УДК 003.026:004.056

ПОРІВНЯННЯ КАНДИДАТІВ ЕЛЕКТРОННОГО ПІДПИСУ НА ПОСТКВАНТОВИЙ СТАНДАРТ NIST PQC НА БАЗІ MQ-ПЕРЕТВОРЕНЬ ТА ФУНКЦІЙ ҐЕШУВАННЯ

Ю. І. ГОРБЕНКО, І. С. КУДРЯШОВ, Д. С. НАУМЕНКО, В. В. ОНОПРІЄНКО

Наводяться результати порівняльного аналізу кандидатів на стандарти перспективних електронних підписів, що будуються на основі мультиваріативних квадратичних перетворень та функцій ґешування. Результати аналізу отримані в ході використання методики порівняння криптографічних механізмів на основі експертних оцінок за сукупністю умовних та безумовних критеріїв. Зроблено рекомендації щодо перспектив застосування кандидатів.

Ключові слова: MQ-перетворення, постквантовий алгоритм, електронний підпис, порівняльний аналіз, експертні оцінки, підпис на основі ґеш-функцій.

ВСТУП

Наприкінці 2016 року NIST США оголосив конкурс на нові стандарти постквантової асиметричної криптографії [1], зокрема, механізми електронного підпису (ЕП), направленого шифрування (НШ) та протоколи інкапсуляції ключів (ПІК). Необхідність їх розробки викликана суттєвим розвитком квантових обчислень – математичних квантових методів та квантових комп'ютерів, що можуть бути застосованими для криптоаналізу асиметричних криптоперетворень [2–22].

Серед поданих на конкурс кандидатів на стандарт ЕП значне число розроблено на основі застосування мультиваріативних квадратичних перетворень (Multivariate Quadratic Transformations, MQ-transformations) [2–10]. Перше за все механізми MQ-перетворень дозволяють забезпечити необхідні рівні стійкості, швидкодію та застосування в малоресурсних системах, а також можуть застосовуватися у загальному випадку. Властивості MQ-перетворень мають суттєве значення для практичних додатків, тому їхній аналіз та порівняння є важливою проблемною задачею, тим більше що вона вирішується NIST США на міжнародному рівні. Аналіз показав, що на конкурс NIST було подано 9 кандидатів ЕП на основі MQ-перетворень, а саме: LUOV [2], Gui [3], Rainbow [4], MQDSS [5], TPSig [6], DualModeMS [7], HiMQ-3 [8], GeMSS [9] та DME [10].

Також теоретичне та практичне визнання, як кандидати на стандарт отримали ЕП, що будуються на основі функцій ґешування та дереві Мерклі. Але проблемою є те, що реалізація таких криптосистем ЕП вимагає для створення нової інфраструктури відкритого ключа. Як показав аналіз конкурентними як кандидати на ЕП є Gravity-SPHINCS [11] та SPHINCS$^+$ [12].

Зрозуміло, що при такій значній наявності кандидатів на постквантовий стандарт ЕП, неохдно проводити їх порівняння за значною кількістю безумовних та умовних критеріїв [20–22].

Метою цієї статі є порівняльний аналіз кандидатів на постквантові стандарти ЕП, як всередині груп ЕП на основі певних математичних методів, так між ними, в даному випадку, що ґрунтуються на застосуванні мультиваріативних квадратичних перетворень та гешфункцій.

Таким чином, у цій статті наводяться початкові результати порівняльного аналізу кандидатів на постквантові стандарти ЕП. Під час досліджень за основу вибрані джерела [1–19], а також наша стаття [20].

1. СУТНІСТЬ ТА ЗАГАЛЬНА ХАРАКТЕРИСТИКА MQ-МЕХАНІЗМІВ

Серед кандидатів на асиметричні перетворення типу АСШ, ЕП та ПІК 10 грунтуються на механізмах багатовимірних MQ-перетворень [1–11, 20]. Аналіз показує, що багатовимірна MQ криптографія ґрунтується на складності вирішення задач, які пов'язані з багатовимірними поліномами над кінцевими полями та вирішенням систем багатовимірних поліноміальних рівнянь. Основними особливостями MQ-перетворень є невеликі, порівняно з іншими, складність асиметричних перетворень та невеликі обчислювальні ресурси здійснення перетворень. Як наслідок, вказане дозволяє реалізувати MQ-перетворення у відносно простих засобах ЕП.

Розглянемо сутність MQ-перетвореннння. Нехай F_q є скінченне поле з q елементами. Також нехай система мультиваріативних квадратичних поліномів $P=(P^{(1)},...,P^{(m)})$, з m рівняннями та n змінними визначена як:

$$P^{(k)}(x_1,...,x_n)=\sum_{i=1}^{n}\sum_{j=1}^{n}\gamma_{ij}^{(k)}x_ix_j+\sum_{i=1}^{n}\beta_i^{(k)}x_i+\alpha_0^{(k)},$$

$$k=1...m,\gamma_{ij}^{(k)},\beta_i^{(k)},\alpha_0^{(k)}\in F_q. \quad (1)$$

Основна ідея для конструкції MQ-схем полягає у тому, що необхідно обрати секретну систему $F=(F^{(1)},...,F^{(m)}):F_q^n\to F_q^m$ (так зване центральне відображення), яка складається з m мультиваріативних

квадратичних поліномів, n змінних, яка може бути інвертована з поліноміальною складністю.

Для того, щоб сховати структуру центрального відображення F у публічному ключі, необхідно також обрати два афінних лінійних відображення $S: F_q^m \to F_q^m$ та $T: F_q^n \to F_q^n$. Як публічний ключ використовується композиція квадратичних відображень $P = S \circ F \circ T$, яку важко відрізнити від випадкової системи і тому складно інвертувати. Як приватний ключ використовується сукупність відображень (S, F, T), знаючи які можна інвертувати публічний ключ P.

Послідовність (схема) генерації та перевірки ЕП [8], що базується на MQ-перетвореннях, наведено на рис. 1.

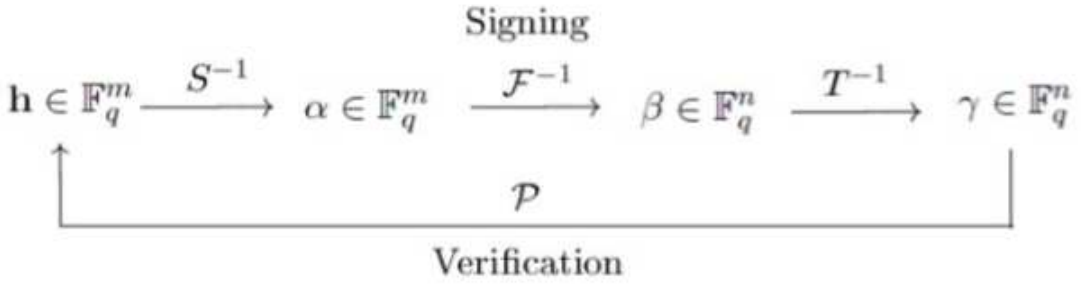

Рис. 1. Схеми створення та перевірки підпису на основі MQ-схеми

2. СУТНІСТЬ ТА ЗАГАЛЬНА ХАРАКТЕРИСТИКА ЕП НА ОСНОВІ ФУНКЦІЙ ҐЕШУВАННЯ

Спираючись на роботу Лемпорта [13], Діффі та Геллман запропонували одну з найпростіших схем підпису на основі ґеш-функцій[14–18]. В схемі задано параметр безпеки n та однонаправлену функцію $F: \{0,1\}^n \to \{0,1\}^n$. Сама схема використовується для підписання одного біту. Секретний ключ складається з випадкових значень $x_0, x_1 \in \{0,1\}^n$. Відкритий ключ складається з ґеш значень елементів секретного ключа – $(y_0, y_1) \coloneqq (F(x_0), F(x_1))$. Підпис σ біту b складається з відповідного значення секретного ключа: $\sigma = x_b$. Перевірка підпису виконується шляхом визначення ґеш значення підпису та перевірки виконання умови $y_b = F(\sigma)$.

Авторами роботи було також запропоновано використовувати m реалізацій описаної вище схеми для підписання повідомлення довжиною m біт. За допомогою такої схеми неможливо підписати повідомлення, довжина якого більше m біт. Для вирішення цієї проблеми було запропоновано таку конструкцію: стійка до колізій ґеш функція H, з довжиною вихідного значення m біт, застосовується до повідомлення M, у результаті чого отримується ґеш значення $h = H(M)$ довжиною m біт. Отримане значення підписується за допомогою схеми, яку було описаною вище.

Така схема є одноразовою, в ній кожна ключова пара може використовуватися для підписання лише одного повідомлення. Іншим прикладом схеми одноразового підпису є підпис Вінтерніца.

Основна ідея схеми одноразового підпису Вінтерніца (Winternitz one-time signature scheme – WOTS) вперше була запропонована Мерклєм. Базуючись на його роботі Вінтерніц удосконалив схему. Для n-бітного простору повідомлень обираються параметри ℓ та w такі, що $\ell \cdot \log_2 w = n$. Секретний ключ схеми є собою ℓ n-бітними рядками $(s_1, \dots, s_\ell)$, а відкритим ключем є $\left(F^{w-1}(s_1), \dots, F^{w-1}(s_\ell)\right)$, де F^{w-1} означає застосування функції F до секретного ключа $w-1$ раз. Цю конструкцію можна розглядати як ℓ ланцюгів, кожен з яких має довжину $w-1$. Для підписання повідомлення x, яке розбито на ℓ блоків довжиною $\log_2 w$ біт $(x_1, \dots, x_\ell)$, підписувач обчислює $\left(F^{x_i}(s_1)\right)_{1 \le i \le \ell}$. Перевірка виконується шляхом обчислення $F^{w-1-x_i}(y_i)$ для кожного елементу підпису y_i, та порівняння результату з відповідним елементом відкритого ключа $F^{w-1}(s_i)$.

Існують декілька варіантів ланцюгової функції F^i: WOTS^{CR}, WOTS^{PRF}, WOTS^{+}. В [14] було запропоновано WOTS^{+}, де в кожній ітерації використовується випадкова маска r_i, тобто $F_K^0(x) = x, F_K^i = F_K\left(F_K^{i-1}(\cdot) \oplus r_i\right)$. Ключ ПВГ K та маски $(r_1, \dots, r_w)$ є частиною відкритого ключа. Перевагою WOTS^{+} є те, що стійкість до колізій функції $\mathcal{F}_n$ не є обов'язковою, а достатньо стійкості до колізій та псевдовипадковості.

На практиці необхідно мати можливість створювати набагато більше підписів. У реальному житті ця цифра може досягати до 2^{50} підписів повідомлень за допомогою однієї ключової пари. Для конкурсу, NIST вимагає підписання 2^{64} повідомлень однієї ключовою парою.

Одним з варіантів створення схеми багаторазового підпису з схеми одноразового підпису є використання конструкції, запропонованої Мерклі в [15]. При заданих цілих чисел n, h та ґеш функції $H: \{0,1\}^{2n} \to \{0,1\}^n$, деревом Мерклє є двійкове дерево висотою h,

чиї вузли є $x \in \{0,1\}^n$, а значення вузла обчислюється як $x = H(y||z)$, де y та z є лівою та правою дитиною вузла відповідно. Листям дерева є значення особистого ключа. Корінь дерева r може публікуватися для подальшої автентифікації будь-якого з 2^h листів $v_1, \dots, v_{2^h}$. Для підтвердження того, що значення v є i-м листом, необхідно мати v, i та шлях автентифікації. Шлях автентифікації складається з усіх вузлів-сестер на шляху від i-го листа до кореня (всього h значень). Він дозволяє рекурсивно обчислити значення всіх внутрішніх вузлів до самого кореня, та порівняти його з r. Приклад шляху автентифікації для автентифікації i-го листа зображено на рисунку 2. Тобто шляхом автентифікації є сукупність вузлів, що зображені на рисунку сірим кольором.

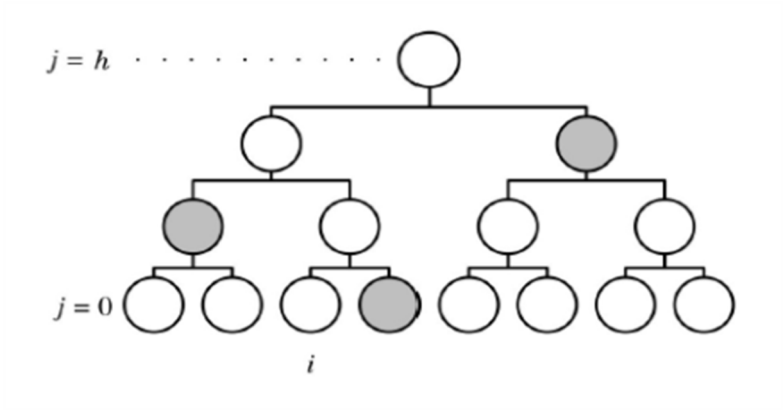

Рис. 2. Приклад шляху автентифікації i-го листа дерева Мерклє

У [16] Голдріх презентував конструкцію, яка базується на використанні двійкового дерева одноразових підписів. Для реалізації запропонованої схеми потрібно не просто ґешувати значення разом (як в стандартній конструкції дерева Мерклє), а замість цього прикріпляти ключову пару до кожного вузла дерева та використовувати її для підписання дочірніх вузлів. У цьому випадку немає необхідності повністю обчислювати дерево. Для цього необхідно, щоб ключі вузлів разом зі шляхом від випадкового вузла до кореня, були детерміновано згенерованими залежно від порядку. Це може бути досягнуто завдяки використанню псевдовипадкової функції, яка приймає на вхід секретне початкове значення та індекс вузла.

Хоча конструкція Голдріха дозволяє відмовитись від збереження стану, вона є досить неефективною. Покращеною версією такого підпису є конструкція SPHINCS [17].

По-перше, для листів дерева замість OTS (One Time Signature) використовується FTS (Few Time Signature), що дозволяє зменшити ймовірність виникнення колізії шляхів та зменшити висоту дерева. По-друге, внутрішні вузли дерева замінюються деревами Мерклє. Кожне з таких дерев підписує 2^h дітей, замість 2. Таким чином формується гіпер-дерево. За допомогою використання такої конструкції зменшується необхідний на генерацію підпису час та розмір підпису, адже до самого підпису входить менша кількість реалізацій OTS.

«Віртуальна» структура схеми SPHINCS повністю визначається ключовою парою . Основним елементом схеми є гіпер-дерево, яке має висоту h. Це дерево складається з d рівнів, кожен з яких складається з дерев висотою h/d. Кожне з цих дерев виглядає наступним чином. Листи дерев є $2^{h/d}$ коренями двійкового дерева. Кожен з коренів стискає відкритий ключ ключової пари WOTS$^+$. Тобто, дерево може розглядатися як ключова пара, кожна з яких може бути використана для підписання $2^{h/d}$ повідомлень. Всього а гіпер-дерево d рівнів. Рівень $d-1$ складається з одного дерева, рівень $d-2$ складається з $2^{h/d}$ дерев. Корені дерев на цьому підписуються за допомогою ключових пар WOTS$^+$ дерева на рівні $d-1$. В загальному випадку рівень i складається з $2^{(d-1-i)\binom{h}{d}}$ дерев, і, відповідно корені дерев на даному рівні підписуються за допомогою ключових пар WOTS$^+$ дерев на рівні $i+1$. На рівні 0 кожна з ключових пар WOTS$^+$ використовується для підписання відкритого ключа схеми HORST (модифікація схеми HORS (Hash to Obtain Random Subset) [18], яка була запропонована в [17]). Такою є так звана «віртуальна» структура схеми SPHINCS. Вона так називається через те, що всі значення встановлюються вибором початкового значення і біт-масок, а дерево повністю ніколи не обчислюється. Початкове значення є частиною секретного ключа і використовується для псевдовипадкової генерації ключів [17]. На рисунку 3 зображений один шлях в гіпер-дереві.

3. АНАЛІЗ КАНДИДАТІВ ЩОДО БЕЗУМОВНИХ КРИТЕРІЇВ

Для конкурсу NIST PQC було розроблено методику порівняння механізмів ЕП [20, 21], які мають протистояти загрозам постквантового періоду. При цьому кожний з алгоритмів ЕП має відповідати певним безу-

мовним критеріям, які наведено у таблиці 1. Ці критерії є обов'язковими, тобто якщо хоча б один з них не задовольняється, то кандидат відкидається.

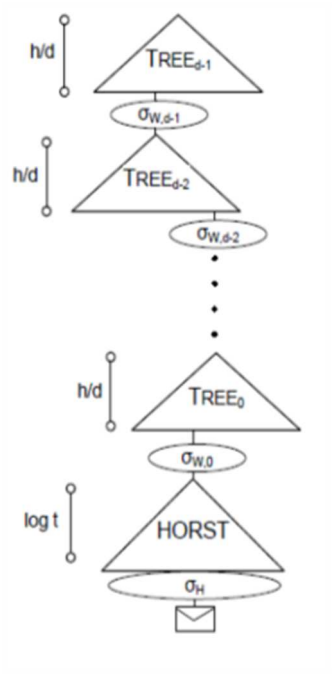

Рис. 3. Віртуальна структура підпису SPHINCS

Відповідно до прийнятих безумовних критеріїв проведено аналіз відповідності кожного з наведених алгоритмів ЕП, які приймають участь у конкурсі NIST PQC за такими умовами:

1. Наведені критерії вимагають чіткої відповідності, тому критерієм добору є логічна зміна так або ні (1 або 0). Тобто безумовний критерій можна подати у математичному поданні з урахуванням:

$$(W_{б1}, W_{б2}, W_{б3}, W_{б4}, W_{б5}, W_{б6}, W_{б7}) \in (1,0). \quad (2)$$

2. Використовуючи правило (2) функцію відповідності алгоритму вимогам, що викладені в таблиці 1, можна подати у вигляді інтегрального безумовного критерію:

$$W_б = W_1 \wedge W_2 \wedge W_3 \wedge W_4 \wedge W_5 \wedge W_6 \wedge W_7 .$$

Тобто, якщо $W_б$ відповідає значенню 0, то можна стверджувати, що криптоперетворення не відповідає безумовним критеріям, якщо 1 – то навпаки, відповідає.

Відповідно до поданих критеріїв проведений аналіз механізмів електронного підпису, який наведено у таблицях 2, 3.

Таблиця 1

Безумовні критерії оцінки постквантових криптографічних перетворень типу електронного підпису (ЕП)

№	Безумовні критерії	Позначення
1	Надійність, простота та прозорість математичної бази (математичних перетворень), що застосовуються в ході реалізації постквантових криптоперетворень ЕП.	$W_{б1}$
2	Практична захищеність криптоперетворення типу ЕП від відомих атак з використанням квантового комп'ютера та доступу криптоаналітика до 2^{64} обраних повідомлень, для моделі безпеки EUF – CMA	$W_{б2}$
3	Обгрунтованість реальної захищеності (стійкості) криптоперетворень типу ЕП від усіх відомих та потенційно можливих криптоаналітичних атак постквантового періоду на основі використання загальних параметрів та ключів з необхідними розмірами та властивостями (ключі 128 біт та більше класичної стійкості(безпеки)), включаючи статистичну безпеку.	$W_{б3}$
4	Теоретична захищеність криптографічних перетворень типу ЕП у постквантовий період проти існуючих силових, аналітичних та спеціальних атак для діючих моделей загроз (мінімум для моделі EUF – CMA для ЕП).	$W_{б4}$
5	Можливість заміни існуючих стандартизованих криптопримітивів на постквантові та застосування в діючих криптографічних системах та протоколах у певних умовах та обмеженнях.	$W_{б5}$
6	Обчислювальна ефективність – складність прямого $I_{пр}$ та зворотного $I_{зв}$ криптографічних перетворень ЕП, а також генерування асиметричних пар ключів $I_{кл}$ не вище за поліноміальну, забезпечення необхідних значень складності (швидкодії) $I_{пр}$, $I_{зв}$ та $I_{кл}$ при практичному застосуванні в додатках з апаратно-програмною та програмною їх реалізацією.	$W_{б6}$
7	Виконання обмежень на мінімальну та максимальну довжини особистих та відкритих ключів, розміри та збитковість ЕП, відсутність слабких особистих ключів для моделей безпеки постквантового періоду.	$W_{б7}$

У поданій специфікації DME[10] описані практичні досліди щодо безпеки алгоритму, але немає жодних уявлень щодо теоретичної захищеності від усіх відомих атак. Цей факт викликає підозру стосовно реальної захищеності механізму і відносно заявленого досягнутого рівня безпеки [19].

Відносно HiMQ3[8] наразі було знайдено недолік у доказі безпеки EUF-CMA[6], тому можливо визначити чи дійсно цей механізм задовольняє практичну та реальну захищеності відносно відомих та потенційно можливих криптоаналітичних атак.

Запропонований механізм TPSig[6] був відкликаний з конкурсу через те, що має лінійну складність відновлення секретного ключа[6]. Тому можна вважати, що три вищезгадані механізми отримали незадовільнений результат згідно з перевіркою на відповідність безумовним інтегральним критеріям.

Таблиця 2

Оцінка постквантових криптографічних перетворень типу електронного підпису (ЕП) на базі MQ-перетворень на відповідність безумовним критеріям

Scheme	$W_{\delta 1}$	$W_{\delta 2}$	$W_{\delta 3}$	$W_{\delta 4}$	$W_{\delta 5}$	$W_{\delta 6}$	$W_{\delta 7}$	W_{δ}
TPSig	1	0	0	1	1	1	1	0
HiMQ3	1	0	0	1	1	1	1	0
DME	1	1	0	1	1	1	1	0
LUOV	1	1	1	1	1	1	1	1
GUI	1	1	1	1	1	1	1	1
Rainbow	1	1	1	1	1	1	1	1
MQDSS	1	1	1	1	1	1	1	1
DualModeMS	1	1	1	1	1	1	1	1
GeMSS	1	1	1	1	1	1	1	1

Таблиця 3

Оцінка постквантових криптографічних перетворень типу електронного підпису (ЕП) на основі функцій гешування

Scheme	$W_{\delta 1}$	$W_{\delta 2}$	$W_{\delta 3}$	$W_{\delta 4}$	$W_{\delta 5}$	$W_{\delta 6}$	$W_{\delta 7}$	W_{δ}
Gravity-SPHINCS	1	1	1	1	0	1	1	0
SPHINCS^{+}	1	1	1	1	0	1	1	0

Надалі пропонується аналіз алгоритмів, які отримали позитивний результат перевірки, відносно умовних критеріїв та інтегрального умовного критерію, тобто LUOV[2], GUI[3], Rainbow[4], MQDSS[5], DualModeMs[7] та GeMSS[9].

За результатами, які наведено в таблиці 3 можна побачити, що запропоновані схеми відповідають всім умовним критеріям, окрім критерію $W_{\delta 5}$, який вимагає можливості заміни існуючих стандартизованих криптопримітивів на нові. Це є одним з основних недоліків постквантових схем електронного підпису на основі функцій гешування, адже для того, щоб застосовувати такі схеми, необхідно переробляти систему відкритого ключа. Але такі схеми все одно можуть знайти застосування, наприклад, у закритих спеціалізованих системах.

4. ПОРІВНЯННЯ АЛГОРИТМІВ ЩОДО УМОВНИХ КРИТЕРІЇВ

Для аналізу можливості використання тих чи інших алгоритмів, необхідно оцінити можливості кожного, а також оцінити перевагу одного алгоритму над іншим. Таку задачу можна вирішити за допомогою порівняння алгоритмів із застосуванням методу вагових коефіцієнтів. Далі наведено порівняння умовних оцінок алгоритмів.

Умовними оцінками виступали такі характеристики алгоритмів:

1) $I_{ст.}$ – рівень криптографічної стійкості;
2) lв.к – довжина відкритого ключа;
3) lо.к – довжина особистого ключа;
4) lрез. – довжина результату криптоперетворення (підпис);
5) Ткл. – швидкість створення ключової пари;
6) Тпр. – швидкість прямого криптоперетворення (створення підпису);
7) Тзв. – швидкість зворотного криптоперетворення (перевірка підпису).

Для поданих характеристик застосовується оцінка важливості, яку виставляють експерти в області криптографії. Числова шкала оцінки, числові значення, та вагові коефіцієнти важливості характеристик наведені у таблиці 4.

Таблиця 4

Експертні оцінки характеристик криптоалгоритмів методом ранжування

Показники / Експерти	Іст.	lв.к	lо.к	lрез.	$T_{кл.}$	Тпр.
1	7	5	3	2	1	4
2	6	7	1	3	2	4
3	5	6	1	2	3	4
4	5	6	1	4	2	3
5	6	2	1	4	3	5
W	**0,207**	**0,186**	**0,05**	**0,107**	**0,079**	**0,143**

Безпосередньо на конкурс NIST PQC було подано безліч механізмів із різними модифікаціями, тому було прийнято рішення для алгоритмів на базі MQ-перетворень порівнювати лише алгоритми, які мають позитивний інтегральний безумовний критерій. Для кожного такого алгоритму була обрана модифікація, яка відповідно до специфікації гарантує найвищий рівень безпеки.В таблицях 5, 6 наведено характеристики обраних для порівняння алгоритмів електронного підпису.

Всі значення розмірів ключів та підписів у таблицях 5 та 6 наведено в байтах, а швидкості виконання операцій – в циклах процесора. Для того, щоб проаналізувати ефективність виконуваних обчислень описаних алгоритмів, швидкість виконання операцій вимірюється в кількості циклів, які необхідно виконати процесору для реалізації операції. Цей показник залежить від характеристик системи, яка використовується для виконання операції. Обчислювальні можливості процесора вимірюються в Гц, що еквівалентно секунді в -1 ступені. Таким чином, значення кількості циклів, необхідних для виконання будь-якої операції можна отримати за формулою:

$$n = \nu \cdot t,$$

де n – кількість циклів процесора, ν – частота процесора, t – час виконання операції.

Таблиця 5

Характеристики алгоритмів електронного підпису на базі MQ-перетворень

Схема	$\mathbf{I_{ст}}$	$\mathbf{l_{в.к}}$	$\mathbf{l_{о.к}}$	$\mathbf{l_{рез}}$	$\mathbf{T_{кл.}}$	$\mathbf{T_{пр}}$	$\mathbf{T_{зв}}$
LUOV	256	100 967	32	521	276 912 036	144 203 736	84 564 465
GUI	256	5 928 141	159 642	83	239 502 000 000	872 949 000 000	2 004 155
Rainbow	256	1 351 373	892 109	118	45 064 000 000	3 916 000	2 897 000
GeMSS	256	3 603 792	82 056	104	18 174 000 000	12 740 000 000	160 420 000
MQDSS	192	88	48	67 800	6 680 606	776 183 461	571 665 382
DualModeMS	128	528	18 038 184	32 640	2 072 200 000 000	6 006 000 000	6 994 000

Таблиця 6

Характеристики алгоритмів електронного підпису на основі функцій ґешування

Схема	$\mathbf{I_{ст}}$	$\mathbf{l_{в.к}}$	$\mathbf{l_{о.к}}$	$\mathbf{l_{рез}}$	$\mathbf{T_{кл.}}$	$\mathbf{T_{пр}}$	$\mathbf{T_{зв}}$
Gravity-SPHINCS S	128	32	65 536	12 640	781 646 000	17 964 000	104 000
Gravity-SPHINCS M	128	32	262 144	28 929	24 229 712 000	18 900 000	252 000
Gravity-SPHINCS L	128	32	131 072	35 168	11 789 080 000	21 054 000	338 000
SPHINCS+ 128s	128	32	64	8 080	917 405 356	16 992 635 344	19 360 272
SPHINCS+ 128f	128	32	64	16 976	28 814 020	1 056 761 824	45 964 624
SPHINCS+ 192s	192	48	96	17 064	1 244 530 184	38 062 259 596	27 243 200
SPHINCS+ 192f	192	48	96	35 664	42 782 840	1 276 694 620	69 760 728
SPHINCS+ 256s	256	64	128	29 792	1 817 324 180	28 860 355 888	42 380 420
SPHINCS+ 256f	256	64	128	49 216	113 876 252	3 172 247 452	76 203 004

На рисунках 4 та 5 відображено гістограми відносної переваги алгоритмів, що базуються на MQ-перетвореннях та функціях ґешування.

Як видно з рисунку 4, серед алгоритмів на базі MQ-перетворень, відповідно до проведеної методики, кращими алгоритмами є Rainbow та LUOV. Останні місця займають MQDSS та DualModeMS. Серед алгоритмів, які базуються на функціях ґешування, кращими є Gravity-SPHINCS S, Gravity-SPHINCS M та SPHINCS$^+$ 128s. Останні місця займають SPHINCS$^+$ 192f та SPHINCS$^+$192s.

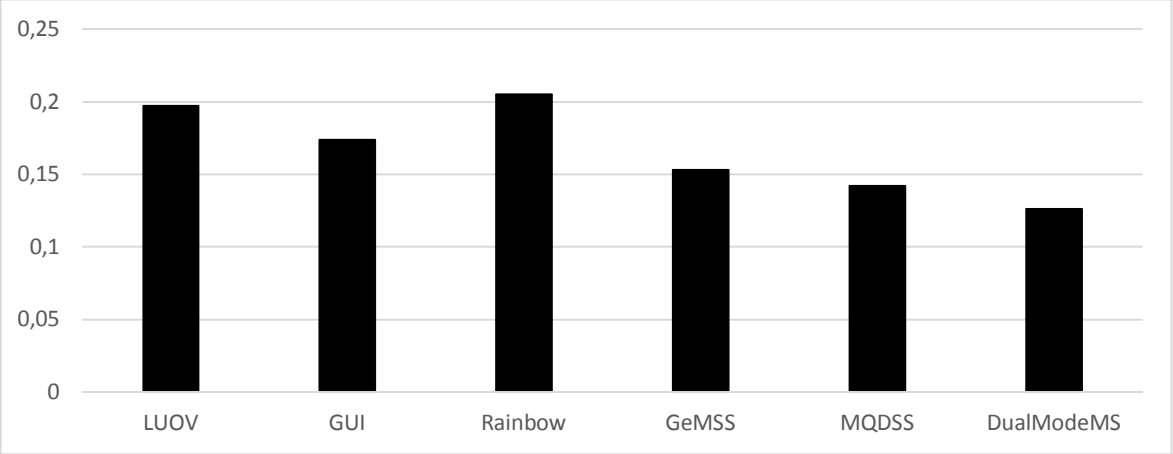

Рис. 4. Відносна перевага алгоритмів ЕП на базі MQ перетворень

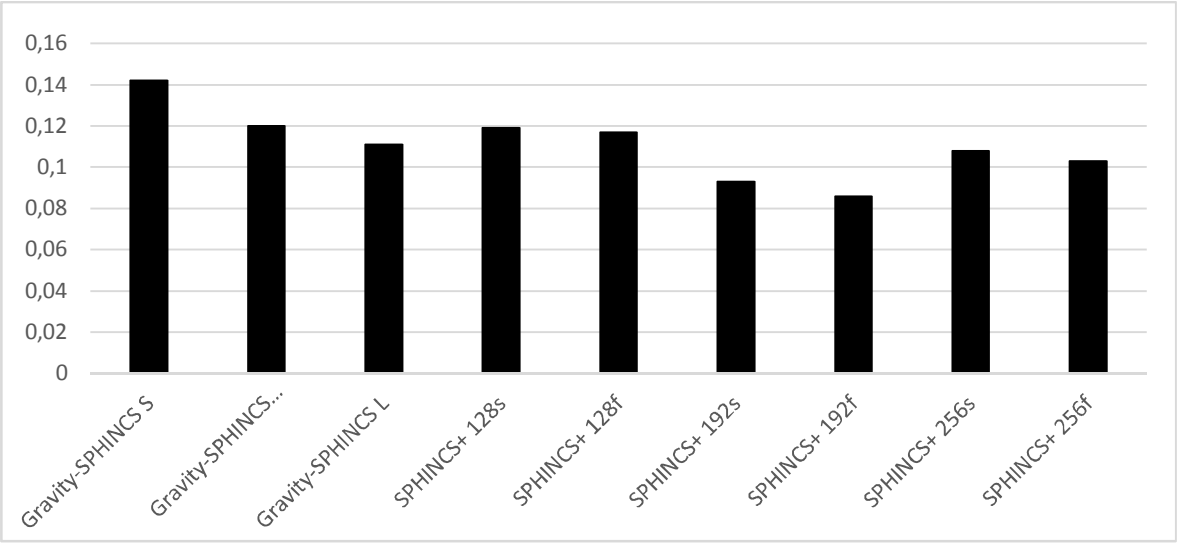

Рис. 5. Відносна перевага алгоритмів ЕП на основі функцій ґешування

5. ПОРІВНЯННЯ КРАЩИХ АЛГОРИТМІВ ВІДНОСНО УМОВНИХ КРИТЕРІЇВ

Далі наводиться порівняння найперспективніших алгоритмів ЕП, які було проаналізовано в розділі 4. Цими алгоритмами є LUOV, Rainbow. Gravity-SPHINCS S та SPHINCS$^+$ 128s. Алгоритм Gravity-SPHINCS M не було взято до порівняння, через те, що він є ще однією модифікацією алгоритму Gravity-SPHINCS, та має не дуже велику перевагу над SPHINCS$^+$ 128s.

Для порівняння було взято ті ж характеристики, а також показники з таблиць 4, 5, 6.

На рисунку 6 наведено результати цього порівняння.

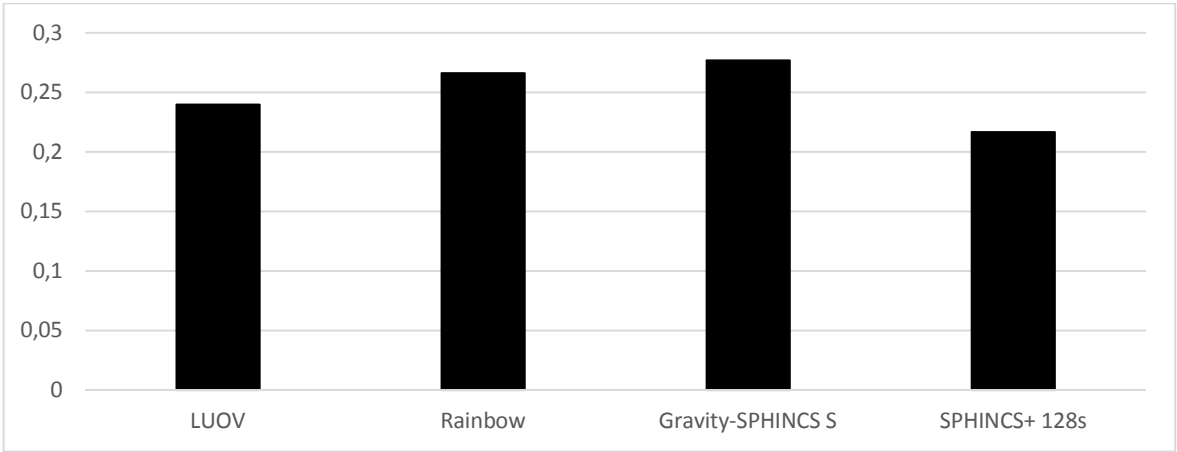

Рис. 6. Відносна перевага алгоритмів ЕП

Як видно з рисунка 6, алгоритм Gravity-SPHINCS S має найвищий показник, отже, є найперспективнішим з описаних алгоритмів. На другому місці є Rainbow. Як було зазначено вище, описані алгоритми на основі функцій ґешування, не можуть використовуватись як заміна існуючим національним стандартам, через необхідність перебудування існуючої інфраструктури відкритого ключа. Отже, алгоритм Gravity-SPHINCS S є дуже перспективним, але може використовуватися лише в спеціалізованих закритих системах, а алгоритм Rainbow є гарним кандидатом для використання на національному рівні.

ВИСНОВКИ

1. Первинний аналіз кандидатів, що представлені NIST США на конкурс постквантової криптографії, зроблено з використанням техніко-економічних показників, а саме розміру публічного та приватного ключа, рівнів криптографічної стійкості ЕП, розміру підпису, складності (швидкодії) генерування ключової пари, складності (швидкодії) обчислення та перевірки ЕП.

2. Значне число кандидатів на стандарт ЕП розроблено на основі застосування мультиваріативних квадратичних перетворень (Multivariate Quadra-tic Transformations, MQ-transformations). Механізми MQ-перетворень дозволяють забезпечити необхідні рівні стійкості, швидкодію та застосування в мало-ресурсних системах, а також можуть застосовуватися у загальному випадку.

3. Шість з дев'яти кандидатів на ЕП - LUOV, Rainbow, GUI, GeMSS, MQDSS, DualModeMS алгоритмів, що базуються на MQ-перетвореннях, відповідають безумовним критеріям.

4. Стосовно алгоритмів на основі функції ґешування слід зазначити, що такі алгоритми практично уже відповідають усім представленим безумовним критеріям. Проблемним, з точки зору складності, є реалізація сертифікації відкритих ключів.

5. Кандидати на стандарт Rainbow та LUOV мають найбільшу перевагу серед алгоритмів на базі MQ-перетворень, тому їх можна важати найбільш перспективними.

6. Алгоритм Gravity-SPHINCS S виявився найкращим в результаті порівняння відносно умовних критеріїв.

7. Як кандидат на національний стандарт найперспективнішим з описаних є алгоритм Rainbow.

8. Проект Gravity-SPHINCS S має найвищий показник, отже, є найперспективнішим з описаних алгоритмів. На другому місці є Rainbow.

Література

[1] Post-Quantum Cryptography, Round 1 Submissions, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

[2] *Ward Beullens, Bart Preneel, Alan Szepieniec, Frederik Vercauteren.* LUOV: Lifted Unbalanced Oil and Vinegar, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

[3] *Jintai Ding, Ming-Shen Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang.* Gui, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

[4] *Jintai Ding, Ming-Shen Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang.* Rainbow. NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

[5] *Simona Samardjiska, Ming-Shing Chen, Andreas Hulsing, Joost Rijneveld, Peter Schwabe.* MQDSS, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

[6] *Joseph Peretz, Nerya Granot.* TPSig, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

[7] *J.-C. Faugère, L Perret, J Ryckeghem.* DualModeMS: A Dual Mode for Multivariate-based Signature, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

[8] *Kyuang-Ah Shim, Cheol-Min Park, Aeyoung Kim.* HiMQ-3: A High Speed Signature Scheme based on Multivariate Quadratic Equations, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

[9] *A. Casanova, J.-C. Faugère, G. Macario-Rat, J Patarin, L Perret, J Ryckeghem.* GeMSS: A Great Multivariate Short Signature, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

[10] *Ignacio Luengo, Martin Avendano, Michel Marco.* DME: DME a public key, signature and KEM system based on double exponentiation., NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions. Unpublished.

[11] Jean-Philippe Aumasson. Gravity-SPHINCS v1, November 29, 2017.

[12] Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Andreas Hülsing, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe. SPHINCS+. Submission to the NIST post-quantum project. November 30, 2017.

[13] *Leslie Lamport.* Constructing digital signatures from one-way functions. Technical report, Technical Report CSL-98, SRI International Palo Alto, 1979.

[14] *Andreas Hulsing.* W-OTS+ - shorter signatures for hash-based signature schemes. In Progress in Cryptology - AFRICACRYPT 2013, 6th International Conference on Cryptology in Africa, Cairo, Egypt, June 22–24, 2013. Proceedings, pages 173–188, 2013.

[15] *Ralph C. Merkle.* A certifed digital signature. In Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20–24, 1989, Proceedings, pages 218–238, 1989.

[16] *Oded Goldreich.* The Foundations of Cryptography - Volume 2, Basic Applications. Cambridge University Press, 2004.

[17] Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O'Hearn. SPHINCS: practical stateless hash-based signatures. In Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26–30, 2015, Proceedings, Part I, pages 368–397, 2015.

[18] *Leonid Reyzin, Natan Reyzin.* Better than BiBa: Short One-time Signatures with Fast Signing and Verifying. In Information Security and Privacy, 7th Australian Conference, ACISP 2002, Melbourne, Australia, July 3–5, 2002, Proceedings, pages 144–153, 2002.

[19] Post-Quantum Cryptography Lounge, 2018 [On-line]. Internet: https://www.safecrypto.eu/pqclounge/.

[20] *І.Д. Горбенко, І.С. Кудряшов, В.В. Онопрієнко.* Порівняльний аналіз пост квантових стандартів електронного підпису на основі мультиваріативних квадратичних перетворень // Радиотехника: всеукр. межвед. науч.-техн. сб. – Харьков: ХТУРЕ. – 2018. – Вып. 195. – С. 46–60.

[21] Yu. I. Gorbenko, T. V. Melnik, I.D. Gorbenko. "Analysis of Potential Post-Quantum Schemes of Hash-Based Digital Signatur" *Telecommunications and Radio Engineering*, Volume 77, 2018, Issue 7, pp. 603–626.

[22] Yu. I. Gorbenko, K. V. Isirova. "Improved Mechanism of One-Time Keys for Post-Quantum Period Based on the Hashing Functions" *Telecommunications and Radio Engineering*, Volume 77, 2018, Issue 14, pp. 1277–1296.

Надійшла до редколегії 25.12.2018

Горбенко Юрій Іванович, кандидат технічних наук, перший заступник головного конструктора АТ «ІІТ». Галузь наукових інтересів – системи, комплекси та засоби криптографічного захисту інформації.

Кудряшов Іван Сергійович, студент ХНУ ім. В. Н. Каразіна, факультет комп'ютерних наук, кафедра безпеки інформаційних систем і технологій. Галузь наукових інтересів – криптографічні властивості булевих функцій.

Науменко Данило Сергійович, студент факультету комп'ютерних наук Харківського національного університету імені В. Н. Каразіна. Галузь наукових інтересів – постквантовий електронний підпис.

Онопрієнко Віктор Васильович, кандидат технічних наук, генеральний директор АТ «ІІТ». Галузь наукових інтересів – системи, комплекси та засоби криптографічного захисту інформації.

УДК 003.026:004.056

Горбенко Ю. И. **Сопоставление кандидатов электронной подписи на постквантовый стандарт NIST PQC на базе MQ-преобразований и функций хеширования** / Ю. И. Горбенко, И. С. Кудряшов, Д. С. Науменко, В. В. Оноприенко // Прикладная радиоэлектроника: науч.-техн. журнал. –2018. – Том 17. № 3, 4. – С. 138–146.

Приводятся результаты сравнительного анализа кандидатов на стандарты перспективных электронных подписей, которые строятся на основе мультивариативних квадратичных преобразований и на функции гешування. Результаты анализа получены при использовании методики сравнения криптографических механизмов на основе экспертных оценок по совокупности условных и безусловных критериев. Сделаны рекомендации относительно перспектив применения кандидатов.

Ключевые слова: MQ-преобразования, постквантовый алгоритм, электронная подпись, сравнительный анализ, экспертные оценки, подпись на основе хеш-функций.

Табл.: 6. Ил.: 6. Библиогр.: 22 назв.

UDC 003.026:004.056

Gorbenko Yu. I. **Comparison of electronic signature candidates to the post quantum standard NIST PQC on the basis of MQ-transformations and functions of hashing** / Yu. I. Gorbenko, I. S. Kudryashov, D. S. Naumenko, V. V. Onoprienko // Applied Radio Electronics: Sci. Journ. – 2018. – Vol. 17. № 3, 4. – P. 138–146.

The results of a comparative analysis of candidates for the standards of promising electronic signatures, which are based on multivariate quadratic transformations and the hashing function, are presented. The results of the analysis are obtained using the methodology for comparing cryptographic mechanisms based on expert estimates using a combination of conditional and unconditional criteria. Recommendations are made regarding the prospects for candidates application.

Keywords: MQ-transformations, post-quantum algorithm, electronic signature, comparative analysis, expert estimates, signature based on hash functions.

Tab.: 6. Fig.: 6. Ref.: 22 items.