Germany, 2015; pp. 368–397.

22. Ding, J.; Chen, M.-S.; Kannwischer, M.; Patarin, J.; Petzoldt, A.; Schmidt, D.; Yang, B.-Y. Rainbow—Algorithm Specification and Documentation; 2020. [Електронний ресурс] – Режим доступу до ресурсу: https://csrc.nist.gov/CSRC/media/Projects/post-quantum-cryptography/documents/round-3/submissions/Rainbow-Round3.zip (дата звернення: 10.04.24).

23. Soni, D.; Basu, K.; Nabeel, M.; Karri, R. A Hardware Evaluation Study of NIST Post-Quantum Cryptographic Signature schemes. In Proceedings of the 2nd NIST PQC Standardization Conference, Santa Barbara, CA, USA, 22–24 August 2019.

24. Ortega, K.D.; Perez, L.J.D. Implementing CRYSTAL-Dilithium on FRDM-K64. In Proceedings of the 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, New York, NY, USA, 1–4 Грудня 2021.

25. Beckwith, L. High-Performance Hardware Implementation of CRYSTALS-Dilithium [Електронний ресурс] / Beckwith, L., Nguyen, D.T., Gaj, K. // Proceedings of the 2021 International Conference on Field-Programmable Technology (ICFPT), Auckland, New Zealand. – 2021. – Режим доступу до ресурсу: https://eprint.iacr.org/2021/1451.pdf.

26. Zhao C. A Compact and High-Performance Hardware Architecture for CRYSTALS-Dilithium [Електронний ресурс] / C. Zhao, N. Zhang, H. Wang // IACR Trans. Cryptogr. Hardw. Embed. Syst.. – 2022. – Режим доступу до ресурсу: https://tches.iacr.org/index.php/TCHES/article/view/9297/8863.

27. Becker, H. Neon NTT: Faster Dilithium, Kyber, and Saber on Cortex-A72 and Apple M1 [Електронний ресурс] / Becker, H., Hwang, V., Kannwischer, M.J. // IACR Transactions on Cryptographic Hardware and Embedded Systems; 2022; Volume 2022. – 2022. – Режим доступу до ресурсу: https://eprint.iacr.org/2021/986.pdf.

28. Bradbury J. Fast Quantum-Safe Cryptography on IBM Z [Електронний ресурс] / J. Bradbury, B. Hess // Proceedings of the 3rd NIST PQC Standardization Conference. – 2021. – Режим доступу до ресурсу: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/hess-fast-quantum-safe-pqc2021.pdf.

29. Kim, Y. Accelerating Falcon on ARMv8 [Електронний ресурс] / Kim, Y., Song, J., Seo, S. // IEEE Access. – 2022. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9762260.

30. Amiet, D. FPGA-based SPHINCS+ Implementations: Mind the Glitch [Електронний ресурс] / D. Amiet,, Leuenberger, L., Curiger, A. // Proceedings of the 2020 23rd Euromicro Conference on Digital System Design (DSD), Kranj, Slovenia. – 2020. – Режим доступу до ресурсу: https://www.researchgate.net/publication/344627240_FPGA-based_SPHINCS_Implementations_Mind_the_Glitch.

31. Hülsing, A. ARMed SPHINCS [Електронний ресурс] / Hülsing, A., Rijneveld, J., Schwabe, P. // PKC 2016; Springer: Berlin/Heidelberg, Germany. – 2016. – Режим доступу до ресурсу: https://joostrijneveld.nl/papers/armedsphincs/

32. Roma C. Energy Efficiency Analysis of Post-Quantum Cryptographic Algorithms [Електронний ресурс] / C. Roma, C. Tai, M. Hasan // IEEE Access. – 2021. – Режим доступу до ресурсу: https://www.researchgate.net/publication/351708179_Energy_Efficiency_Analysis_of_Post-Quantum_Cryptographic_Algorithms.

33. Dimopoulos, C. Energy Consumption Evaluation of Post-Quantum TLS 1.3 for Resource-Constrained Embedded Devices [Електронний ресурс] / Dimopoulos, C., Fournaris, A., Zhao, R. // Proceedings of the 20th ACM International Conference on Computing Frontiers, Bologna. – 2023. – Режим доступу до ресурсу: https://eprint.iacr.org/2023/506.pdf.