УДК 004.056.55

А.С. КИЯН, М.С. ЛУЦЕНКО, А.А. КУЗНЕЦОВ, д-р техн. наук

ПЕРВИННИЙ АНАЛІЗ ТА ДОСЛІДЖЕННЯ КОДОВИХ СХЕМ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ ТА НАПРАВЛЕНОГО ШИФРУВАННЯ З NIST PQC

Вступ

Сьогодні ми живемо на межі зміни епох інформаційної безпеки, оскільки поява повномасштабного квантового комп'ютера, винахід якого анонсовано на найближчі 10 – 15 років, є викликом захищеності сучасних криптографічних систем [1 – 3]. У більшості з існуючих криптографічних механізмів і протоколів задача пошуку секретного ключа за відомим відкритим ключем пов'язана з вирішенням відомої та складної математичної задачі (наприклад, дискретного логарифмування, факторизації тощо). Однак квантові обчислення суттєво прискорюють рішення багатьох математичних задач.

Національний інститут стандартів і технологій (NIST) звернулися до громадськості та оголосили про початок конкурсу для відбору претендентів на стандарти постквантових алгоритмів (Post-Quantum Cryptography, PQC), рішення щодо яких планується прийняти в 2020 – 2022 роках [3].

Нині в межах конкурсу дослідники з усього світу вже представили 82 проекти, 23 з яких обґрунтовують схеми електронного цифрового підпису (ЕЦП), 59 – шифрування та інкапсуляцію ключів. Роботи у сфері постквантової криптографії ведуться у п'яти різних напрямках [1 – 3]:

- криптографія, заснована на геш-функціях (Hash-based cryptography);
- криптографія, заснована на кодах виправляючих помилки (Code –based cryptography);
- криптографія, заснована на решітках(Lattice-based cryptography);
- криптографія, заснована на багатовимірних квадратичних системах (Multivariate cryptography);
- шифрування з відкрити ключем.

Варто відзначити, що найбільше досліджень проводять в області криптографії, заснованої на решітках (всього подано 28 проектів) та на кодах (20 претендентів на стандартизацію) [4].

Особливістю конкурсу, оголошеного NIST, є те, що на нього можуть бути подані алгоритми, які базуються на математичних методах, які є недостатньо випробуваними. Тому дослідження таких алгоритмів щодо їх стійкості до класичного та квантового криптоаналізу потребує значних витрат часу. Вищезгаданий факт обумовлює актуальність всебічного вивчення представлених проектів, їх порівняльний аналіз, а також оцінку їх захищеності. В межах даної роботи ми обмежимося дослідженням алгоритмів ЕЦП та направленого шифрування, що засновані на кодах, проведемо їх первинний аналіз та систематизацію.

Характеристика проектів кодових схем ЕЦП

На сьогодні авторами представлено три різних схеми формування та перевірки ЕЦП, алгоритми яких базуються на кодових криптосистемах: pqsigRM, RaCoSS, RankSign. Розглянемо поступово кожну з цих схем.

Схема pqsigRM. Схему pqsigRM було розроблено групою дослідників з Кореї: Wijik Lee, Young-Sik Kim,Yong-Woo Lee та Jong-Seon No [5]. Вона ґрунтується на коді Ріда – Мюллера (РМ), покращуючи схему підпису на основі кодів Гоппа, розроблену свого часу Courtois, Finiasz та Sendrier (CFS) [1]. Перевагами даного алгоритму є контрольований час підписання. У порівнянні з CFS час підпису не залежить від можливості виправлення помилок t. Також час підпису та рівень безпеки контролюється завдяки налаштуванню параметрів. Управління

відношенням між часом підпису та рівнем безпеки здійснюють завдяки змінам параметрів N і w, де N – очікувана кількість ітерацій, w – параметр ваги похибок. Обмеження pqsigRM – це відносно великий розмір відкритого ключа, оскільки код РМ не квазіциклічний, розмір відкритого ключа дорівнює (n – k) × k (де n, k – параметри коду). У проекті представлено експерименти щодо ефективності підпису для різних рівнів безпеки, а саме 128, 196,256, які, як відомо, позначають, що з метою подолання захисту необхідно здійснити 2^{128},2^{196} та 2^{256} операцій відповідно [5].

Схема RacoSS. Назва цього алгоритму розшифровується як Random Code-based Signature Scheme, що в перекладі означає: «Випадкова схема підпису, заснована на кодуванні» [4]. Вона є здобутком спільної роботи японських дослідників (Partha Sarathi Roy, Rui Xu, Kazuhide Fukushima, Shinsaku Kiyomoto, Tsuyoshi Takagi) та вченого з американського університету (Kirill Morozov). Представлено дві версії реалізації цієї схеми: довідкова та оптимізована, перша з яких призначена для покращення розуміння функціонування алгоритму, а друга-для демонстрації продуктивності.

Авторами зазначаються такі переваги RacoSS:

– RaCoSS виявився стійким та екзистенційно непідробним в умовах атаки обраного повідомлення;
– підпис має невеликий розмір у порівнянні з іншими схемами підпису на основі кодування, за виключенням схеми підпису CFS з 81-бітовою безпекою. Але, розміри ключів CFS значно більші, ніж потребує RaCoss;
– процеси, виконувані у алгоритмі (формування ключів, перевірка та формування підпису), можуть бути легко прискорені паралельними обчисленнями.

Незважаючи на всі переваги схеми, вона має також суттєвий недолік: діапазон підпису обмежений [4].

Схема RankSign. Криптосистема RankSign була представлена у 2014 року [4]. Її розробниками виступили Nicolas Aragon, Olivier Ruatta, Philipp e Gaborit, Gilles Zémor та Adrien Hauteville. Ця схема підпису заснована на коді в ранговій метриці. Загальною ідеєю є використання коду LRPC (який є еквівалентом для MDPC в метриці Хеммінга або NTRU в евклідовій метриці) як лазівки для обчислення помилки пов'язаної з повідомленням. Головна проблема цієї криптосистеми полягала у тому, що ймовірність розрізнення підпису та випадкового вектора дорівнювала 2/q (де q – степінь основи поля Fq), тобто повинно використовуватися дуже велике значення q. Через це на конкурс було представлено модифіковану версію RankSign, де додатково відбувається додавання невеликої випадкової помилки до підпису, тобто це дозволяє зменшити спроможність зловмисника розрізнити підписи. Схема підпису має невеликі параметри і є відносно швидкою. Оскільки нам потрібно взяти велике значення q, всі відомі комбінаторні атаки є недієвими для порушення стійкості RankSign. Таким чином, найкращі атаки на неї ґрунтуються на розрахунках Грейбнера. У оцінці безпеки не враховується просторова складність цих алгоритмів, оскільки, зараз не існує квантового прискорення для них, автори очікують, що параметри будуть досить стійкими [4].

Порівняльний аналіз представлених алгоритмів ЕЦП

Порівняльний аналіз представлених алгоритмів ЕЦП доцільно провести з точки зору їх швидкодії та довжини параметрів. У табл. 1 наведено значення основних параметрів для різних версій алгоритмів з різними рівнями забезпечуваної безпеки. З метою продемонструвати значення більш наглядно довжини наведено у байтах.

Продемонструємо дані, наведені у таблиці, за допомогою графіків (рис. 1 – 3) в логарифмічному масштабі. Сутність використання такого масштабу полягає в перетворенні довжин даних наступним чином: $x = \log_{10} X$, де: X – параметр, такий як довжина

відкритого або особистого ключа, довжина шифротекста, яка підлягає масштабуванню; x – результат обчислення десяткового логарифма над масштабованим значенням.

Таблиця 1

Характеристика основних криптографічних параметрів ЕЦП

№	Назва	Версії	Рівень безпеки	Секретний ключ, байт	Відкритий ключ, байт	Підпис, байт
1	pqsigRM	/pqsigRM-4-12	1	1382118	336804	260
		/pqsigRM-6-12	3	334006	501176	516
		/pqsigRM-6-13	5	2105344	2144166	1028
2	RacoSS	Reference	-	703000	99600	586
		Optimized	-	703000	99600	586
3	RankSign	RankSign I	1;$q=2^{32}$	-	80640	11008
		RankSign II	1; $q=2^{24}$	-	96768	12000
		RankSign III	3; $q=2^{32}$	-	155520	17280
		RankSign IV	5; $q=2^{32}$	-	228480	23424

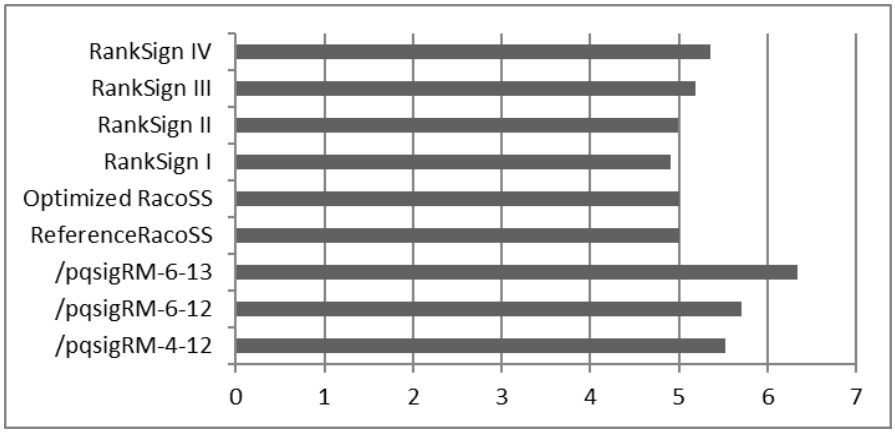

Рис. 1. Порівняння довжин відкритого ключа (в байтах, логарифмічний масштаб) різних схем ЕЦП

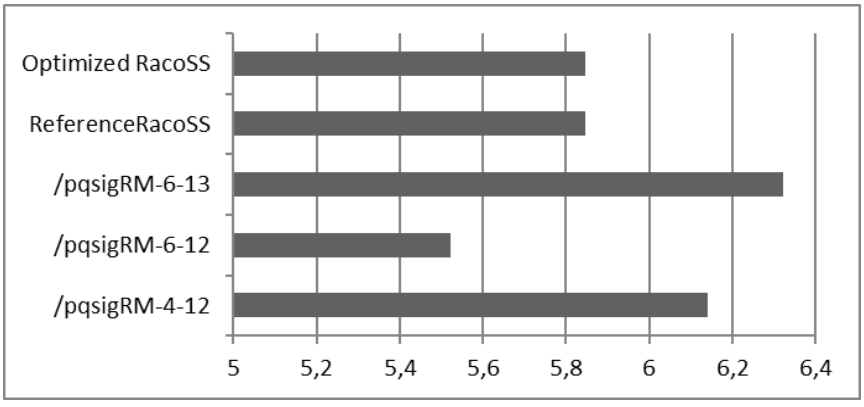

Рис. 2. Порівняння довжин секретного ключа (в байтах, логарифмічний масштаб) різних схем ЕЦП

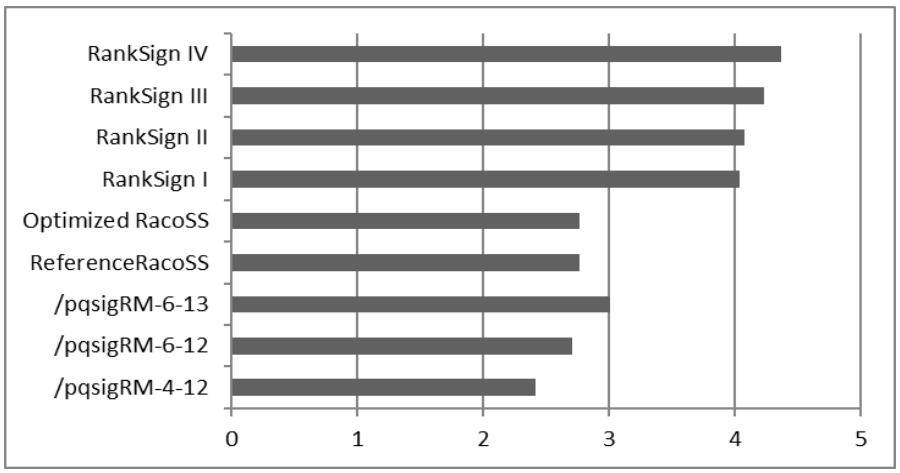

Рис. 3. Порівняння довжин сформованого підпису (в байтах, логарифмічний масштаб) різних схем ЕЦП

Аналізуючи отримані дані, можна зазначити, що для версії алгоритму pqsigRM-6-13 довжини відкритого та секретного ключів найбільші, при цьому довжина шифртексту для даної схеми приймає одне з найменших значень. Дослідити довжину секретного ключа схеми RankSign не вдалося, оскільки вона не передбачає використання секретного ключа. Найбільша довжина шифртексту відповідає алгоритму RankSign і зі зростанням рівня безпеки, що надає ця схема, довжина шифртексту збільшується, як і довжина відкритого ключа.

У табл. 2 наведено показники швидкості генерації ключів, формування і верифікації підпису, а також зазначена обчислювальна платформа, яка використовувалась при випробувані схем. Дані швидкості, що були надані у мілісекундах, зведені до кількості циклів з урахуванням особливостей конкретної обчислювальної платформи.

Таблиця 2

Показники швидкодії алгоритмів ЕЦП

№	Назва	Обчислювальна платформа	Версії	Генерація ключових даних,цикл	Формування підпису, цикл	Верифікація підпису, цикл
1	pqsigRM	Intel(R) Xeon(R) CPU E5-2698 v4 (2,2 ГГц)	/pqsigRM-4-12	9641836	15194705	81178
			/pqsigRM-6-12	1983428	77735436	116906
			/pqsigRM-6-13	22668519	1557210	540378
2	RacoSS	Intel Core i7-4770K CPU (3,50 ГГц)	Reference	24815000000	60900000	31850000
			Optimized	840000000	22680000	213150000
3	RankSign	Intel(R) Core™ i7-4700HQ (3,4 ГГц)	RankSign I	190000000	18600000	7300000
			RankSign II	432000000	33100000	13600000
			RankSign III	537000000	43100000	17500000
			RankSign IV	1030000000	67800000	28200000

Представимо отримані результати за допомогою графічного зображення (рис. 4). Оскільки показники для різних схем різняться в десятки разів, для кращого сприйняття дані наведені у логарифмічному масштабі.

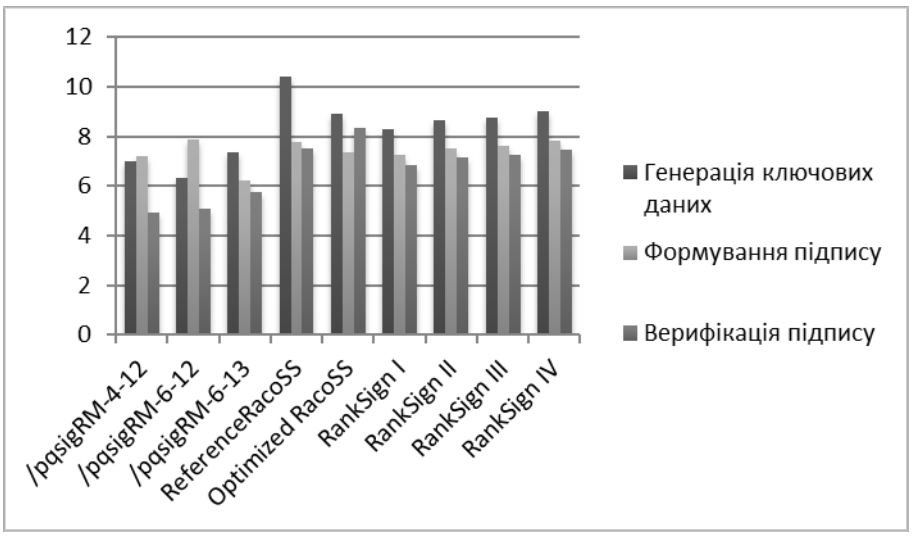

Рис. 4. Показники на швидкості усіх етапах алгоритмів

З точки зору швидкодії очевидно, що більш продуктивним буде той алгоритм, показники для якого більші. Аналізуючи гістограми, бачимо, що оптимізована версія RacoSS (Optimized RacoSS) є найбільш швидкою з усіх представлених алгоритмів. Тоді як схема підпису pqsigRM для різних своїх версій продемонструвала порівняні показники, що є на порядок меншими за швидкість RankSign та RacoSS.

Характеристики проектів направленого шифрування

По результатах аналізу наданих на конкурс проектів було виділено п’ять кодових схеми направленого шифрування: BIG QUAKE [6], HQC [7], LEDApkc [8], LOCKER [4] та McNie [4].

Схема шифрування BIG QUAKE. У рамках проекту запропоновано схему шифрування з відкритим ключем, яка перетворюється в механізм інкапсуляції ключів [6]. Автори проекту (Alain Couvreur, Magali Bardet, Elise Barelli, Olivier Blazy, Rodolfo Canto-Torres, Philippe Gaborit, Ayoub Otmani, Nicolas Sendrier, Jean-Pierre Tillich) передбачають використання у даній схемі двійкових кодів Гоппа. BIQ QUAKE побудовано як і схему Нідеррайтера, але у порівнянні з оригінальною схемою ця пропозиція уникає обчислення бієкції між словами фіксованої довжини та словами із постійною вагою. Це дозволяє уникнути громіздких обчислень, що стосуються великих цілих чисел, і робить схему більш придатною для вбудованої системи з обмеженими обчислювальними ресурсами [6].

Схема шифрування HQC. Авторами схеми шифрування виступили Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor [7]. Назва HQC є абревіатурою Hamming Quasi-cyclic, що передбачає використання квазіциклічного коду Хеммінга. HQC – криптосистема з відкритим ключем на основі коду з декількома корисними властивостями:

- за конструкцією HQC дозволяє отримати гібридну схему шифрування з сильними гарантіями безпеки (IND-CCA2) і високою економічністю;
- на відміну від більшості криптосистем, що базуються на кодах, припущення про те, що сімейство кодів, що використовуються, не розрізняється серед випадкових кодів, більше не потрібно;
- схема має аналіз вірогідності помилок дешифрування.

Основними перевагами HQC над існуючими криптосистемами, заснованими на кодах, як стверджують автори, є:

– зменшення її IND-CPA до добре зрозумілих проблем теорії кодування: проблема дешифрування квазіциклічного синдрому;
– стійкість проти атак, спрямованих на відновлення прихованої структури коду, що використовується;
– закриті оцінки невдалого розшифрування.

Серед обмежень криптосистеми можна виділити низькі оцінки шифрування. Можливо зашифрувати 256 біт відкритого тексту, як того вимагає NIST, але збільшуючи об'єм потрібно збільшувати також і параметри [7].

Схема LEDApkc. Цей проект представила група італійських дослідників: Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, Gerardo Pelosi, Paolo Santini [8]. LEDApkc – це криптосистема з відкритим ключем, побудована на кшталт криптосистеми Мак-Еліса на основі лінійних виправляючих помилки кодів. Зокрема, ця схема використовує переваги перевірки парності з низькою щільністю, що забезпечує високу швидкість перетворень та компактність ключових пар. Серед переваг схеми LEDApkc можна виділити наступні:
– побудована на NP-повній проблемі;
– компактні ключові пари (не більше 23 кбітів), секретні ключі мінімального розміру;
– потребує лише операцій додавання та множення у полі $F_{2\,[x]}$;
– повна патентована, автономна, відкрита кодова база даних, написана на ANSI-C99, її легко інтегрувати в існуючі криптографічні бібліотеки [8].

Схема LOCKER. Головними розробникам схеми шифрування LOCKER є Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philipp e Gaborit, Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich та Gilles Zémor [4]. Пропозиція заснована на варіаціях підходу LRPC. Схема ефективна з точки зору величини параметрів та обчислюваної складності, яка користується властивостями рангової метрики. LOCKER має імовірність відмови, але ця імовірність обґрунтована і може бути дуже низькою від 2^{-64} до 2^{-128}.

Запропонована схема дуже ефективна, як з точки зору розміру ключів, так і обчислювальної складності. Також позитивним моментом є те, що вибір параметрів носить універсальний характер.

Схема McNie. Авторами гібридної схеми, що об'єднає елементи криптосистеми McElice та Niderreiter, є корейські вчені Lucky Galvez, Jon-Lark Kim, Myeong Jae Kim, Young-Sik Kim, Nari Lee [4]. У порівнянні з іншими схемами шифрування McNie забезпечує значно менші розміри відкритих ключів, які збільшуються з більш поступовим темпом зі збільшенням рівня безпеки.

McNie може використовувати різноманітні види відомих блокових кодів в якості вхідних даних, навіть незважаючи на те, що криптосистема McEliece на основі цих кодів була порушена. Причина в тому, що McNie використовує випадковий код, що є більш безпечним, ніж у криптосистемі McEliece. Також завдяки використанню випадкового коді McNie захищений від структурних атак та атак з набором декодованої інформації [4].

Порівняльний аналіз представлених схем направленого шифрування

Порівняльний аналіз представлених на конкурс схем шифирування, як і схем формування ЕЦП, доцільно буде здійснити за двома критеріями: довжинами основних криптографічних параметрів, а також показниками щвидкодію, яку забезпечують кожен з алгоритмів.

У табл. 3 наведено показники довжин секретного, відкритого ключа, а також шифртексту для різних версій представлених схем шифрування, що надають різні рівні безпеки.

Таблиця 3

Характеристика основних криптографічних параметрів схем шифрування

№	Назва	Версії	Рівень безпеки		Секретний ключ, байт	Відкритий ключ, байт	Шифртекст, байт
1	Big Quake	Big Quake-1	1		14772	25482	201
		Big Quake-3	3		30860	84132	406
		Big Quake-5	5		41804	149800	492
2	HQC	Basic- I	1; $P_{пом} \le 2^{-64}$		40	2819	5662
		Basic- II	1; $P_{пом} \le 2^{-96}$		40	3009	6002
		Basic- III	1; $P_{пом} \le 2^{-128}$		40	3125	6234
		Advanced- I	3; $P_{пом} \le 2^{-64}$		40	5115	1021
		Advanced- II	3; $P_{пом} \le 2^{-128}$		40	5499	10982
		Advanced- III	3; $P_{пом} \le 2^{-192}$		40	5884	11752
		Paranoic- I	5; $P_{пом} \le 2^{-64}$		40	7417	14818
		Paranoic-II	5; $P_{пом} \le 2^{-128}$		40	7989	15962
		Paranoic- III	5; $P_{пом} \le 2^{-192}$		40	8503	16990
		Paranoic- IV	5; $P_{пом} \le 2^{-256}$		40	8897	17778
3	LEDApkc	LEDApkc-1	1	$n_0=2$	3480	668	6960
				$n_0=3$	4688	844	7032
				$n_0=4$	6408	1036	8544
		LEDApkc-3	2-3	$n_0=2$	7200	972	14400
				$n_0=3$	10384	1196	15576
				$n_0=4$	13152	1364	17536
		LEDApkc-5	4-5	$n_0=2$	12384	1244	24768
				$n_0=3$	18016	1548	27024
				$n_0=4$	22704	1772	30272
4	LOCKER	LOCKER I	1		-	736,625	800,625
		LOCKER II	3		-	1047,875	1111,875
		LOCKER III	5		-	1190,375	1252,875
		LOCKER IV	1		-	997,375	1061,375
		LOCKER V	3		-	1248,875	1312,875
		LOCKER VI	5		-	1377,625	1441,625
		LOCKER VII	1		-	1545,875	1609,875
		LOCKER VIII	3		-	1881,125	1945,125
		LOCKER IX	5		-	2139,125	2203,125
5	McNie	McNie-1	1		401	417	422
		McNie-3	3		512	539	651
		McNie-5	5		601	647	781

Представимо дані таблиці за допомогою схематичного зображення (рис. 5 – 7). На графіках позначено тільки по три версії кожного алгоритму для кращого візуального сприйняття. Було обрано ті варіанти схем шифрування, що забезпечують різні рівні безпеки.

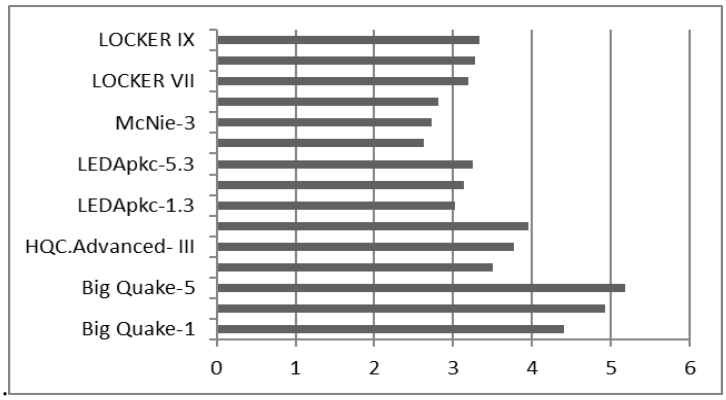

Рис. 5. Порівняння довжин відкритих ключів (в байтах, логарифмічний масштаб) різних схем шифрування

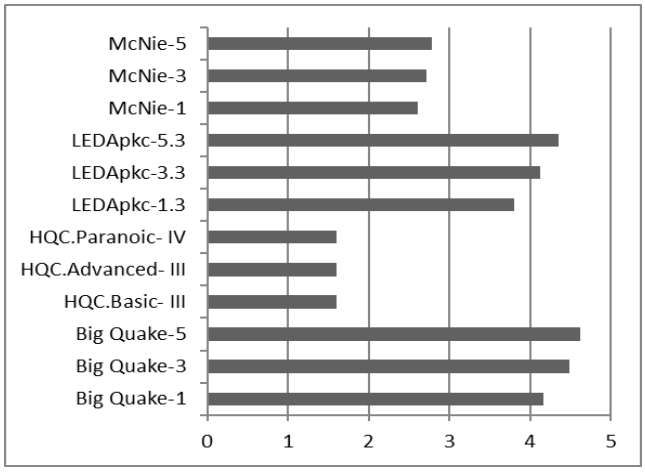

Рис. 6. Порівняння довжин секретних ключів (в байтах, логарифмічний масштаб) різних схем шифрування

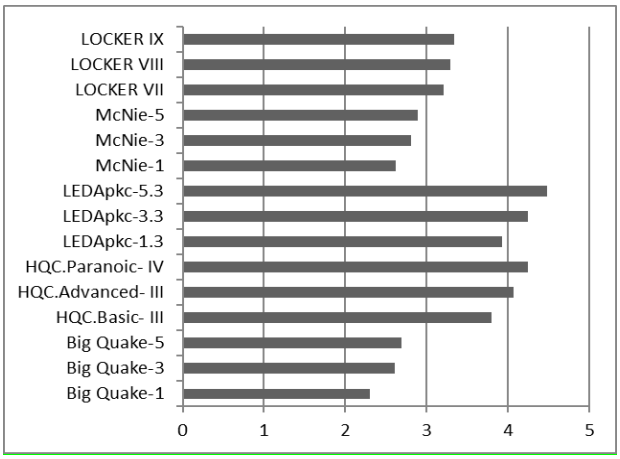

Рис. 7. Порівняння довжин шифртексту (в байтах, логарифмічний масштаб) різних схем шифрування

Аналізуючи отримані результати, варто зазначити, що довжини відкритого ключа та шифртексту для алгоритму Big Quake є найбільшими. McNie напроти демонструє найменші показники для усіх трьох параметрів, при тому що здатен забезпечувати п’ятий рівень безпеки, як і інші схеми.

Наступним кроком дослідимо швидкодію розглянутих вище схем шифрування, що представлені на конкурс. Вивчається швидкість трьох етапів алгоритмів: генерація ключових

даних, шифрування та розшифрування. Отримані результати представлені у табл. 4. Дані, що були надані у мілісекундах, було зведено до кількості циклів, які потребує виконання алгоритму з урахуванням особливостей використовуваної обчислювальної платформи.

Таблиця 4

Показники швидкодії схем шифрування

№	Назва	Обчислювальна платформа	Версії	Генерація ключових даних,цикл	Шифрування, цикл	Дешифрування, цикл
1	Big Quake	Intel(R) Xeon™ E3-1240v5 (3,5 ГГц)	Big Quake-1	268000000	4305000	4935000
			Big Quake-3	8641500000	10500000	31885000
			Big Quake-5	16509500000	15610000	47950000
2	HQC	Intel(R) Core™ i7-4770 (3.4ГГц)	Basic- I	578000	1224000	1938000
			Basic- II	612000	1292000	2074000
			Basic- III	646000	1360000	2142000
			Advanced- I	1258000	2618000	3842000
			Advanced- II	1360000	2822000	4114000
			Advanced-III	1462000	3026000	4352000
			Paranoic- I	2210000	4692000	6664000
			Paranoic-II	2584000	5440000	7548000
			Paranoic-III	2652000	5610000	7990000
			Paranoic-IV	2788000	5984000	850000
3	LEDApkc	AMD Ryzen 5 1600 CPU (3.2 ГГц)	1	144960000	9952000	66784000
				67072000	9300000	80576000
				57568000	12608000	90560000
			2-3	635168000	38592000	200160000
				321248000	41792000	184256000
				232896000	45376000	191200000
			4-5	1788288000	108672000	369152000
				956512	119296000	374176000
				668480000	127520000	503136000
4	LOCKER	IntelR Core TMi7-4700HQ CPU(3,4 ГГц)	LOCKER-I	2710000	550000	2570000
			LOCKER-II	3190000	540000	1080000
			LOCKER-III	3580000	600000	3770000
			LOCKER-IV	3720000	710000	2860000
			LOCKER-V	4360000	860000	4320000
			LOCKER-VI	4680000	750000	4060000
			LOCKER-VII	8440000	1350000	4780000
			LOCKER-VIII	9480000	1390000	5000000
			LOCKER-IX	10400000	1490000	6600000
5	McNie	Intel Core i7-4790 (3.6 ГГц)	McNie-1	280800000	2444400	5788800
			McNie-2	511200000	3492000	8445600
			McNie-3	668880000	4287600	10342800

Продемонструємо наведені результати у графічному вигляді (рис. 8 – 11). Варто зазначити, що через те, що дані для різних алгоритмів різняться в сотні разів, графіки було побудовано з використанням логарифмічного масштабу.

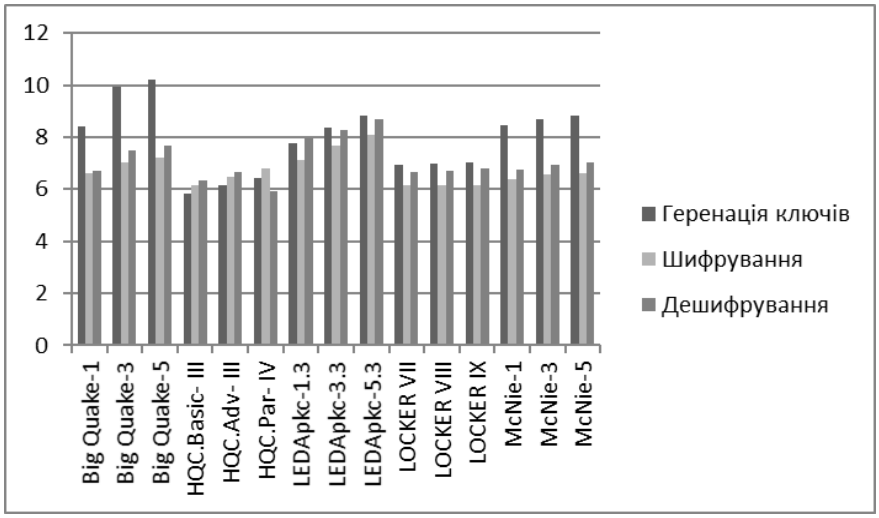

Рис. 8. Гістограма показників швидкодії схем шифрування (логарифмічний масштаб)

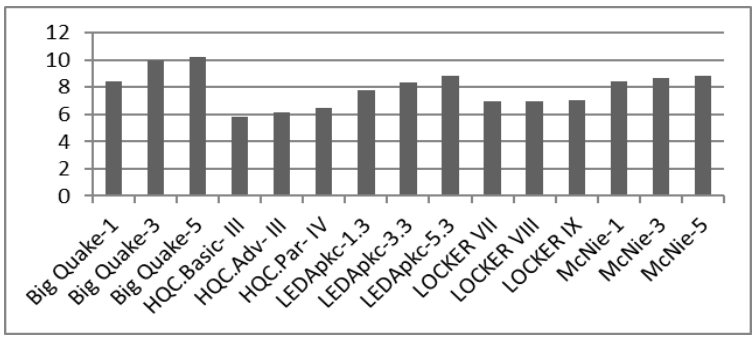

Рис. 9. Порівняння показників швидкості генерації ключових даних різних схем шифрування (логарифмічний масштаб)

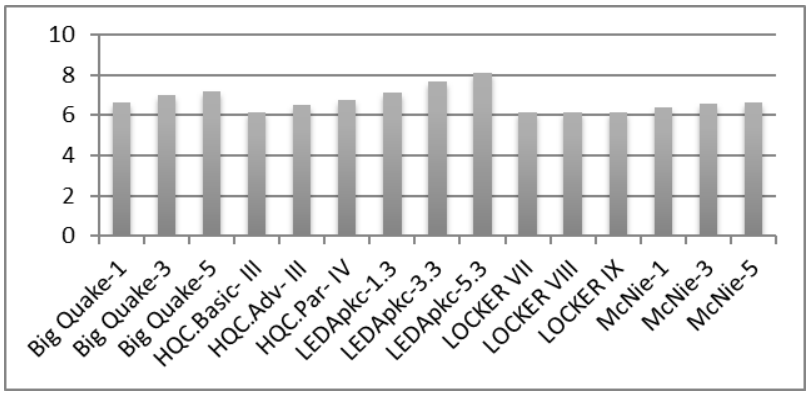

Рис. 10. Порівняння показників швидкості шифрування різних схем шифрування (логарифмічний масштаб)

Big Quake надає найбільшу швидкість генерації ключів. Приблизно порівняні результати показали алгоритми McNie та LEDApkc, тоді як версії алгоритму HQC забезпечують найменшу швидкодію з усіх розглянутих схем. Отже, Big Quake надає найбільшу швидкість генерації ключів, тоді як версії алгоритму HQC забезпечують меншу швидкодію, порівняно з іншими алгоритмами.

Аналізуючи дані, бачимо, що швидкість шифрування досить висока у всіх схем шифрування, але LEDApkc-5.3 забезпечує найкращі показники.

Швидкість дешифрування порівняна у алгоритмів McNie, Big Quake та HQC, тоді як показники LEDApkc є найкращими.

Швидкість дешифрування порівняна у алгоритмів McNie, Big Quake та HQC, тоді як показники LEDApkc є найкращими.

Отже, з точки зору швидкодії, найефективнішою з представлених схем є схема LEDApkc у всіх її варіантах, а HQC, у свою чергу, показала найгірші результати.

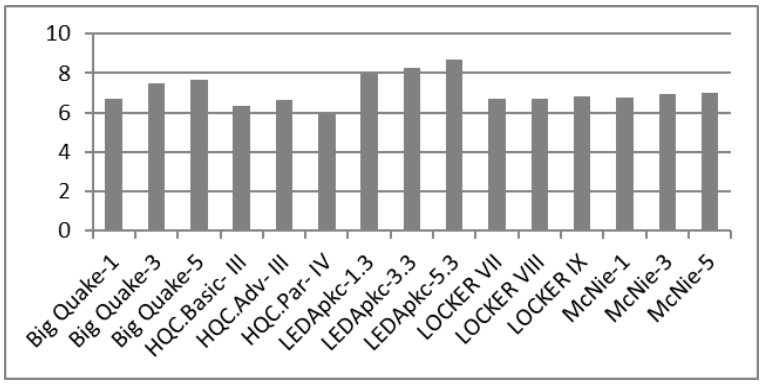

Рис. 11. Порівняння показників швидкості дешифрування різних схем шифрування (логарифмічний масштаб)

Висновки

Висока імовірність появи повномасштабного квантового комп'ютера в найближчі роки обумовлює зростання актуальності досліджень в області постквантової криптографії з метою стандартизації нових алгоритмів, що будуть здатні залишатися стійкими в умовах застосування квантових обчислень. Національний інститут стандартів і технологій США оголосив про початок конкурсу для відбору претендентів на стандарти постквантових алгоритмів, рішення щодо яких планується прийняти в 2020 – 2022 роках. На сьогодні у рамках конкурсу подано 82 проекти.

Криптографія, що ґрунтується на кодах, нині вважається одним з найперспективніших напрямків. Це підтверджується тим, що з 82 проектів, представлених на конкурс, 20 базуються саме на кодах. Серед них три схеми формування та верифікації електронного цифрового підпису, п'ять схем шифрування та дванадцять механізмів інкапсуляції ключів.

В цій роботі алгоритми формування підпису і схеми направленого шифрування порівняно за двома критеріями: за довжинами основних криптографічних параметрів та за показниками швидкодії, які забезпечує кожен з алгоритмів. З точки зору швидкодії, найефективнішою виявилась схема направленого шифрування LEDApkc та алгоритм формування електронного цифрового підпису RacoSS. Використовуючи перший критерій порівняння, найкращі показники продемонстрували pqsigRM та McNie для формування ЕЦП та шифрування відповідно.

Слід відмітити, що наведені оцінки спираються на дані, що були надані безпосередньо авторами проектів, тобто вважати їх повністю об'єктивними неможливо. Для всебічного дослідження з метою стандартизації вичерпний аналіз триватиме роками і це є перспективним напрямком подальших робіт.

Список літератури:

1. Bernstein D., Buchmann J. and Dahmen E. Post-Quantum Cryptography. Springer-Verlag, Berlin-Heidleberg, 2009. 245 p.

2. Koblitz N. and Menezes A.J.. A Riddle Wrapped in an Enigma. [Електронний ресурс] URL: https://eprint.iacr.org/2015/1018.pdf, Oct. 20, 2015 [Aug. 21, 2016]

3. Moody D. Post-Quntum Cryptography: NIST's Plan for the Future. The Seventh International Conference on Post-Quntum Cryptography, Japan, 2016. [Електронний ресурс] URL: https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf [March 8, 2016].

4. Computer Security Resource Center [Електронний ресурс] URL: https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions

5. A modified RM code-based post-quantum digital signature algorithm [Електронний ресурс]. URL: https://sites.google.com/view/pqsigrm/home

6. Binary Goppa QUAsi-cyclic Key Encsapulation [Електронний ресурс] URL: https://bigquake.inria.fr/

7. Hamming Quasi-Cyclic [Електронний ресурс]. URL: http://pqc-hqc.org/

8. LEDApkc Public Key Cryptosystem [Електронний ресурс]. URL: https://www.ledacrypt.org/LEDApkc/

Харківський національний
університет імені В.Н.Каразіна

Надійшла до редколегії 10.03.2018