Інформаційні технології

УДК 004.056.55

Колесник Дмитро Олександрович

студент

Харківського національного університету імені В.Н. Каразіна

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПЕРСПЕКТИВНИХ ЦИФРОВИХ ПІДПИСІВ НА ОСНОВІ АЛГЕБРАЇЧНИХ РЕШІТОК

Анотація. *Проведено порівняльний аналіз семи цифрових підписів на основі алгебраїчних решіток на основі конкурсу NIST.*

Ключові слова: *алгебраїчні решітки, постквантова криптографія, асиметричне шифрування.*

На конкурс PQC, що проводить NIST США, було подано 69 пакетів заявок. Деякі пакети містять декілька алгоритмів, тому у сумі було отримано до розгляду більше 80 алгоритмів різного типу – шифрування, підпису, інкапсуляції ключів. З них було отримано 22 алгоритми (електронного) підпису (ЕП), що базуються на різних математичних апаратах. З усіх цих підписів я обрав лише 5, які відносяться до підписів на основі алгебраїчних решіток. У табл. 1 наведено криптографічні алгоритми типу ЕП [1].

Таблиця 1

Механізми підпису на основі решіток

№	Назва	Анотація
1.	CRYSTALS-DILITHIUM	Схема цифрового підпису Dilithium, захист якої ґрунтується на складності пошуку коротких векторів у решітках.
2.	DRS	Діагональне домінантне зменшення для підпису на основі решітки
3.	FALCON	Швидкі компактні підписи на основі решітки Фур'є над NTRU – Falcon є схемою підпису на основі решітки. Високоякісний конструкція Falcon є простою: ми аналізуємо теоретичні рамки, описані Gentry, Peikert і Vaikuntanathan для побудови гешування-та-підпису схем підпису на основі решітки. Ця структура вимагає двох складових: Клас криптографічних решіток. Обрано клас решіток NTRU. Зразок лазівки. Покладаються на нову техніку, яка називаються швидкою вибіркою Фур'є. Коротко, схема підпису

		Falcon може бути описана таким чином: Falcon = GPV рамка + решітки NTRU + Швидка вибірка Фур'є.
4.	pqNTRUsign	pqNTRUSign: схема цифрового підпису на основі модульної решітки, яка використовує решітку NTRU або з однорідною, або з гаусовою вибіркою.
5.	qTESLA	Схема постквантового підпису, який базується на складності рішення проблеми кільцевого навчання з помилками (R-LWE). На відміну від інших альтернатив, qTESLA є консервативною, але ефективною схемою підпису, що було показано відповідно до наданого зменшення безпеки. Тобто, екземпляри qTESLA достовірно захищені в (квантовій) випадковій моделі оракула. З цією метою ця схема супроводжується несуттєвим скороченням випадкової моделі оракула та жорстким зменшенням квантової випадкової моделі оракула з R-LWE.

Джерело: розробка автора

У таблиці 2 наведено механізми підпису, які були на сьогоднішній день вже атаковані, або відкликані [2].

Таблиця 2

Атаковані (відкликані) механізми підпису

Кандидат	**Тип**	**Підтип**	**Клас**	**Статус**	**Аналіз**	**Примітки**
pqsigRM	Код	Розбитий (проколотий) код Ріда-Мюллера (РМ)	Підпис	Раунд 1	Атаковано	Розбиті (Проколоті) стовпці відкритої матриці перевірки парності можна ідентифікувати статистично з кількох сотень підписів.
RaCoSS	Код	Схема підпису на основі випадкового коду	Підпис	Раунд 1	Атаковано	Геш-функція з малою вагою, що використовується в RaCoSS, не є безпечною. RaCoSS може швидко підписати будь-яке повідомлення для будь-якого відкритого ключа з вказаними параметрами RaCoSS, не знаючи секретного ключа.
WalnutDSA	Коси	Групові теоретичні OWF	Підпис	Раунд 1	Атаковано	Атака існує на більш ранню версію. Запобігання атаці здійснено за рахунок зміни структури секретного (особистого) ключа, але проблеми залишаються. Можна генерувати v-довгі підроблені підписи –

						проблема доказу навколишньої безпеки. Схема може бути вразливою до атак "квадратного коріння" – <2^512 можливостей для кожної половини відкритого ключа у WalnutDSA.
SRTPI	MQE		Підпис	Раунд 1	Відкликано	Зламаний на основі КМА: підпис операцій секретного ключа є лінійним.
DME	MQ	PK	Підпис	Раунд 1		Занепокоєння щодо досягнутого рівня безпеки

У таблиці 3 наведено розміри основних параметрів вищерозглянутих механізмів підпису [2].

Таблиця 3

Розміри та часові характеристики основних параметрів механізмів підпису

Submission	Specific Implementation	Category	Keypair Average (тактів)	Sign Average (тактів)	Open Average (тактів)	sk (байт)	pk (байт)	bytes (байт)
CRYSTALS-Dilithium	Dilithium_medium	Lattices	244 278	1 185 462	307 111	2 800	1 184	2 044
CRYSTALS-Dilithium	Dilithium_recommended	Lattices	606 338	2 753 772	558 281	3 504	1 472	2 701
CRYSTALS-Dilithium	Dilithium_very_high	Lattices	651 600	2 293 141	611 325	3 856	1 760	3 366
DRS	DRS128	Lattices	1 001 828 786	62 867 536	505 869 989	51 274	5 094 433	8 550
DRS	DRS192	Lattices	1 910 198 595	95 622 249	814 640 083	84 060	8 410 001	11 020
DRS	DRS256	Lattices	2 147 483 647	148 424 947	1 419 704 155	144 527	14 402 026	14 421
Falcon	falcon1024	Lattices	300 030 872	19 884 364	1 384 574	8 193	1 793	1 330
Falcon	falcon512	Lattices	91 009 209	8 359 971	666 108	4 097	897	690
Falcon	falcon768	Lattices	157 623 028	13 058 641	1 117 624	6 145	1 441	1 077
pqNTRUsign	Gaussian-1024	Lattices	259 672 814	349 028 118	2 955 494	2 604	2 065	2 065
pqNTRUsign	Uniform-1024	Lattices	268 329 761	202 185 303	2 726 230	2 604	2 065	2 065
qTESLA	qTesla_128	Lattices	3 223 865	2 020 404	459 633	2 112	4 128	3 104
qTESLA	qTesla_192	Lattices	6 571 755	9 899 854	955 576	8 256	8 224	6 176
qTESLA	qTesla_256	Lattices	12 746 635	8 143 869	1 436 949	8 256	8 224	6 176

sk – особистий (секретний) ключ; pk – відкритий ключ;

sk size – розмір особистого (секретного) ключа у байтах;

pk size – розмір відкритого ключа у байтах;

pk/sk size – розмір відношення відкритий/особистий ключ у байтах;

Sign Average (signing (average)) – кількість тактів процесора, що витрачається на процес підпису (в середньому);

Keypair Average (KeyGeneration (Average)) – кількість тактів процесора, що витрачається на генерацію ключової пари (в середньому);

Open Average (Verification (average)) – кількість тактів процесора, що витрачається на перевірку підпису (в середньому);

bytes (Signature Size) – розмір підпису в байта

Джерело: розробка автора

1. Порівняльний аналіз механізмів підпису за основними параметрами

Наведемо порівняння механізмів підпису, що розглянуті у таблиці 3 за параметрами цієї ж таблиці.

Результати порівняння наведено на рисунках 1 – 7 [2]

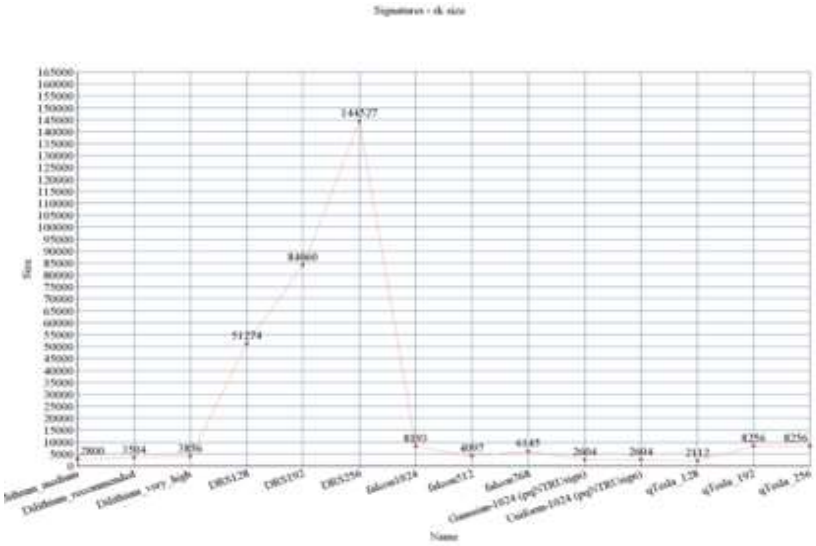

Рис. 1. Порівняння розміру особистих (секретних) ключів механізмів підпису у байтах

Джерело: розробка автора

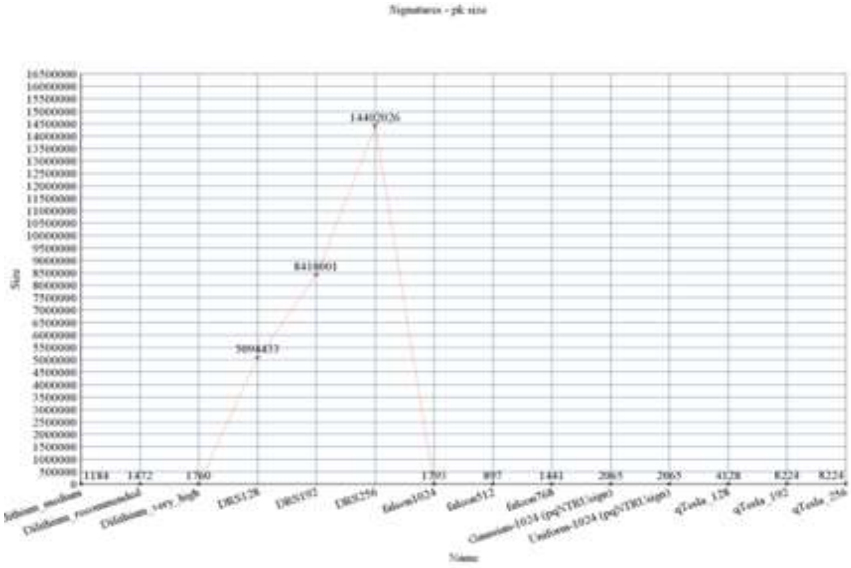

Рис. 2. Порівняння розміру відкритих ключів механізмів підпису у байтах

Джерело: розробка автора

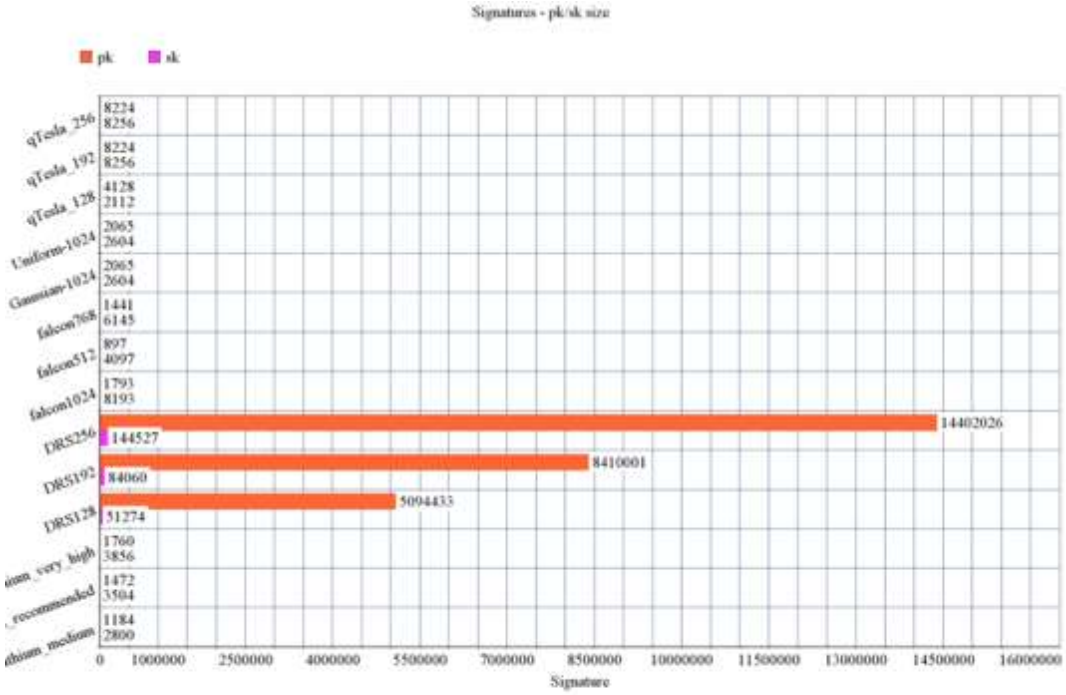

Рис. 3. Порівняння розміру відношення відкритих/особистих ключів механізмів підпису у байтах

Джерело: розробка автора

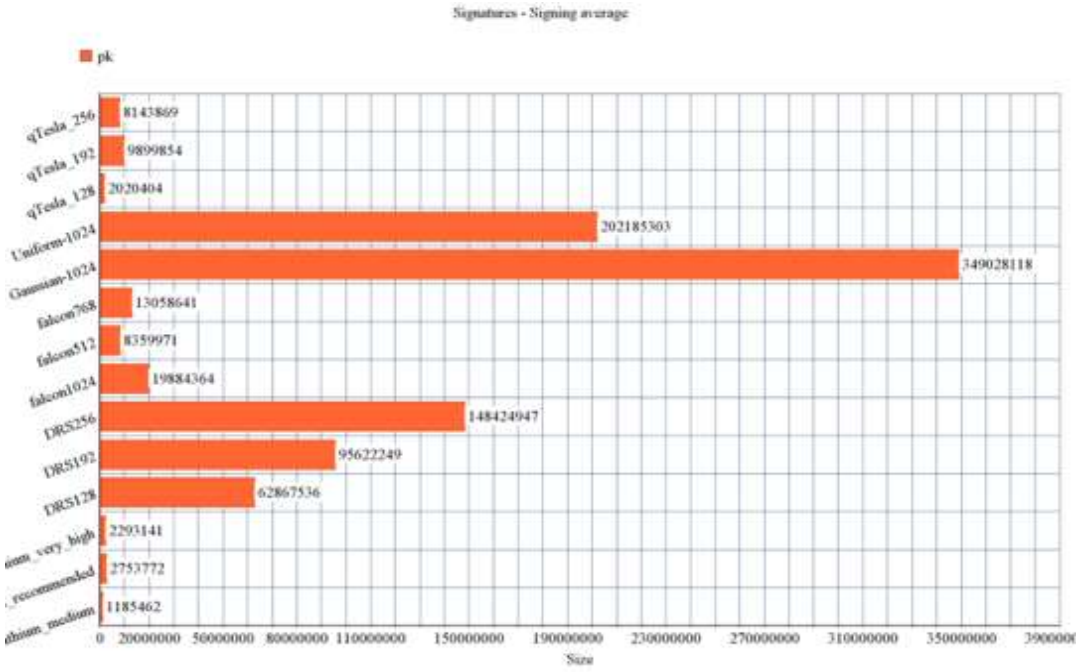

Рис. 4. Порівняння кількості тактів процесора, що витрачається на процес підпису (в середньому)

Джерело: розробка автора

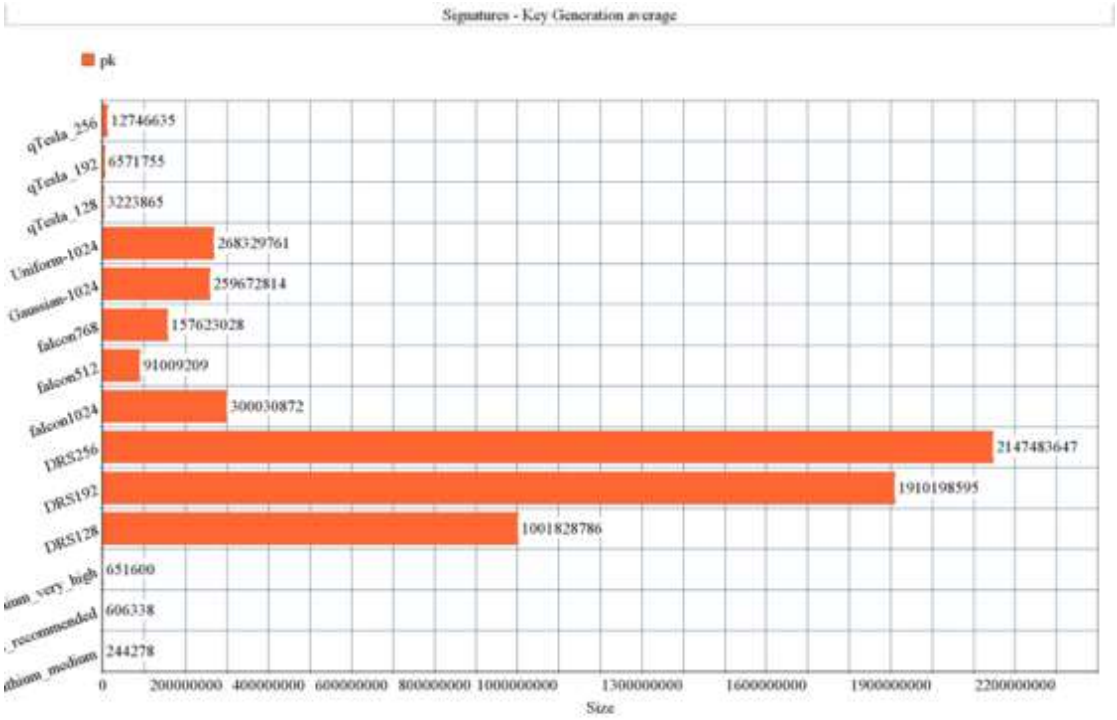

Рис. 5. Порівняння кількості тактів процесора, що витрачається на генерацію ключової пари (в середньому)

Джерело: розробка автора

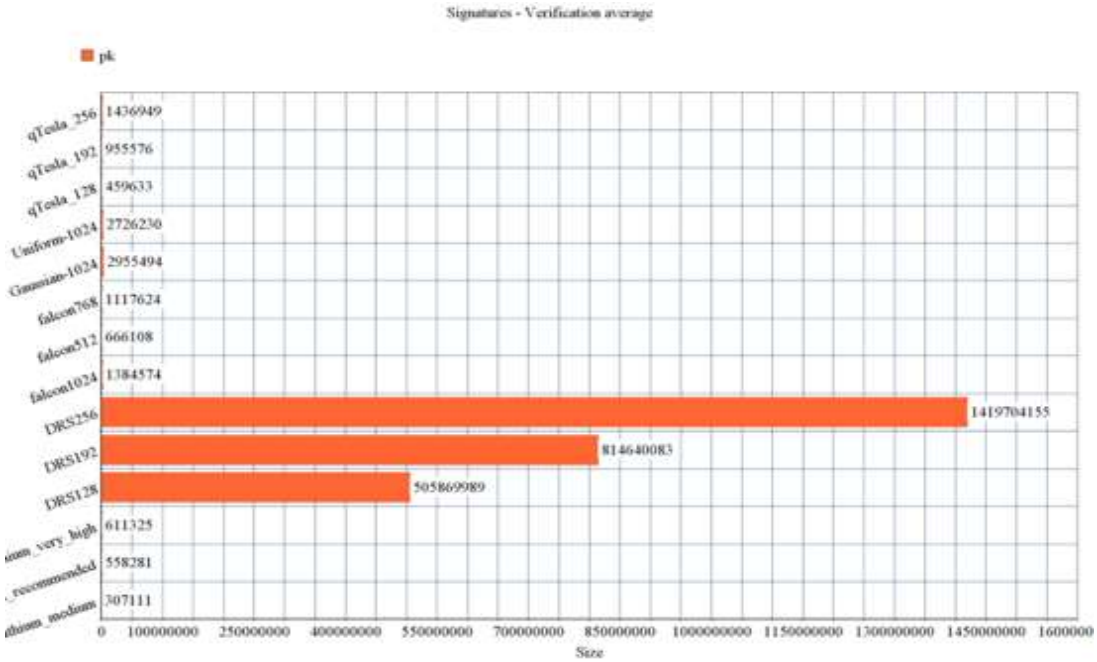

Рис. 6. Порівняння кількості тактів процесора, що витрачається на перевірку підпису (в середньому)

Джерело: розробка автора

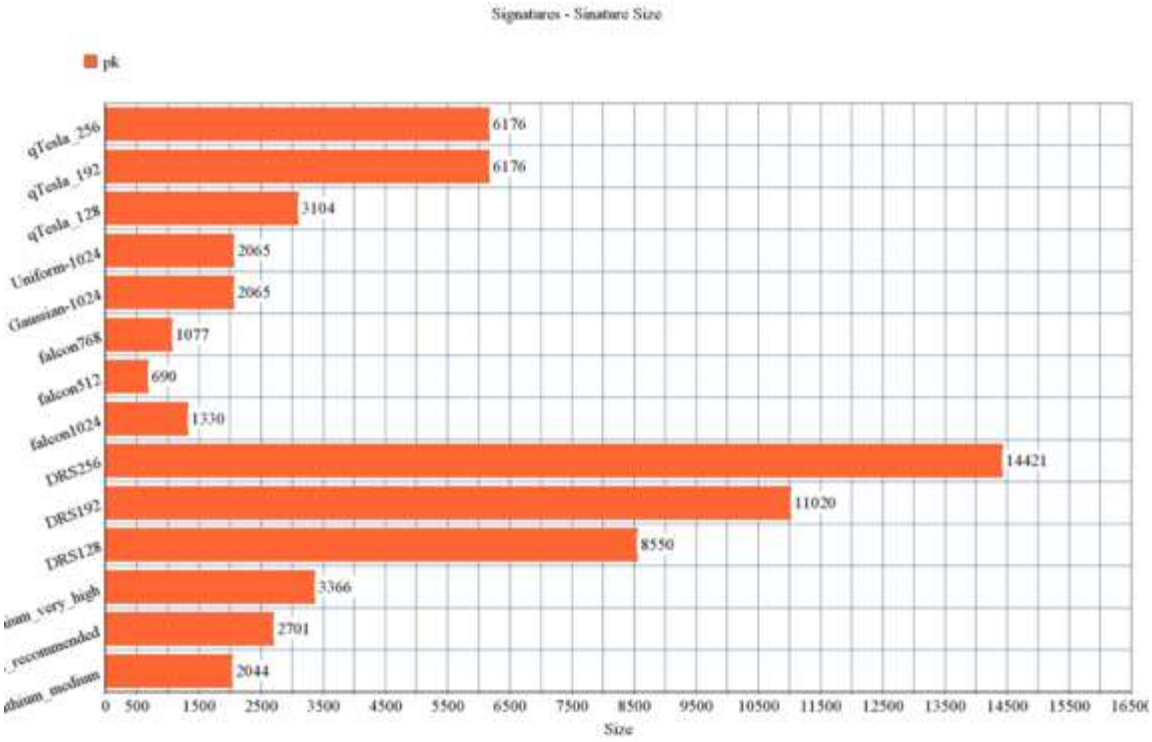

Рис. 7. Порівняння розміру підпису в байтах
Джерело: розробка автора

2. Порівняльний аналіз механізмів підпису за сукупністю безумовних та умовних критеріїв

Під час порівняльного аналізу використовувалася сукупність безумовних та умовних оцінок. Умовними виступали наступні характеристики алгоритмів:

- $I_{ст.}$ – рівень криптографічної стійкості;
- $l_{в.к}$ – довжина відкритого ключа;
- $l_{о.к}$ – довжина особистого ключа;
- $l_{рез.}$ – довжина результату криптоперетворення;
- $T_{пр.}$ – швидкість прямого криптоперетворення;
- $T_{зв.}$ – швидкість зворотного криптоперетворення.

Експертні оцінки використовувалися для оцінки важливості кожної наведеної характеристики, а безпосередньо при оцінці алгоритмів використовувалися об'єктивні числові значення, шкала оцінки та вагові коефіцієнти важливості характеристик, що були отримані при експертному оцінюванні (таблиця 4) [3].

Таблиця 4

Експертні оцінки характеристик криптоалгоритмів

Експерти/Показники	**$I_{ст.}$**	**$l_{в.к}$**	**$l_{о.к}$**	**$l_{рез}$**	**$T_{пр.}$**	**$T_{зв.}$**
1	0,316	0,179	0,101	0,045	0,179	0,179
2	0,209	0,342	0,038	0,078	0,124	0,209
3	0,111	0,242	0,027	0,051	0,111	0,457
4	0,107	0,239	0,045	0,107	0,045	0,458
5	0,206	0,125	0,041	0,140	0,171	0,317
W	0,190	0,225	0,050	0,084	0,126	0,324

В цьому дослідженні при виборі алгоритмів висувалися додаткові безумовні вимоги:

1. Алгоритм повинен гарантувати, що найменше 3 рівень безпеки за класифікацією NIST.
2. Якщо існує декілька варіантів наборів параметрів для одного алгоритму, то в порівнянні бере участь варіант, який гарантує найбільшу безпеку.

В таблиці 5 наведені характеристики обраних для порівняння алгоритмів, що засновані на використані перетворень в алгебраїчних решітках [4-5].

Таблиця 5

Характеристики алгоритмів підпису

Алгоритми	**Тип**	**$I_{ст.}$**	**$l_{в.к}$**	**$l_{о.к}$**	**$l_{рез.}$**	**$T_{пр.}$**	**$T_{зв.}$**
Dilithium_very_high	Lattices	3	1 760	3 856	3 366	2 293 141	611 325
DRS256	Lattices	5	14 402 026	144 527	14 421	148 424 947	1 419 704 155
falcon1024	Lattices	5	1 793	8 193	1 330	19 884 364	1 384 574
Gaussian-1024	Lattices	5	2 065	2 604	2 065	349 028 118	2 955 494

Uniform-1024	Lattices	5	2 065	2 604	2 065	202 185 303	2 726 230
falcon768	Lattices	3	1441	6145	1 077	13 058 641	1 117 624
qTesla_256	Lattices	5	8 224	8 256	6 176	8 143 869	1 436 949

У таблиці 6 наведено результати оцінювання вибраних механізмів підпису.

Таблиця 6

Результати оцінювання механізмів підпису

Назва алгоритму	**Значення оцінки**
Dilithium_very_high	0,0964
DRS256	0,0216
falcon1024	0,0715
Gaussian-1024	0,0436
Uniform-1024	0,0468
falcon768	0,0712
qTesla_256	0,0660

Джерело: розробка автора

На рисунку 8 відображено діаграму відносної переваги алгоритмів. Як видно за рисунка, перше місце займає Dilithium_very_high, друге місце ділять falcon1024 та falcon768, а третє місце займає qTesla_256.

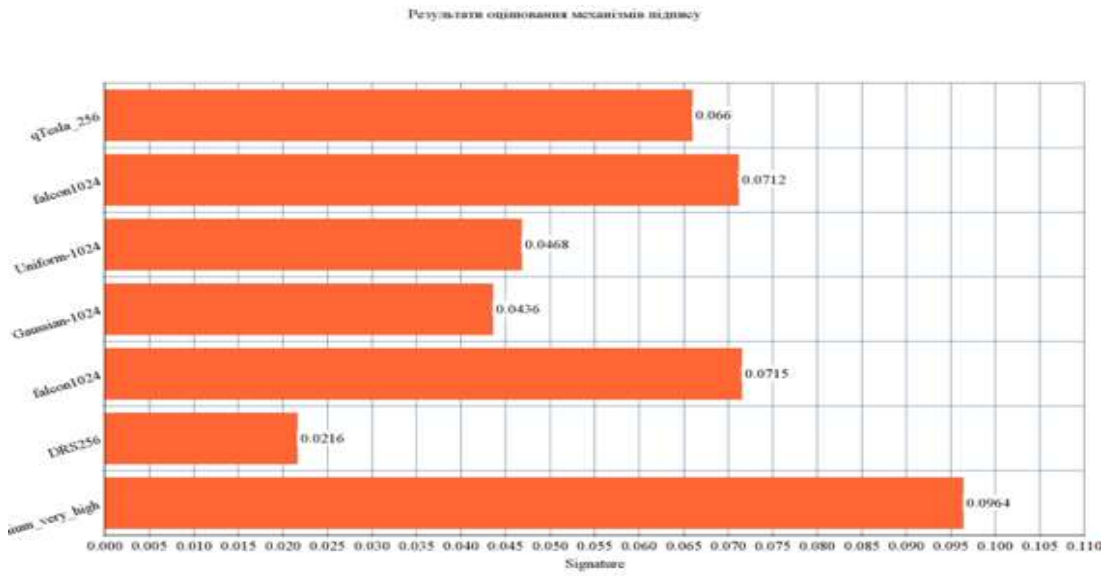

Рис. 8. Відносна перевага алгоритмів підпису

Джерело: розробка автора

Подивимись детально на результати порівняння алгоритмів. Особливістю порівняння стало те, що одразу два алгоритми розділили між собою друге місце, їх відмінність між значеннями була лише у четвертому знаці після коми.

Розглядаючи алгоритми, можна відмітити наступне. Алгоритм falcon768 відрізняється від falcon1024 більш низькою стійкістю на рівні Dilithium_very_high. Falcon1024 має більш високий рівень стійкості, а falcon768 має більш високі інші основні характеристики. Алгоритм qTesla_256 має більші розміри підпису, але все одно не сильно поступається переможцям.

Література

1. Post-quantum crypto project. – Access mode: http://csrc.nist.gov/groups/ST/post-quantum-crypto/index.html.
2. Post-quantum cryptography lounge. [Електронний ресурс] – Режим доступу: https://www.safecrypto.eu/pqclounge/.
3. Yesina Maryna, Gorbenko Yurij (supervisor). Methods of cryptographic primitives comparative analysis // Inżynier XXI wieku ("Engineer of XXI Century" – the VI Inter University Conference of Students, PhD Students and Young Scientists: University of Bielsko-Biala, Poland, December 02, 2016). – Bielsko-Biała: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, 2016. – P. 451–462. – ISBN 978-83-65182-51-7. – Chapter in monograph.
4. Post-Quantum Cryptography [Electronic resource]. – Access mode: https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.
5. NIST Software performance tests [Electronic resource]. – Access mode: https://www.safecrypto.eu/pqclounge/.