ISSN 2519-2310 (Online)

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА, 2025, № 1 (27)

COMPUTER SCIENCE AND CYBERSECURITY, 2025, Iss. 1 (27)

DOI: https://doi.org/10.26565/2519-2310-2025-1-01
УДК 004.056.5

ОЦІНКА ТА ПОРІВНЯННЯ КРИПТОПЕРЕТВОРЕНЬ ТИПУ ЕЛЕКТРОННИЙ ПІДПИС ДОДАТКОВОГО КОНКУРСУ NIST США «DIGITAL SIGNATURE SCHEMES»

Іван Горбенко[1], доктор технічних наук, професор, e-mail: i.d.gorbenko@karazin.ua,
ORCID: https://orcid.org/0009-0003-6979-8946
Єлизавета Острянська[1], молодший науковий співробітник, e-mail: antelizza@gmail.com,
ORCID: https://orcid.org/0000-0003-1412-8470
Володимир Пономар[1], старший науковий співробітник, e-mail: Laedaa@gmail.com,
ORCID: https://orcid.org/0000-0001-5271-2251
[1]*Харківський національний університет імені В.Н. Каразіна,*
майдан Свободи, 4, Харків, 61022, Україна
Рукопис надійшов 1 березня 2025 р. Отримано після рецензування 1 квітня 2025 р.
Прийнято 2 травня 2025 р.

Анотація: У сучасному світі розвиток квантових обчислень ставить під загрозу класичні криптографічні алгоритми, зокрема RSA, EC-DSA та DSA, які використовуються для забезпечення цифрової безпеки. Це створює необхідність розробки постквантових криптографічних рішень, здатних протистояти атакам квантових комп'ютерів. Особливо важливими є стійкі алгоритми електронного підпису, адже вони забезпечують автентифікацію, цілісність та незаперечність інформації у фінансових, юридичних та державних системах. У статті проведено аналіз та порівняння криптографічних схем електронного підпису, що беруть участь у додатковому конкурсі NIST «Digital Signature Schemes». Досліджено ключові математичні основи цих алгоритмів, зокрема криптографію на решітках, схеми на основі кодів, багатовимірні перетворення, ізогенії еліптичних кривих та методи MPC-in-the-Head. Оцінено їхню продуктивність, безпеку та ефективність у контексті постквантових загроз. Проведено детальний аналіз розмірів відкритих ключів, підписів та швидкості операцій генерації ключів, підписання й перевірки. Виявлено основні переваги та недоліки кожного з підходів, визначено перспективні напрями розвитку постквантових електронних підписів та їх можливе практичне застосування. Дослідження є актуальним у зв'язку з необхідністю переходу на нові криптографічні стандарти, що гарантуватимуть безпеку даних у майбутньому. Отримані результати дозволяють оцінити сильні та слабкі сторони розглянутих алгоритмів, а також визначити перспективні напрями подальшого розвитку постквантової криптографії.

Ключові слова: *постквантова криптографія, NIST PQC, електронний підпис, квантово-стійкий, квантово-безпечний*

Як цитувати: Горбенко І., Острянська Є., Пономар В. Оцінка та порівняння криптоперетворень типу електронний підпис додаткового конкурсу NIST США «Digital Signature Schemes». *Комп'ютерні науки та кібербезпека.* 2025; № 1(27): С. 6–16. https://doi.org/10.26565/2519-2310-2025-1-01

In cites: Gorbenko I., Ostrianska Ye., Ponomar V. (2025). Evaluation and comparison of cryptographic digital signature transformations of the additional NIST competition «Digital Signature Schemes». *Computer Science and Cybersecurity. 1*(27): 6–16. https://doi.org/10.26565/2519-2310-2025-1-01 (in Ukrainian)

1. Вступ

У сучасному цифровому світі електронні підписи відіграють ключову роль у забезпеченні автентичності, цілісності та незаперечності інформації. Вони використовуються у фінансових транзакціях, електронному документообігу, цифрових сертифікатах, блокчейн-технологіях та багатьох інших сферах. Так, наприклад, і в Україні вже впроваджено стандарт квантово-стійкого електронного підпису ДСТУ 9212:2023 [4]. Однак із розвитком квантових технологій постає новий виклик – традиційні криптографічні алгоритми можуть стати вразливими до атак квантових комп'ютерів. Саме тому криптографія на решітках є перспективним напрямком досліджень, який активно розвивається в останні роки.

У зв'язку з цим Національний інститут стандартів і технологій США (NIST) запустив ініціативу з розробки нових, стійких до квантових атак електронних підписів (ЕП). Окрім основного конкурсу, NIST також організував додатковий відбір алгоритмів електронного підпису, який включає нові перспективні розробки, що можуть стати альтернативою вже відібраним кандидатам [3]. Цей процес є важливим для забезпечення максимальної безпеки та ефективності майбутніх криптографічних стандартів і він спрямований на оцінку нових перспективних алгоритмів, які можуть забезпечити стійкість до атак квантових комп'ютерів. NIST розглядає різні підходи до побудови постквантових підписів, зокрема криптографію на основі решіток, кодів, багатовимірних рівнянь, ізогеній еліптичних кривих та інтерактивних доказів знання.

Метою цієї роботи є оцінка та експериментальний порівняльний аналіз математичних методів криптоперетворень типу ЕП, які повинні бути стійкими згідно національних вимог до квантовостійких стандартів криптографічних перетворень ЕП та конкурсу NIST США «Digital Signature Schemes». У цій статті також розглянуто принципи роботи електронних підписів, та аналізуються найбільш перспективні алгоритми, що претендують на роль майбутніх криптографічних стандартів.

2. Попередні визначення та критерії порівняння

На даний момент після більш, ніж року оцінювання, NIST обрав 14 алгоритмів-кандидатів ЕП (див. табл. 1) для другого раунду додаткового конкурсу електронних підписів для процесу стандартизації NIST PQC [1].

Критерії для визначення кандидатів у першому раунді включали положення щодо еталонного та оптимізованого коду C, тести з відомими відповідями, письмову специфікацію та необхідні заяви про інтелектуальну власність. Це були єдині критерії, за якими оцінювали пакети подання. Інші фактори, такі як безпека, вартість і характеристики алгоритму та реалізації кандидатів, не враховувалися під час процесу перевірки перед першим раундом, а також криптоаналіз або дані продуктивності подання не вплинули на прийняття кандидатів у першому раунді.

Вже для другого раунду NIST [2] визначив три широкі аспекти критеріїв оцінки, які будуть використовуватися для порівняння алгоритмів-кандидатів на роль підпису в рамках процесу стандартизації NIST PQC: 1) безпека, 2) вартість і продуктивність і 3) характеристики реалізації. Також схеми повинні суттєво відрізнятися від схем підписів, які NIST вже вибрав для

стандартизації. Зокрема, в умовах конкретно зазначено, що подання повинні, як мінімум, відповідати одному з наступних критеріїв:

• Схеми на основі решітки повинні забезпечувати принаймні одну велику перевагу в продуктивності порівняно зі вже стандартизованими Crystals-Dilithium і Falcon.

• Алгоритми, що не базуються на решітці, повинні забезпечувати принаймні одну велику перевагу в продуктивності над SPHINCS+.

Щодо безпекових критеріїв відбору, то NIST перерахував бажані властивості безпеки, такі як стійкість до бічних каналів і атак з кількома ключами та стійкість до неправильного використання. У поданнях заохочувалося зазначати додаткові бажані властивості безпеки, надані крім стандартної непідробності (наприклад, ексклюзивне право власності, підписи в повідомленні та можливість повторного підписання). Нарешті, NIST вимагав узагальнення відомих криптоаналітичних атак на схеми та оцінку складності цих атак.

Другим за важливістю критерієм під час оцінки потенційних алгоритмів були вартість і продуктивність, зокрема, розмір відкритих ключів і підписів та обчислювальна ефективність операцій підписання та перевірки, а також генерації ключів (тобто швидкість алгоритмів). Вимоги до пам’яті стосуються як розміру коду, так і вимог до оперативної пам’яті (RAM) для програмних реалізацій.

Таблиця 1 – Схеми ЕП другого раунду конкурсу NIST

Table 1 – Digital signature schemes of the 2nd round of the NIST competition

№	Підпис Signature	Математична основа Mathematical foundation
1.	CROSS	Коди/Codes
2.	LESS	
3.	SQIsign	Ізогенії/Isogenies
4.	HAWK	Алгебраїчні решітки/ Algebraic lattices
5.	Mirath (об’єднання MIRA/MiRitH)	MPC-in-the-Head
6.	MQOM	
7.	PERK	
8.	RYDE	
9.	SDitH	
10.	MAYO	Багатовимірні перетворення/ Multidimensional transformations
11.	QR-UOV	
12.	SNOVA	
13.	UOV	
14.	FAEST	Симетричні перетворення/ Symmetric transformations

Серед кандидатів, визначених в таблиці 1: два алгоритми ЕП на основі кодів, один алгоритм ЕП на основі ізогеній, один алгоритм ЕП, в основі якого лежать операції на решітках, п’ять кандидатів на роль алгоритму ЕП на основі методу MPC-in-the-Head та чотири алгоритми, в основі яких лежать багатовимірні перетворення. На основі симетричних криптоперетворень було обрано одну схему електронного підпису.

3. Короткий огляд алгоритмів підписів

CROSS (Codes and Restricted Objects Signature Scheme) [5] – це постквантова схема електронного підпису, що базується на кодах, розроблена для забезпечення безпеки в умовах квантових обчислень. Вона використовує структури кодів та обмежених об'єктів для створення стійких до квантових атак підписів. Ця схема підпису отримана шляхом застосування перетворення Фіата-Шаміра до інтерактивного протоколу ідентифікації з нульовим знанням (ZK). CROSS базується на так званій проблемі декодування обмеженого синдрому (R-SDP), NP-складній задачі, яку можна розглядати як варіант класичної проблеми декодування синдрому (SDP). Хоча немає поки відомих атак проти CROSS, проблеми відносно нові. NIST чекає подальшого аналізу основних проблем і протоколу ідентифікації ZKPoK. CROSS пройшов до другого раунду частково через зацікавленість NIST у ньому як у схемі «не на решітках», яка демонструє переваги продуктивності порівняно з SLH-DSA.

LESS [6] – це криптографічна схема, що використовує кодові структури для забезпечення безпеки в умовах квантових обчислень. Вона розроблена для створення стійких до квантових атак електронних підписів, використовуючи складність декодування лінійних кодів. LESS будується шляхом застосування перетворення Фіата-Шаміра до інтерактивного ZKPoK розв'язку задачі еквівалентності обчислювального коду. Безпека LESS базується на складності проблеми лінійної еквівалентності (LEP). У результаті було отримано дуже гнучку схему, яка пропонує для кожного рівня безпеки кілька компромісів між простотою, швидкістю, розміром відкритого ключа та розміром підпису. Крім того, параметри легко вибирати та масштабувати.

SQIsign [7] – це постквантова схема електронного підпису, що базується на ізогеніях суперсингулярних еліптичних кривих. Вона використовує математичні властивості ізогеній для забезпечення безпеки та компактності підписів. Як і кілька інших кандидатів, SQIsign використовує парадигму Фіата-Шаміра, щоб перетворити схему ідентифікації з нульовим знанням на схему підпису. Безпека базується на знанні секретної ізогенії еліптичної кривої. SQIsign має новий підхід, і тому потребує додаткової оцінки та аналізу. NIST сподівається, що додаткові дослідження призведуть до подальшої оптимізації, яка покращить продуктивність.

HAWK [8] – це схема підпису типу hash-and-sign на основі решітки, яка тісно пов'язана з Falcon. Центральними математичними об'єктами в HAWK є матриці елементів з одного сімейства кілець, які використовуються в алгоритмах на основі решітки, обраних для стандартизації. Falcon використовує швидке перетворення Фур'є, яке використовує арифметику з плаваючою комою. HAWK покладається на проблему найкоротшого вектору (omSVP) і проблему ізоморфізму решітки модуля пошуку (smLIP), щоб уникнути витоку секретної інформації. NIST вирішив залишити HAWK на 2-й раунд через його високу ефективність.

Mirath [9] (злиття MIRA та MiRitH) – це схема електронного підпису, заснована на складності вирішення проблеми MinRank. MIRA і MiRitH – це схеми підписів, створені на парадигмі багатосторонніх обчислень (MPCitH). Підписи для обох схем генеруються шляхом застосування перетворення Фіата-Шаміра до ZKPoK розв'язку задачі MinRank. Безпека як для MIRA, так і для MiRitH базується на складності проблеми MinRank. Ці схеми містять варіанти, які використовують структуру гіперкубу, яка є оптимізацією в рамках парадигми MPCitH, яка використовує додатковий обмін секретами, що дозволяє розпаралелювати протокол MPCitH.

MQOM [10] – це схема підпису, побудована на парадигмі MPCitH, яка базується на складності розв'язання випадкової багатовимірної системи квадратних рівнянь з рівною кількістю змінних і рівнянь. Незважаючи на те, що проблема вирішення багатовимірних квадратичних систем була добре вивчена, нещодавні результати можуть мати незначний вплив на її параметри, необхідні для досягнення цільових рівнів безпеки. Як і інші схеми, що базуються на методах «in the head», MQOM забезпечує дуже малі розміри відкритих ключів і

середній розмір підписів. NIST вважає, що зміни в другому раунді допоможуть знайти оптимальні компроміси між продуктивністю та розмірами підписів на основі різних припущень складності.

PERK [11] – це схема електронного підпису, заснована на складності вирішення проблеми PERmuted Kernel. Вона розроблена для забезпечення безпеки від атак як класичних, так і квантових комп’ютерів. PERK – підпис, який складається із ZKPoK секретної перестановки. Хоча проблема, на яку спирається PERK, була запропонована близько 30 років тому, існує невизначеність щодо її конкретної складності. Додаткові дослідження цього припущення допоможуть підвищити впевненість у конкретних параметрах PERK для різних рівнів безпеки.

RYDE [12] – схема підпису, побудована на парадигмі MPCitH. Подібно до інших схем підпису MPCitH, побудова RYDE передбачає генерування випадкового рівняння разом із рішенням. NIST висунув RYDE до другого раунду конкурсу через конкурентоспроможність схеми в категорії схем підписів MPCitH і VOLEiTH. Основна складна проблема декодування синдрому рангу також виглядає неструктурованою, а відповідне припущення щодо безпеки виглядає консервативним.

Syndrome Decoding in the Head (SDitH) [13] – базується на структурі MPCitH і пропонує набори параметрів з використанням двох методів оптимізації. Тобто схема SDitH має два варіанти: варіант гіперкуба і пороговий варіант. Безпека базується на складності розв’язання d-розподіленого варіанту проблеми декодування синдрому для випадкових лінійних кодів над кінцевими полями. Незважаючи на те, що SDitH тісно пов’язаний із відомою NP-складною проблемою, NIST вважає, що SDitH може отримати користь від аналізу безпеки.

MAYO [14] – це варіант UOV з меншими відкритими ключами. Відновлення ключа MAYO зводиться до пошуку простору «oil» UOV, а підробка підпису MAYO зводиться до спроби інвертувати відображення, схоже на UOV. Завдяки цій додатковій структурі MAYO значно покращує розмір відкритого ключа порівняно з UOV, успадковуючи малий розмір підпису UOV. Хоча він не такий швидкий, як UOV, MAYO все ще дуже ефективний.

QR-UOV [15] є варіантом UOV з меншими відкритими ключами з використанням фактор-кільця. На відміну від матриць UOV, елементи яких належать скінченному полю . Завдяки додатковій структурі відкритий ключ QR-UOV на 50% менший порівняно з UOV. NIST зберігає інтерес до QR-UOV через його конкурентоспроможність, але структура QR-UOV потребує подальшого вивчення. NIST передбачає, що продуктивність може бути покращена, і заохочує розробників до подальшої оптимізації їх впровадження.

Алгоритм електронного підпису SNOVA [16] є варіантом алгоритму UOV, який зберігає характеристику коротких підписів UOV, водночас пропонуючи меншу довжину відкритого ключа порівняно з традиційним алгоритмом UOV, що забезпечує переваги як у аспектах безпеки, так і в ефективності електронних підписів. Під час першого раунду SNOVA зазнала атаки, яка вплинула на деякі з поданих наборів параметрів. Потім SNOVA оновила свої параметри, але зазнала нової атаки. Тим не менш, деякі з представлених наборів параметрів SNOVA перенесли обидві атаки. Новизна SNOVA та історія її атак змушують NIST поставити під сумнів її безпеку навіть більше, ніж інші схеми структурованого UOV, спрямовані на значно зменшений розмір ключа. Проте той факт, що SNOVA все ще має безперебійні набори параметрів із найменшими відкритими ключами, доступними для схем на основі UOV, робить його привабливим кандидатом для продовження вивчення

UOV (Unbalanced Oil and Vinegar) [17] – це схема електронного підпису, яка залишається безпечною навіть проти квантових комп’ютерів. Схема UOV є найстарішою безперервною багатовимірною криптосистемою, яка була запропонована в 1999 році. Структура UOV базується на системі квадратних рівнянь, для якої існує секретний підпростір, на якому

система оцінюється як нуль. Ця схема забезпечує безпеку EUF-CMA. Хоча UOV є зрілою та досить стабільною схемою, атака за останні чотири роки незначно знизила безпеку деяких режимів її параметрів. NIST рекомендує суспільству залишатися пильним і продовжувати критично аналізувати безпеку UOV.

FAEST [18] – це схема електронного підпису, створена за допомогою відносно нової техніки під назвою VOLEitH. Ця техніка пов'язана з підходом MPCitH, який використовується кількома іншими схемами підписів у процесі постквантової стандартизації NIST. Хоча теоретична безпека FAEST базується лише на припущеннях симетричного ключа, його продуктивність значно краща, ніж у більшості інших схем із такою властивістю, включаючи SLH-DSA. Однак продуктивність FAEST не конкурентоспроможна зі схемами на основі решітки, такими як ML-DSA і FN-DSA. Таким чином, FAEST є багатообіцяючою схемою для програм, які не вимагають продуктивності, що забезпечується підписами на основі решітки.

4. Порівняльний аналіз підписів

У цьому розділі у таблицях 2-6, відповідно, наведено результати порівняння розмірів підписів, відкритих ключів, а також швидкодію розглянутих в попередньому розділі підписів додаткового конкурсу NIST. Порівняння було проведено для 1, 3 та 5-го рівнів безпеки NIST відповідно. Усі значення розмірів ключів і підписів в таблицях 2-6 наведено в байтах, а швидкодія в – у циклах процесору. В таблиці 2 розглянуто порівняння алгоритмів на кодах.

Таблиця 2 – Порівняння схем ЕП на кодах

Table 2 – Comparison of code-based schemes performance

Схема	Параметри	Відкритий ключ (байти)	Підпис (байти)	Генерація ключів (цикли)	Підписання (цикли)	Верифікація (цикли)
CROSS	R-SDP(G)-1-f	54	9120	130,000	3,713,000	2,125,000
	R-SDP(G)-3-f	83	22464	140,000	5,630,000	3,530,000
	R-SDP(G)-5-f	106	40100	165,000	11,756,000	7,448,000
LESS	LESS-1-252	67484	1745	1,300,000	94,400,000	93,500,000
	LESS-3-400	35074	5585	4,000,000	336,800,000	365,100,000
	LESS-5-548	85793	9464	10,000,000	981,200,000	998,000,000

В таблиці 3 наведено порівняння алгоритмів на MPC-in-the-Head перетвореннях. Запуски алгоритмів та середні оцінки часу було здійснено та розраховано на комп'ютері на процесорі Intel Core i9-13900K на 3 GHz з використанням AVX2 інструкцій. Також слід зазначити, що схема SDitH розглядалася для варіанта гіперкуба, а інші схеми в таблиці 3 розглядалися в швидкому варіанті.

Таблиця 3 – Порівняння схем на MPC-in-the-Head перетвореннях

Table 3 – Comparison of MPC-in-the-Head-based schemes performance

Схема	Параметри	Відкритий ключ (байти)	Підпис (байти)	Генерація ключів (цикли)	Підписання (цикли)	Верифікація (цикли)
Mirath	Mirath-1a-Fast	73	3,728	200,000	11,000,000	9,800,000
	Mirath-3a-Fast	107	8,537	300,000	33,600,000	34,400,000
	Mirath-5a-Fast	147	15,507	500,000	86,700,000	65,100,000
RYDE	RYDE-1-Fast	69	3,597	35,900	6,700,000	6,600,000

	RYDE-3-Fast	101	8,264	64,700,000	27,300,000	27,100,000
	RYDE-5-Fast	133	14,609	77,500,000	49,000,000	44,500,000
SDitH	gf256-L1-hyp	132	8,496	14,200,000	10,800,000	9,700,000
	gf256-L3-hyp	180	19,544	16,600,000	26,200,000	22,900,000
	gf256-L5-hyp	244	33,924	28,700,000	49,900,000	44,000,000
PERK	PERK-I-fast5	240	8,030	89,000	7,000,000	4,900,000
	PERK-III-fast5	370	18,000	186,000	15,000,000	11,000,000
	PERK-V-fast5	510	31,700	324,000	33,000,000	26,000,000
MQOM	L1-gf251-fast	59	7809	480,000	11,520,000	10,160,000
	L3-gf251-fast	92	17161	1,960,000	32,850,000	29,580,000
	L5-gf251-fast	125	29919	4,830,000	81,550,000	75,580,000

Нижче в таблиці 4 розглянуто порівняння алгоритмів на багатовимірних перетвореннях, тобто схем, в основі яких лежить принцип UOV. Для схеми UOV ми розглядали класичний варіант, для схеми MAYO для рівня безпеки NIST I було розглянуто набір параметрів MAYO_one, який має менші відкриті ключі та більший розмір підпису, а також було обрано варіант, що має AVX2 оптимізації. Щодо схеми підпису QR-UOV, то було розглянуто еталонну реалізацію на коді C з AVX2 інструкціями та AES PRG для наборів параметрів (q,v,m,l): (127,156,54,3), (127,228,78,3), (127,306,105,3). Для алгоритму SNOVA в таблиці в дужках зазначено, що до розміру підпису/відкритого ключа додатково додається +16 байт солі/початкового значення, відповідно.

Таблиця 4 – Порівняння схем ЕП на багатовимірних перетвореннях

Table 4 – Comparison of multivariate schemes performance

Схема	**Параметри**	**Відкритий ключ (байти)**	**Підпис (байти)**	**Генерація ключів (цикли)**	**Підписання (цикли)**	**Верифікація (цикли)**
UOV	uov-I-classic	412,160	128	4,203,437	105,324	90,336
	uov-III-classic	1,225,440	200	17,603,360	299,316	241,588
	uov-V-classic	2,869,440	260	49,490,856	591,812	470,886
MAYO	I	1420	454	216,704	872,216	392,541
	III	2986	681	362,446	1,676,585	665,382
	V	5554	964	910,684	3,582,362	10,737,685
QR-UOV	I	24,255	200	8,587,000	1,586,000	1,224,000
	III	71,891	292	32,311,000	4,599,000	3,410,000
	V	173,676	392	95,579,000	10,504,000	7,463,000
SNOVA	I	9,826(+16)	90(+16)	9,595,012	10,964,945	3,161,199
	III	31,250(+16)	136(+16)	44,658,255	47,587,816	9,443,639
	V	71,874(+16)	188(+16)	166,196,633	158,443,732	25,289,616

В таблиці 5 розглянемо єдину схему підпису на решітках додаткового конкурсу NIST, а саме HAWK та порівняємо її зі схемою Falcon, що також в основі має математику на решітках. Вона використовує швидке перетворення Фур’є для підписання повідомлення та покладається на проблему найкоротшого вектору (omSVP). Для HAWK та Falcon ми розглядаємо параметри для I (HAWK-512) та V (HAWK-1024) рівнів безпеки NIST та робили тести з використанням AVX2 інструкцій.

Таблиця 5 – Порівняння схем ЕП на алгебраїчних решітках

Table 5 – Comparison of lattice-based schemes performance

Схема	Параметри	Відкритий ключ (байти)	Підпис (байти)	Генерація ключів (цикли)	Підписання (цикли)	Верифікація (цикли)
HAWK	HAWK-512	1024	555	8,432,840	85,371	156,224
	HAWK-1024	2440	1221	43,660,958	190,936	314,625
Falcon	1	897	666	19,872,000	1,009,764	81,036
	5	1793	1280	63,135,000	2,053,080	160,596

В таблиці 6 розглянуто схеми FAEST та SQISign, що базуються на симетричних перетвореннях та ізогеніях, відповідно. Обидві схеми ЕП використовують перетворення Фіата-Шаміра для протоколу з нульовим знанням та мають малі розміри відкритих ключів, але, як показано в таблиці 6 нижче, є дуже повільними, особливо в порівнянні зі схемами на решітках.

Таблиця 6 – Порівняння схем FAEST та SQISign

Table 6 – Comparison of FAEST and SQISign schemes performance

Схема	Параметри	Відкритий ключ (байти)	Підпис (байти)	Генерація ключів (цикли)	Підписання (цикли)	Верифікація (цикли)
FAEST	FAEST-128f	32	4,506	5,000	12,787,000	9,783,000
	FAEST-192f	40	11,260	11,000	54,687,000	42,290,000
	FAEST-256f	48	20,696	13,000	76,330,000	74,546,000
SQISign	I	65	148	43,300,000	401,600,000	5,100,000
	III	97	224	134,000,000	899,200,000	18,600,000
	V	129	292	212,000,000	1,207,500,000	35,700,000

Таким чином, розглянувши окремо порівняння алгоритмів на різних математичних конструкціях (табл. 2-6), для повноти дослідження на рис. 1 ми наводимо їх загальне порівняння.

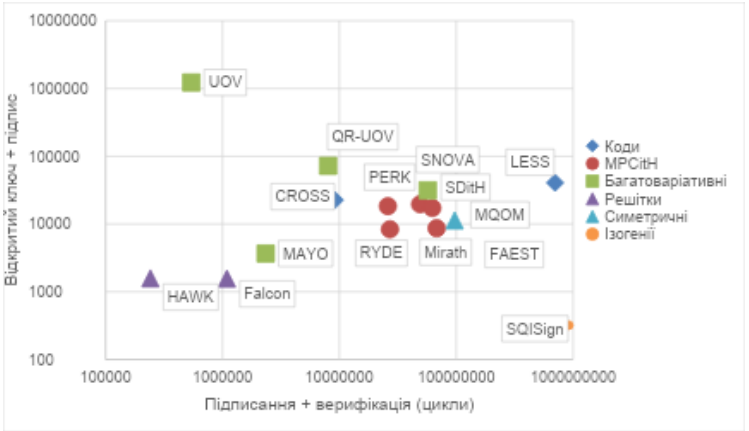

Рис. 1 – Порівняння алгоритмів підпису за співвідношенням відкритий ключ+підпис та час підписання+верифікації

Fig. 1 – Comparison of signature algorithms by public key+signature length ratio and signing+verification time

В результаті аналізу алгоритмів підпису з рис.1 можна зробити висновки, що кожен із підходів має власні переваги та обмеження, які необхідно враховувати при розробці стандартів криптографічного підпису.

Щодо розміру відкритих ключів та підписів, то найменший розмір підпису в сумі з довжиною відкритого ключа спостерігається у схемі на основі ізогеній (SQISign). Також доволі невеликі відкриті ключі та підписи демонструють схеми на основі MPC-in-the-Head перетворень (MQOM, RYDE, Mirath), що робить їх привабливими для застосувань із обмеженими ресурсами. Натомість, найбільші відкриті ключі характерні для UOV та SNOVA, що може бути значним недоліком у реальних сценаріях використання. Хоча в той же час UOV має дуже короткі підписи та високу швидкість підписання та перевірки. Найменший розмір підпису в сумі з довжиною відкритого ключа забезпечує SQIsign, тоді як у CROSS та PERK підписи є значно більшими.

Найшвидші алгоритми для створення підпису та верифікації – схеми, в основі яких лежать перетворення на алгебраїчних решітках і це HAWK (і Falcon), але схеми на основі багатовимірних перетворень, такі як UOV та MAYO, також демонструють непогану швидкість підписання, що робить їх ефективними для великомасштабних операцій. Схеми на кодах такі як CROSS і LESS, мають нижчу продуктивність у процесі підписання через складні обчислення. Але вони потрапили до другого раунду частково через зацікавленість NIST у них як у схемах «не на решітках», що демонструють переваги продуктивності порівняно з SLH-DSA. Щодо схеми SQIsign на основі ізогеній, то генерація підпису є повільнішою порівняно з іншими кандидатами через складність математичних конструкцій, і таким чином є складним для впровадження.

Якщо розглядати алгоритми з точки зору безпеки та стійкості до атак, то схеми на основі кодів (CROSS, LESS) вважаються безпечними, але потребують додаткового аналізу з точки зору довготривалої стійкості. А також їх структура є доволі специфічною тому, реалізація може бути складною, що вимагає ретельного підходу та експертизи HAWK та інші схеми на решітках використовують перевірені математичні припущення, але можуть бути уразливими до атак бічними каналами.

Окремо виділяється схема FAEST на основі техніки VOLEitH. Хоча теоретична безпека FAEST базується лише на припущеннях симетричного ключа, його продуктивність значно краща, ніж у більшості інших схем із такою властивістю, включаючи SLH-DSA. Основна техніка VOLEitH, що лежить в основі схеми була представлена тільки в 2023. Конструкція дещо складна та нова, а надійність безпеки дуже технічна. Тому спільності криптографів та науковців необхідний час, щоб впевнитися в безпеці даної конструкції.

Схема на основі ізогеній (SQIsign) вимагає оптимізації та глибшого аналізу криптостійкості через складну структуру. Інші схеми підпису, особливо на багатовимірних перетвореннях, покладаються на добре вивчені проблеми, такі як MinRank, Rank-SD, тощо, і є стійкими до квантових атак, але деякі з них потребують додаткового криптоаналізу.

6. Висновки

1. Дослідження алгоритмів електронного підпису, що беруть участь у другому раунді додаткового конкурсу NIST [3], дозволяє оцінити їхні сильні та слабкі сторони з точки зору безпеки, продуктивності та ефективності реалізації. Конкурс спрямований на доповнення основного процесу стандартизації, забезпечуючи різноманітність криптографічних підходів, які можуть бути використані в постквантовому середовищі.

Другий раунд додаткового конкурсу NIST представляє важливий крок у розробці постквантових алгоритмів електронного підпису. Алгоритми, що базуються на

MPC-in-the-Head, демонструють високу продуктивність та ефективність, тоді як схеми на решітках, кодах та багатовимірних перетвореннях мають потенціал завдяки своїм унікальним властивостям та багаторічному криптоаналізу, тобто надійній стійкості до квантових атак.

Успішна стандартизація та впровадження постквантових підписів у сучасні криптографічні системи є критично важливим завданням для забезпечення довготривалої безпеки цифрових технологій. Тому було розглянуто кандидатів на електронний підпис та проведено порівняльний аналіз. В результаті можна сказати, що NIST зацікавлений в альтернативах схемам на алгебраїчних решітках, бо шукає нові рішення та конструкції для різних застосувань. Перспективами подальшого розвитку поточних досліджень є:

• Оптимізація розміру підписів та ключів: хоча багато алгоритмів демонструють гарну продуктивність, зменшення їх розмірів без втрати безпеки залишається ключовим завданням.

• Зміцнення стійкості до комбінованих атак: деякі алгоритми, особливо на основі кодів та багатовимірних перетворень, потребують додаткових перевірок та більш глибокого криптоаналізу проти нових атак.

• Практичне впровадження: багато алгоритмів поки що не мають ефективних реалізацій, оптимізованих для апаратних платформ та мобільних пристроїв і тому процес впровадження є складним.

Конфлікт інтересів

Автори повідомляють про відсутність конфлікту інтересів.

References

1. Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process (2024). *NIST Internal Report NIST IR 8528* https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8528.pdf
2. National Institute of Standards and Technology (2022) *Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process*. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf
3. National Institute of Standards and Technology (2025) *Post-Quantum Cryptography: Additional Digital Signature Schemes Round 2 Additional Signatures*. https://csrc.nist.gov/projects/pqc-dig-sig/round-2-additional-signatures
4. Information Technologies. Cryptographic Information Protection (2023) Electronic Signature Algorithm on Algebraic Lattices with Deviations: DSTU 9212:2023. Kyiv: Derzhspozhyvstandart of Ukraine [in Ukrainian]
5. CROSS – Codes and Restricted Objects Signature Scheme (2025) *Submission to the NIST Post-Quantum Cryptography Standardization Process*. https://www.cross-crypto.com/CROSS_Specification_v2.0.pdf
6. Baldi M. and others (2025) LESS. *Linear Equivalence Signature Scheme.* https://www.less-project.com/LESS-2025-02-07.pdf
7. Marius A. and others (2025) SQIsign. *Algorithm specifications and supporting documentation*. Version 2.0. URL:. https://sqisign.org/spec/sqisign-20250205.pdf
8. Joppe W. Bos and others (2025) *HAWK*. Version 1.1. URL: https://hawk-sign.info/hawk-spec.pdf
9. Agj G. and others (2025) Mirath Signature Scheme *Algorithm Specifications and Supporting Documentation.* URL: https://pqc-mirath.org/assets/downloads/mirath_v2.0.pdf.
10. Feneuil Th. Rivain M (2023) MQOM: MQ on my Mind *Algorithm. Specifications and Supporting Documentation* (Version 1.0). URL: https://mqom.org/docs/mqom-v1.0.pdf
11. Aaraj Na. and others (2025) PERK. Version 2.0. URL: https://pqc-perk.org/assets/downloads/perk-v2.0.pdf
12. Aragon N. and others. RYDE Signature Scheme. *Algorithm Specifications and Supporting Documentation.* Version 2.0. URL: https://pqc-ryde.org/assets/downloads/ryde_specification_v2.0.pdf

13. Melchor C. A. and others (2023) The Syndrome Decoding in the Head (SD-in-the-Head) Signature Scheme. *Algorithm Specifications and Supporting Documentation* – Version 1.1. URL: https://sdith.org/docs/sdith-v1.1.pdf
14. Beullens W. and others (2023) MAYO. *Algorithm Specifications*. URL: https://pqmayo.org/assets/specs/mayo.pdf.
15. Hiroki Furue and others (2025) QR-UOV. *Algorithm Specifications*. Nippon telegraph and telephone corporation. URL: https://info.isl.ntt.co.jp/crypt/qruov/files/qruov_Spec-v2.0.pdf
16. SNOVA (2023) Proposal for NIST PQC: Digital Signature Schemes project. Version 1.0. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/SNOVA-spec-web
17. Beullens W. and others (2023) UOV: Unbalanced Oil and Vinegar. *Algorithm Specifications and Supporting Documentation.* Version 1.0. URL: https://drive.google.com/file/d/1NdMHuCyyFG6xgOGrpssM99kyiNwA9JG-/view
18. Baum C. and others (2025) FAEST v2: *Algorithm Specifications*. Version 2.0. URL: https://faest.info/faest-spec-v2.0.pdf.

EVALUATION AND COMPARISON OF CRYPTOGRAPHIC DIGITAL SIGNATURE TRANSFORMATIONS OF THE ADDITIONAL NIST COMPETITION «DIGITAL SIGNATURE SCHEMES»

Ivan Gorbenko[1], Doctor of Sciences (Engineering), Full Prof.; e-mail: i.d.gorbenko@karazin.ua;
ORCID: https://orcid.org/0000-0003-6979-8946
Yelyzaveta Ostrianska[1], junior researcher; e-mail: antelizza@gmail.com;
ORCID: https://orcid.org/0000-0003-1412-8470
Volodymyr Ponomar[1], senior researcher fellow; e-mail: Laedaa@gmail.com;
ORCID: https://orcid.org/0000-0001-5271-2251
[1] *V. N. Karazin Kharkiv National University, Ukraine*
Manuscript was received March 1, 2025; Received after review April 1, 2025;
Accepted May 2, 2025

Abstract. In the modern world, the development of quantum computing threatens classical cryptographic algorithms, in particular RSA, ECDSA and DSA, which are used to ensure digital security. This creates a need to develop post-quantum cryptographic solutions that can be resistance under quantum computers attacks. Stable digital signature algorithms are especially important, as they provide authentication, integrity and non-repudiation of information in financial, legal and government systems. The article analyzes and compares cryptographic digital signature schemes participating in the NIST supplementary competition "Digital Signature Schemes". The main mathematical foundations of these algorithms are investigated, in particular, lattice cryptography, code-based schemes, multivariate transformations, elliptic curve isogenies and MPC-in-the-Head methods. Their performance, security and efficiency in the context of post-quantum threats are assessed. A detailed analysis of the length of public keys, signatures and the speed of key generation, signing and verification operations is carried out. The main advantages and disadvantages of each approach are identified, promising directions for the development of post-quantum digital signatures and their possible practical application are identified. The research is relevant in connection with the need to transition to new cryptographic standards that will guarantee data security in the future. The results allow to assess the strengths and weaknesses of the considered algorithms, as well as to identify promising directions for the further researches of post-quantum cryptography.

Keywords: *post-quantum cryptography; NIST PQC, digital signature, quantum-resistant; quantum safe*

Conflicts of Interest: the authors declare no conflict of interest.