УДК 004.056.55

О.В. Шевцов, І.І. Сватовський, Т.Ю. Кузнецова

Харківський національний університет ім. В.Н. Каразіна, Харків

АНАЛІЗ ТА ПОРІВНЯЛЬНІ ДОСЛІДЖЕННЯ АЛГОРИТМІВ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ ДЛЯ ПОСТКВАНТОВОГО ЗАСТОСУВАННЯ

Аналізуються постквантові криптографічні примітиви електронного цифрового підпису та обґрунтовуються умови їхнього застосування в Україні для забезпечення безпеки інформаційних технологій на постквантовий період. Порівнюються кандидати цифрових квантово-стійких підписів за обраними критеріями. Розробляються рекомендації до застосування обраних криптопримітивів в залежності від сфери використання.

***Ключові слова**: постквантова криптографія, алгебраїчні решітки, електронний цифровий підпис, завадостійкі коди.*

Вступ

Важливою сферою застосування криптографії з відкритим ключем є аутентифікація повідомлень за допомогою електронних цифрових підписів (далі – ЕЦП). Сучасні підписи мають різні властивості й досить широке застосування в багатьох сферах, що обумовлює необхідність порівняльного аналізу для розробки рекомендацій з метою подальшого доцільного застосування обраних криптопримітивів. Основні результати щодо класичних підписів RSA, ECC, DSA представлені в роботі [1]. Останні досягнення в області впливу квантових обчислень на стійкість відомих підписів розглянуті в публікаціях [1 – 3]. Проведені дослідження в галузі створення новітніх обчислювальних систем, що використовують явища квантової суперпозиції та квантової заплутаності для передачі та обробки даних, показали, що квантові комп'ютери, які використовують спеціальні алгоритми (наприклад, алгоритм Шора), будуть здатні до факторизації чисел за поліноміальний час [1]. Отже, криптографічні системи RSA, ECC, DSA будуть вразливі до атак "грубої сили" (brute force attacks) з використанням повномасштабного квантового комп'ютера [3].

Тому основні дослідження і розробки криптографічних засобів захисту інформації (КЗЗІ) в нинішній час спрямовані на пошуки рішень, що не мали б вразливостей щодо квантових обчислень і були б одночасно стійкими до атак за допомогою звичайних комп'ютерів. Такі алгоритми отримали назву постквантової криптографії (post-quantum cryptography [4; 6]) або квантово-стійкої криптографії (quantum safe cryptography [3] або quantum resistant cryptography [9]). Найбільш перспективними для використання в постквантовому середовищі в даний час вважають такі [4; 5; 8; 9; 10]: криптографія на основі хеш-функцій; криптографія на основі завадостійких кодів; криптографія на основі факторизації поліномів; криптографія на основі решіток. Вищезазначені криптосистеми та підписи є предметом досліджень даної роботи.

В останні роки недостатньо уваги приділено порівнянню нових схем підписів та параметрів, що з часом змінюються. Через швидку появу нових схем не приділяється достатня увага рекомендаціям щодо сфер використання підписів, які мають обмежену ефективність або обсяг ключів.

Метою роботи є аналіз і порівняльні дослідження алгоритмів ЕЦП, обґрунтування умов їхнього застосування для забезпечення безпеки інформаційних технологій в умовах застосування квантових комп'ютерів.

1. Обґрунтування критеріїв та показників ефективності ЕЦП в умовах квантового криптоаналізу

Для визначення перспективних кандидатів постквантового підпису сформулюємо ряд критеріїв порівняння досліджуваних алгоритмів:

- захищеність алгоритму підпису, яка оцінюється рівнем безпеки (в бітах) складності виконання атаки та розрахунку безпечного часу зламу криптосистеми (безумовний критерій);
- час підписання і перевірки в мілісекундах (умовний критерій);
- час генерації базових параметрів і ключів в мілісекундах (умовний критерій);
- довжина ключів в байтах (умовний критерій);
- довжина підпису в байтах (умовний критерій).

До безумовного критерію ефективності ЕЦП відносяться захищеність від повного розкриття та захищеність від підробки. Під критерієм будемо розуміти ознаку, на основі якої здійснюється оцінка, визначення чи класифікація. Показники оцінки яко-

сті криптоперетворень типу ЕЦП для безумовних критеріїв детально обґрунтовані в [1]. Виберемо та розглянемо основні показники, за якими можна оцінити алгоритми криптографічних перетворень підпису. Існують такі безумовні критерії оцінки:

– надійність математичної бази, що застосовується для ЕЦП при криптоперетвореннях;

– практична захищеність криптографічних перетворень типу ЕЦП від відомих атак;

– реальна захищеність ЕЦП від усіх відомих і потенційно можливих критпоаналітичних атак.

Практичну захищенність криптографічних перетворень типу ЕЦП від силових атак будемо оцінювати, орієнтуючись на розмір особистого ключа [1]: 2^m, де m – кількість біт. Під силовою атакою будемо розуміти простий перебір особистого ключа, що має обиратися випадково. За таких умов ймовірність підбору ключа з однієї спроби можна оцінити як:

$$P(1) \geq \frac{1}{2^m} = 2^{-m},$$

де m – розмір особистого ключа в бітах.

Оцінку складності силової атаки можна здійснити, оцінивши складність атаки I_d та безпечного часу $t_б$ (роки). Відповідно до [1]:

$$I_d = 2^m, \; t_б = \frac{I_d}{\gamma K} P_y,$$

де P_y – ймовірність, з якою може бути здійснено криптоаналіз, γ – потужність криптоаналітичної системи, $K = 3{,}15 \cdot 10^7$ сек/рік.

Реальну захищеність криптоперетворення типу ЕЦП пропонується оцінювати визначенням складності I_a та безпечного часу t_a здійснення атаки типу "повне розкриття". Приміром, обирається найбільш ефективна атака на криптоперетворення типу ЕЦП зі складністю I_a, тоді безпечний час з допустимою точністю можна визначити як:

$$t_a = \frac{I_a}{\gamma K} P_y.$$

Оцінку на відповідність безумовним критеріям пропонується проводити в два етапи: спочатку розглянемо складності атак на криптоперетворення ЕЦП, а потім встановимо відповідність вищевказаним критеріям (детельніше у п. 2).

Для обґрунтування інтегрального критерію порівняння підписів було обрано метод аналізу ієрархій [20] (детальніше в п. 3). Цей метод вирізняється наявністю ряду переваг, зокрема, таких як точність рішення, в порівнянні з іншими підходами, і простота реалізації. Слід відзначити, що при проведенні порівнянь певних складних систем далеко не всі зв'язки між компонентами можуть бути кількісно враховані через відсутність необхідного обсягу інформації, а для певних класів задач таких, як прогностичні й імітаційні, даних може зовсім не бути. У цих випадках необхідні зв'язки зазвичай встановлюються експертним шляхом, наприклад, при прогнозуванні сфери застосування підписів [20]. Порівняння підписів в цій роботі проходить в два етапи: спочатку проаналізовано відповідність цифрових підписів безумовним критеріям, потім здійснено порівняння за умовними критеріями. В результаті проведених досліджень за інтегральним критерієм (п. 3) розроблено пропозиції та обґрунтовані умови застосування алгоритмів цифрового підпису на постквантовий період.

2. Аналіз стійкості цифрових підписів в умовах появи квантового комп'ютера

Для обрання перспективних кандидатів постквантових підписів за безумовним критерієм проведемо порівняння стійкості до квантового криптоаналізу систем ЕЦП на решітках та кодах, розглянемо стан захищеності класичних криптосистем (RSA, ECC, DSA) до квантового криптоаналізу. Оцінки стійкості підписів на основі хеш-функцій та на основі решіток були розглянуті в роботах [6; 8; 10] та відповідають безумовному критерію, тому детально їх не розглядатимемо.

На основі аналізу відомих джерел для оцінки стійкості підписів було виділено основні атаки, які можуть бути реалізованими на квантовому комп'ютері. До основних задач, які можуть бути вирішені за допомогою квантових обчислень, передусім, необхідно віднести:

– квантовий алгоритм факторизації Шора [6; 16];

– квантовий алгоритм Гровера [17];

– квантовий алгоритм Шора вирішення дискретного логарифму в кінцевому полі [16];

– квантовий алгоритм Шора вирішення дискретного логарифму в групі точок еліптичної кривої [16];

– квантовий алгоритм криптоаналізу для перетворень у фактор кільці [16; 18; 19].

Усі відомі нині класичні алгоритми факторизації мають експоненційну, або субекспоненційну складність [1]. Вважається, що найкращим, з точки зору мінімізації складності факторизації, є алгоритм загального решета числового поля та його модифікації. Але застосування алгоритмів загального або спеціального решета числового поля для реальних значень загальних параметрів $N \geq 2^{2048}$ не можуть бути реалізовані. Часова складність таких алгоритмів, оцінюється як субекспоненційна [1]:

$$O(\exp((c + o(1))(\ln n)^{1/3}(\ln \ln n)^{2/3})).$$

Одночасно, квантовий алгоритм Шора має поліноміальну складність. Він здатний факторизувати

число приблизно за час $O(n^3)$ з використанням $O(n)$ кубітів [16].

В результаті впливу квантових обчислень криптосистеми з відкритим ключем RSA DSA ECC втратять стійкість та практичну значимість [1–4].

Складність квантового та класичного криптоаналізу для цих підписів відображені на рис. 1. По горизонтальній осі відображаються рівні стійкості k, по вертикальній осі відображається величина d, що впливає на складність алгоритму атаки як ступінь 10^d .

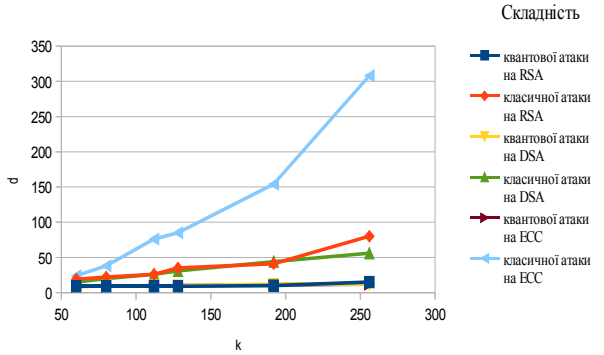

Рис. 1. Складності класичного і квантового алгоритмів криптоаналізу для RSA, DSA, ECC

Розглянемо вплив вказаних алгоритмів квантового криптоаналізу на інші цифрові підписи. Алгоритм цифрового підпису CFS з використанням завадостійких кодів, заснований на схемі Нідеррайтера [6], є одним з найбільш перспективних постквантових кандидатів. Лінійний код представляє k-вимірний підпростростір n-вимірного векторного простору над кінцевим полем F_q, де k та n – цілі позитивні числа із $k < n$ та q – число елементів поля. Елементи коду називаються кодовими словами. Інформаційна швидкість визначається як $R = k / n$. Мінімальною відстанню d коду є мінімальна з відстаней Хемминга для всіх пар кодових слів, а код з цими властивостями позначається як [n, k, d]. Виправляюча здатність лінійного коду є максимальна кількість помилок $t = (d – 1) / 2$, які код може виправити.

В алгоритмі CFS реалізований принцип, який полягає в багаторазовому хешуванні документа, рандомізованого лічильником бітової довжини r, поки не буде отримано правильно виділений синдром. Підписувач використовує свій секретний ключ для визначення відповідного вектора помилок. Разом з поточним значенням лічильника цей вектор помилок буде служити в якості підпису.

Реалізація такої схеми підпису здійснюється відповідно до наступного алгоритму [12]:

1. Загальносистемні параметри: m, $t \in N$.

2. Генерація ключа: генерація пари ключів системи Нідеррайтера на основі використання коду C із класу $[n = 2^m, k = n − mt, 2t + 1]$ двійкових незвідних кодів, для якого породжуються такі матриці:

H: $(n – k) \times n$ – перевірочна матриця коду C, котрий може максимально коректувати t помилок,

X: $(n – k) \times (n – k)$ – випадкова зворотня матриця,

P: $n \times n$ – випадкова матриця перестановок;

Відкритий ключ: матриця $H^* = X \cdot H \cdot P$ і число t;

Секретний ключ: матриці X, H, P і швидкий (поліноміальної складності) алгоритм декодування γ коду C.

3. Формування підпису:

Вхід: h – хеш-функція, алгоритм γ, документ d, котрий повинен бути підписаний;

Вихід: CFS - підпис;

Алгоритм формування CFS-підпису:

– хешування документа d, тобто обчислення $s = h (d)$;

– обчислення $s_i = h ([s | i])$ для $i \in \{0, 1, 2, …\}$, де $[s | i]$ – конкатенація (об'єднання) s та i;

– пошук найменшого i, при якому s_i буде декодовано алгоритмом γ, тобто, має виконуватися умова

$$e H^T = s,$$

де

$$e H^T \in F_q^{n-k},$$

а F_q^{n-k} – синдромний простір;

– відповідні значення вектора помилок e і лічильника i є підписом документа d.

4. Верифікація:

Вхід: підпис у вигляді значення e та i, документ d та H^*;

Вихід: прийняти чи відхилити;

Алгоритм верифікацій:

– обчислення $s_1 = H^* \cdot e^T$;

– обчислення $s_2 = h ([s | i])$;

якщо $s_1 = s_2$, тоді s приймається,

інакше s відхиляється.

Стійкість CFS від підробки може бути зведена до складності рішення проблеми синдромного декодування. Найбільш швидкі атаки на підпис CFS [3] основані на алгоритмі Вагнера вирішення "парадоксу про день народження". Алгоритм Вагнера для екзистенційної підробки має експоненційну складність $2^{mt/3}$. При наборі параметрів CFS: $m = 16$, $t = 9$ ця атака потребує 2^{59} операцій. Послідовно виконуваний алгоритм Вагнера не може бути прискорений за допомогою квантових обчислень. Таким чином, навіть при винайденні квантового комп'ютера, не можна очікувати прискорення атак на CFS.

Алгоритм Гровера перебирає N ключів за $O(\sqrt{N})$ операцій із використанням $\log_2(N)$ кубіт квантового комп'ютера. В табл. 1 наведено порівняння квантового і класичного алгоритмів криптоаналізу кодових криптосистем [6].

Складність алгоритму Гровера дорівнює кореню квадратному від часу виконання відомих алгоритмів [5].

Таблиця 1

Порівняння складності квантового і класичного криптоаналізу криптосистеми McEliece

Параметри McEliece: m,t	Криптоаналіз (в бінарних операціях)		Мінімальна кількість кубіт	Рівень стійкості квантових обчислень (в бітах)
	Класична атака	Квантова атака		
11,32	2^{91}	2^{86}	25	80
11,4	2^{98}	2^{94}	50	88
12,22	2^{93}	2^{87}	29	80
12,45	2^{140}	2^{133}	28	128

Можливість прискорення алгоритму Гровера потребує подальших досліджень. На даний час для захисту від атаки Гровера доцільно збільшувати ключі McEliece в чотири рази [10].

Оцінки стійкості для криптографічних перетворень в решітці на постквантовий період приводяться нижче. Одним із варіантів криптосистеми на решітках є NTRU. Розглянемо підпис та параметри NTRUSign.

Операції ЕЦП можна представити в факторкільці поліномів $(Z/qZ)[X]/(X^N-1)$, де N – це розмір поліному, q степінь двійки. Секретний ключ NTRUSign містить 4 полінома (f,g,F,G). Зокрема, g,f – це поліноми з коефіцієнтами, вибраними з діапазону {-1,0,1}, і f має інверсію в $(Z/qZ)[X]/(X^N-1)$. F,G – поліноми з нормою приблизно $\|F\|=\sqrt{(N-1)/12}$ та задовольняють рівнянню $fG-Fg=q$ [15]. Відкритий ключ NTRUSign визначається поліномом $h=f^{-1}\cdot g$ з коєфіцієнтами з діапазону $[-q/2,q/2]$. Нехай $m=(m_1,m_2)$ – геш значення повідомлення та $m=m_1\|m_2$ – дві рівні половини полінома m. Підпис визначається вектором $(s,t)\in L$, котрий знаходиться близько до повідомлення. Підпис обчислюється за правилом:

$$s\equiv f\cdot B+F\cdot b(\mathrm{mod}\ q),$$

$$t\equiv g\cdot B+G\cdot b(\mathrm{mod}\ q),$$

де B та b обчилюють із співвідношень

$$G\cdot m_1-F\cdot m_2=A+q\cdot B,$$

$$g\cdot m_1-f\cdot m_2=a+q\cdot b.$$

Поліноми a, A мають коефіцієнти із діапазона [-1/2, 1/2] та $b, B\in Z[X]/(X^N-1)$.

Дійсний підпис демонструє вирішення задачі знаходження найближчого вектора $(s,t)\in L$ до заданого вектора $(m_1,m_2)\in R$ [15]. При перевірці підпису обчислюється відстань від (s,t) до $(m_1\,m_2)$, як норма різниці між цими векторами, ця відстань не повинна бути більшою, ніж заздалегідь обрахована перевірочна відстань *NormBound*:

$$\|s-m_1\|^2+\|t-m_2\|^2\le \mathrm{NormBound}^2.$$

В іншому випадку підпис вважається недійсним. Стійкість NTRUSign може бути зведена до складності рішення проблеми знаходження найкоротшого вектора в решітці.

Відомі квантові атаки не порушують стійкість теоретико-складної задачі криптосистем на решітках. Проте існують комбінаторні атаки на реалізацію NTRU [7; 19], наприклад, атака "зустріч посередині" є найбільш ефективним методом пошуку особистого ключа NTRU, часова складність якої до цих пір дуже велика навіть при використанні квантових алгоритмів. У 2003 році Людвіг [7] застосував квантовий алгоритм пошуку Гровера на основі решіток (QRS). Час роботи квантового алгоритму пошуку (QRS), у порівнянні з класичними алгоритмами, зменшився та має експоненційну часову складність. У 2005 році Грехем вказав, що обчислювальна складність QRS більша, ніж у атаки "зустріч посередині". У 2010 році Ванг [19] запропонував квантовий алгоритм пошуку цільового рішення з фіксованою вагою і вперше застосував його для пошуку особистого ключа NTRU. Метод Ванга потребує малого обсягу зберігання даних, але складність обчислень у нього ще більше, ніж у атаки "зустріч посередині".

Проаналізуємо квантові атаки на ЕЦП NTRUSign [15]. Як слідує із [19], метод Ванга може розглядатися як алгоритм квантового пошуку типу "груба сила", який зменшує складність з $O(C_N^{d_f})$ класичного алгоритму до $O(\sqrt{C_{N+1}^{d_f}})$, де d_f кількість одиниць в f. Зазначена оцінка складності вимірюється як кількість операцій, необхідних для успішного криптоаналізу. Порівняльний аналіз часової складності для різних розмірів системних параметрів NTRU та різних атак [15] наведено у табл. 2. В стовбці «Параметри NTRU» записані значення N. Із табл. 2 видно, що удосконалена квантова атака методом Ванга має суттєво меншу складність, ніж складність квантової атаки методом Ксіонга, а також меншу складність ніж складність класичної атаки методом "зустріч посередині". Складність квантової атаки методом Ксіонга більше складності атаки методом Ванга та суттєво більше за класичну атаку "зустріч посередині".

Оцінимо криптоперетворення типу ЕЦП в математичному базисі решіток та завадостійких кодів на відповідність безумовним критеріям.

Практичну захищеність ЕЦП NTRU від силових атак будемо оцінювати орієнтуючись на розмір особистого ключа 2^m, де m = 3512 кількість біт ключа:

$$I_d = 2^m,\ t_б = \frac{2^{3512}}{10^{15}\cdot 3{,}15\cdot 10^7} = 10^{1136{,}96}. \qquad t_б = \frac{10^{4950000}}{10^{15}\cdot 3{,}15\cdot 10^7} = 10^{4949978}.$$

Аналогічна оцінка для CFS, для m = 15000000*:*

Таблиця 2

Часова складність різних алгоритмів криптоаналізу NTRU

Параметри NTRU	Атака "груба сила"	Класична атака "зустріч посередині"	Атака методом Ванга	Квантова атака "зустріч посередині" (метод Ксіонга)	Удосконалена квантова атака "зустріч посередині" (метод Ванга)
251	10^{52}	10^{24}	10^{26}	$3.3\cdot10^{27}+7\cdot10^{12}$	$3.5\cdot10^{18}+1.6\cdot10^{17}$
347	10^{72}	10^{34}	10^{36}	$4.6\cdot10^{37}+6.9\cdot10^{17}$	$9\cdot10^{25}+7.6\cdot10^{23}$
491	10^{100}	10^{48}	10^{50}	$3.2\cdot10^{52}+1.5\cdot10^{25}$	$3\cdot10^{35}+1.8\cdot10^{33}$
587	10^{120}	10^{58}	10^{60}	$4.5\cdot10^{60}+7.6\cdot10^{29}$	$3.8\cdot10^{41}+9\cdot10^{39}$
787	10^{159}	10^{77}	10^{79}	$1.5\cdot10^{81}+2.7\cdot10^{39}$	$4.6\cdot10^{54}+3.7\cdot10^{52}$

Реальну захищеність криптоперетворення ЕЦП NTRU пропонується оцінювати визначенням складності I_a здійснення атаки типу "повне розкриття" методом Ванга.

Складність і безпечний час з допустимою точністю можна визначити як:

$$I_a = \sqrt{C_{N+1}^{d_f}},\ t_a = \frac{I_a}{\gamma K} P_y = \frac{\sqrt{C_{N+1}^{d_f}}}{\gamma K} P_y.$$

При N=491, безпечний час NTRU буде дорівнювати

$$t_a = \frac{10^{35}+10^{33}}{10^{15}\cdot 3{,}15\cdot 10^7} \approx 10^{13}+10^{11}.$$

Оцінимо реальну захищеність криптоперетворення CFS від атаки методом Гровера. Для параметрів криптосистеми $(m,t) = (12,45)$ (табл. 1) маємо:

$$t_a = \frac{10^{44}}{10^{15}\cdot 3{,}15\cdot 10^7} = 10^{22}.$$

В результаті атак на класичних комп'ютерах NTRUSign може вважатися безпечною тільки при одноразовому використанні ключів [10], що значно звужує сферу її використання. Будемо враховувати, що цей криптопримітив не відповідає безумовному критерію для багаторазового використання.

Таким чином, тільки чотири підписи із тих, що аналізуються, відповідають безумовному критерію стійкості, тобто стійкі до квантового криптоаналізу. Серед них: підпис на кодах, підпис на решітках, підпис на хеш-функції, підпис на факторизації поліномів, для яких не винайдено ефективних квантових атак.

3. Порівняння постквантових підписів за умовними критеріями

В результаті аналізу стійкості криптопримітивів було обрано перспективні постквантові кандидати: на основі хеш-функцій (Hash Based); на основі завадостійких кодів (Code Based); на основі решіток (Lattice Based); на основі факторизації поліномів (Multivariate Polynomial Based). Із наведеного переліку криптографія на основі завадостійких кодів привертає увагу дослідників не тільки високою стійкістю до різного роду атак, а й високою швидкодією, а також додатковою перевагою в здатності до виправлення помилок при передачі сигналів по каналах передачі даних. Існують такі криптопримітиви на основі завадостійких кодів*:* CFS*,* Paralell CFS*,* підпис на основі криптосистеми McEliece. Криптографічний апарат хеш-функцій застосовується в алгоритмах підписів Lamport та XMSS. На сьогоднішній день існують схеми цифрового підпису на решітках BLISS та NTRU. Серед ЕЦП на основі факторизації поліномів найбільш відомий ЕЦП Rainbow. Проведемо порівняння вказаних криптоалгоритмів за умовними критеріями. Для цього проведемо аналіз відомих ЕЦП за швидкодією та обсягами ключів та підписів.

В табл. 3 порівнюються криптосистеми за умовними критеріями [1]. За одиницю часу обрано час підписання RSA з ключем довжиною 3072 біт. Рівень безпеки підписів позначається як k та означає рівень стійкості симетричного ключа, який має 128 біт довжини. Масштабування часу та ключа відображає залежність часу операцій від довжини ключів (відповідно рівень стійкості k*,* табл. 3) [1].

Швидкодія базових операцій BLISS більша, ніж ECDSA та RSA. Швидкість підписання операцій в секунду (Оп./сек.) - для BLISS - 7,958 Оп./сек., для ECDSA (множення точки) - 2,631 Оп./сек., для RSA - 548/79 Оп./сек [10]. Для тестування швидкодії електронного підпису CFS проведено комп'ютерне моделювання програмної реалізації на мові java. При цьому випадковим чином обиралася секретна перевірочна матриця H для (n,k,t) - коду Ріда-Соломона, що виправляє t помилок, а для знаходження вектора помилок використовувався алгоритм декодування γ Берлекемпа [13] і хеш-функція SHA-256 (перші 12 біт). Реальні параметри кода (n, k, t), що тестувалися: (15,9,3), (31,23,4), (63,53,5), (127,115,6), (255,241,7). Програмна реалізація зазначеної схеми цифрового підпису запускалася на комп'ютері з характеристиками: тип процесора – Intel Core i7-3630QM, тактова частота – 2,4 ГГц, об'єм оперативної пам'яті – 6 ГБ.

Таблиця 3

Порівняння алгоритмів підписів

Алгоритм		Час генерування ключів	Час підписання	Час перевірки	Обсяг відкритого ключа, біти	Обсяг закритого ключа, біти	Обсяг підпису, біти	Масштабування часу	Масштабування ключа
XMSS		100000	2	0.2	7296	152	19608	k^2	k^2
Підпис на решітках	BLISS	0.005	0.02	0.01	7000	2000	5600	k^2	k
	NTRUSign	0,06	0,01	0,001	3512	14048	3512	k^2	k
Rainbow		20	0.02	0.02	842400	561352	264	k^3	k^3
Підпис на кодах	CFS	5	2000	0,02	9437184	15000000	144	e^k	e^k
	CFS parallel	4	190	0,01	386048	613607	375	e^k	e^k
RSA		50	1	0.01	3072	24,576	3072	k^6	k^3
DSA		0.2	0.2	0.2	3072	3238	3072	k^4	k^3
ECDSA		0.05	0.05	0.05	512	768	512	k^2	k

На рис. 2 наведено результати тестування: по осі абсцис відображено зростання n, по осі ординат зростання часу генерації підпису та ключів CFS.

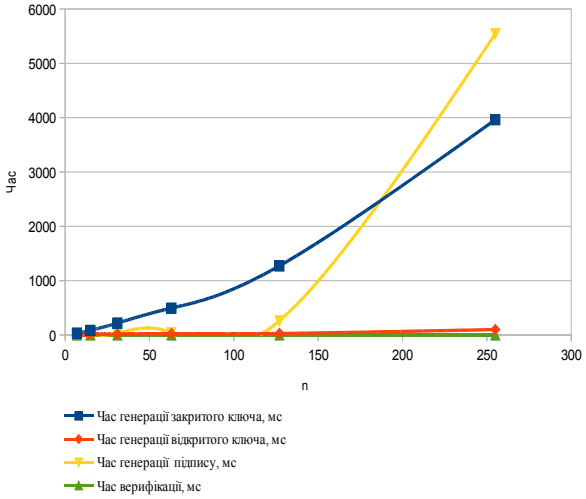

Рис. 2. Часові параметри програмної реалізації цифрового підпису CFS

Аналіз результатів моделювання алгоритму цифрового підпису свідчить про значне збільшення, з ростом довжини використовуваних кодів і їх виправляючої здатності, як часу генерації секретних ключів, так і часу генерації цифрового підпису. Спостерігається значне зростання часових витрат на генерацію секретних ключів і накладення цифрового підпису, а час верифікації підпису залишається постійним і досить малим. Більш вдалим алгоритмом є CFS parallel, який показує значне прискорення як накладення цифрового підпису, так і його перевірки (див. табл. 3). Тому в подальших дослідженнях будемо орієнтуватися саме на ці показники.

4. Методика та результати порівняльних досліджень алгоритмів ЕЦП

На основі результатів аналізу захищеності підписів (безумовний критерій), часу підписання і перевірки, часу генерації базових параметрів і ключів, довжини ключів та підпису (умовні критерії) зробимо загальне порівняння кращих алгоритмів на постквантовий період. Для цього порівняємо за допомогою метода аналізу ієрархій [20] підписи, які були відібрані при виконанні досліджень. Метою порівняння є обґрунтування найкращих алгоритмів ЕЦП, що відповідають умовним критеріям.

Сформулюємо основну суть та теоретичну значимість методики порівняння на основі метода аналізу ієрархій, і потім використаємо ці підходи для отримання результатів дослідження підписів.

Метод аналізу ієрархій (MAI) є одним із різновидів методу дерев [20]. Основним застосуванням методу є оцінювання альтернатив з метою вибору найкращих з них, на основі визначення їх вкладу у загальну ефективність досягнення оцінки глобальної альтернативи. У якості дерева альтернатив при використанні MAI виступає ієрархічний граф типу І-АБО (див. рис. 3). Далі за текстом цієї роботи всі елементи дерева називаються альтернативами.

Суть MAI полягає у тому, що на кожному рівні дерева здійснюється попарне порівняння альтернатив за їх внеском в досягненні альтернатив вищого рівня. Оцінка важливості (значимості внеску) альтернатив дається експертами або особою, що приймає рішення. Експертні оцінки (судження) обробляються, у результаті чого визначається системна оцінка внеску альтернативи кожного, у тому числі і альтернатив останнього рівня у досягнення глобальної оцінки альтернатив. Отже, метод аналізу ієрархій починається з декомпозиції глобальної оцінки альтернативи на частки (локальні) підальтернативи і побудови дерева альтернатив (див. рис. 3).

На рис. 3 позначено: r – рівень ієрархії, E_i – альтернатива. Вважається, що глобальна альтернатива є єдиною альтернативою першого рівня. В MAI критерії порівнюються попарно відносно їх впливу (ваги) на загальну для них характеристику. Нехай $E_1, E_2, ...E_n$,

множина із n альтернатив (в даному випадку підписів) і $v_1, v_2, ...v_n$, відповідно їх вага, або інтенсивність. Подібні оцінки надаються експертами та носять оціночний характер. Пропонується застосовувати шкалу оцінок, де перевага E_i над E_j представлена у вигляді цілого числа від 1 до 9. Чим більший пріоритет має перевага**,** тим більше числове значення вона отримує. Порівняймо попарно вагу кожного елемента множини відносно загальної для них властивості або мети.

Усі матриці попарних порівнянь (формальне представлення наведено у табл. 4) заповнюються таким чином: у лівому стовпці та першому рядку записуються альтернативи, що порівнюються; у верхній лівій клітинці записується альтернатива, по відношенню до якої проводиться оцінювання. Порівняння значущості альтернативи (за запропонованою шкалою) із собою дає одиницю.

Процедура обробки матриць попарних порівнянь полягає у застосуванні двох наступних алгоритмів: алгоритму обчислення вектору вкладу та алгоритму перевірки узгодженості оцінок [20]. Вектор вкладу – це середньо-геометричне $q_i^{(r-1)}$ для кожного рядка матриці [20], що виражає середню оцінку відносного впливу множини вагових коефіцієнтів на загальну оцінку порівняння.

Обчислення

$$q_i^{(r-1)} = \sqrt[n]{(v_i^{(r)} / v_1^{(r)}) \times (v_i^{(r)} / v_2^{(r)}) \times ... \times (v_i^{(r)} / v_n^{(r)})} \quad (1)$$

відбувається як множення всіх чисел рядка матриці та взяття кореня n-ї степені, де n – це кількість елементів рядка матриці.

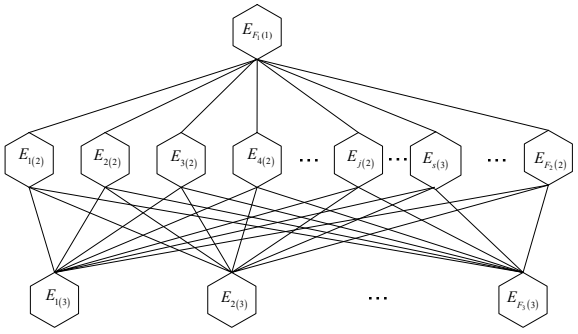

Рис. 3. Графічне представлення дерева (r = 3)

Таблиця 4

Матриця попарних порівнянь

	E_1	E_2	···	E_n
E_1	v_1 / v_1	v_1 / v_2	···	v_1 / v_n
E_2	v_2 / v_1	v_2 / v_2	···	v_2 / v_n
...	...	...	...	...
E_n	v_n / v_1	v_n / v_2	···	v_n / v_n

Отриманий за допомогою формули (1) вектор нормалізується діленням кожного числа на суму всіх чисел вектору:

$$\gamma_i^{(r-1)} = \frac{q_i^{(r-1)}}{\sum_{j=r}^{n} q_j^{(r-1)}}. \quad (2)$$

Розрахована величина $\gamma_i^{(r-1)}$ характеризує значущість альтернативи E_i у порівнянні із всіма іншими альтернативами.

Далі виконується згортка ієрархій – із векторів нормованих значень формуються проміжні матриці, які перемножуються на нормований вектор верхнього рівня ієрархії.

Згортка виконується ітеративно до тих пір, поки не будуть отримані глобальні значення ступеня переваги однієї альтернативи над іншою.

Проведемо аналіз відповідності алгоритмів ЕЦП умовним критеріям за методикою MAI. Для цього визначимо внесок кожного критерію до загальної оцінки порівняння. Результати цього аналізу представлені в табл. 5.

Тепер оцінимо кожний критерій і побудуємо матриці попарних порівнянь у вигляді табл. 5 відносно всіх алгоритмів підпису. В результаті обчислень за формулою (2) отримано значення $q_i^{(r-1)}$ та $\gamma_i^{(r-1)}$, які представлені в табл. 6.

Для отримання результуючого вектору пріоритетів перемножимо вектор пріоритетів 1-го рівня (табл. 5) і матрицю пріоритетів 1-го рівня (стовбці з γ із табл. 6):

$$\begin{pmatrix} 0{,}2114652507 \\ 0{,}0406938781 \\ 0{,}3255633447 \\ 0{,}1151083568 \\ 0{,}0406938781 \\ 0{,}2664752917 \end{pmatrix} \times \begin{pmatrix} 0{,}0455 & 0{,}2609 & 0{,}1786 & 0{,}375 & 0{,}4 & 0{,}0588 \\ 0{,}4091 & 0{,}3043 & 0{,}2857 & 0{,}3125 & 0{,}3333 & 0{,}1765 \\ 0{,}2273 & 0{,}3043 & 0{,}25 & 0{,}125 & 0{,}1333 & 0{,}4118 \\ 0{,}3182 & 0{,}1304 & 0{,}2857 & 0{,}1875 & 0{,}1333 & 0{,}3529 \end{pmatrix} = \begin{pmatrix} 0{,}15350674 \\ 0{,}28765833 \\ 0{,}23071647 \\ 0{,}24847257 \end{pmatrix}.$$

Таким чином, підписи, що пройшли відбір за безумовним критерієм, мають схожі характеристики за умовними критеріями. Результати порівняння досліджуваних алгоритмів представлені на рис. 4.

На основі проаналізованих даних отримано ранжируваний список ЕЦП, що відображає результат їх порівняння (1-й – найкращий, 4-й – гірший): 1) підпис на основі решіток 0,28; 2) підпис на основі завадостійких кодів 0,25; 3) підпис на основі факторизації поліномів 0,23; 4) підпис на основі хеш-функцій 0,15.

Таблиця 5

Порівняння критеріїв між собою

	Час генерування ключів	Час підписання	Час перевірки	Обсяг відкритого ключа	Обсяг закритого ключа	Обсяг підпису	q	γ
Час генерування ключів	1	3	0,75	1,5	3	1	1,7164	0,2115
Час підписання	0,3333	1	0,25	0,5	1	0,3333	0,3303	0,0407
Час перевірки	1,3333	4	1	2	4	1,3333	2,6425	0,3256
Обсяг відкритого ключа	0,6667	2	0,5	1	2	0,6667	0,9343	0,1151
Обсяг закритого ключа	0,3333	1	0,25	0,5	1	0,3333	0,3303	0,0407
Обсяг підпису	1,1667	3,5	0,875	1,75	3,5	1,1667	2,1629	0,2665

Таблиця 6

Вектори вкладу в матриці парних порівнянь

	Порівняння за критерієм швидкості генерування ключів		Порівняння за критерієм швидкості підписання		Порівняння за критерієм швидкості перевірки		Порівняння за критерієм довжини відкритого, ключа		Порівняння за критерієм довжини закритого ключа		Порівняння за критерієм довжини підпису	
	q	γ	q	γ	q	γ	q	γ	q	γ	q	γ
Підпис на основі хеш-функцій	0,2374	0,0455	1,101	0,2609	0,7268	0,1786	1,6381	0,375	1,8128	0,4	0,2985	0,0588
Підпис на основі решіток	2,1363	0,4091	1,2845	0,3043	1,1629	0,2857	1,3651	0,3125	1,5107	0,3333	0,8954	0,1765
Підпис на основі факторизації поліномів	1,1868	0,2273	1,2845	0,3043	1,0175	0,25	0,546	0,125	0,6043	0,1333	2,0893	0,4118
Підпис на основі завадостійких кодів	1,6616	0,3182	0,5505	0,1304	1,1629	0,2857	0,819	0,1875	0,6043	0,1333	1,7908	0,3529

Проведені дослідження показують перевагу підписів на основі решіток та завадостійких кодів у порівнянні з іншими криптопримітивами.

Завдяки невеликим розмірам ключів та підписів криптосистеми на решітках (NTRU, BLISS) отримують область переважного використання в пристроях з обмеженою пам'яттю. Одноразові криптосистеми (NTRUSign) можуть знайти застосування в системах анонімних платежів типу Zerocoin. Через анонімність користувачів в цих протоколах термін дії секретного ключа ЕЦП обмежений одноразовим використанням.

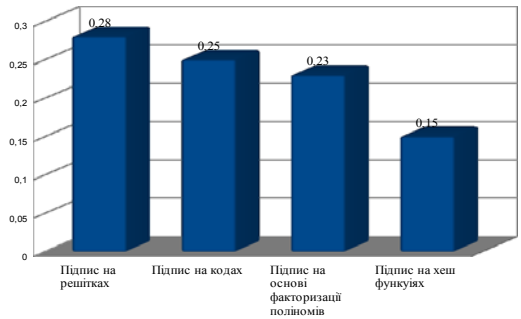

Рис. 4. Результати порівняння підписів у вигляді діаграми

Постквантові криптосистеми, що порівнюються, загалом мають швидкодію таку саму або кращу, ніж у класичних аналогів для однакових рівнів безпеки. Але вони мають, разом з тим, більші обсяги ключів і розміри підписів, ніж DSA та ECC. Перевагою криптосистем на основі завадостійких кодів є малий обсяг підпису та велика швидкість перевірки, що може дати приріст в швидкості обробки даних на серверній частині систем мікроплатежів.

Результати порівнянь за запропонованою в роботі методикою дозволяють сформулювати предмет та напрямок подальших досліджень. Доцільним є аналіз моделей та методів ЕЦП на кодах та решітках, зокрема, питання оцінки забезпечення гарантованої стійкості.

Висновки

За допомогою використання математичного апарату методу аналізу ієрархій проведено порівняння цифрових підписів і показано перевагу криптоперетворень ЕЦП на завадостійких кодах та решітках над іншими порівнюваними алгоритмами за застосованими критеріями порівняння. Отримано ранжування ЕЦП по інтегральному критерію. Сформульовано рекомендації до застосування конкретних криптопримітивів в умовах появи повномасштабного квантового комп'ютера**.** Використання методу аналізу ієрархій дозволяє пов'язати сферу застосування та характеристики самих підписів, що дає можливість більш гнучко-

го реагування на вимоги захисту інформації в умовах дії нових криптопротоколів і алгоритмів ЕЦП. Порівняні підписи мають різні швидкісні характеристики, обсяги параметрів та обмеження застосування.

Список літератури

1. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування [Текст]: монографія / І.Д. Горбенко, Ю.І. Горбенко. – Харк. нац. ун-т радіоелектроніки, ЗАТ "Ін-т інформ. технологій". – Х. : Форт, 2012. – 868 с.

2. ETSI White Paper No. 8, Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges, June 2015. [Електронний ресурс]. – Режим доступу до ресурсу: http://www.etsi.org/ - 24.07.2016 - Загол. з екрану.

3. Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010, Proceedings NSA acknowledges need for quantum-safe crypto. [Електронний ресурс]. – Режим доступу до ресурсу: http://www.idquantique.com/nsa-quantum-safe-crypto/- 24.07.2016 - Загол. з екрану.

4. NISTIR 8105 DRAFT Report on Post-Quantum Cryptography. National Institute of Standards and Technology Internal, Report 8105. [Електронний ресурс]. – Режим доступу до ресурсу: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf - 24.07.2016 - Загол. з екрану.

5. Evaluating Post-Quantum Asymmetric Cryptographic Algorithm Candidates / Tolga Acar, Josh Benaloh, Craig Costello, Dan Shumow. - MSR Security and Cryptography Group. [Електронний ресурс]. – Режим доступу до ресурсу: http://csrc.nist.gov/groups/ST/post-quantum-2015/presentations/session7-shumow-dan.pdf – 24.07.2016 – Загол. з екрану.

6. Bernstein D. Post-quantum cryptography [Text] / D. Bernstein, J. Buchmann, E. Dahmen. – Berlin: Springer, 2009. – 246 p.

7. Горбенко Ю.І. Аналіз шляхів розвитку криптографії після появи квантових комп'ютерів / Ю.І. Горбенко, Р.С. Ганзя // Вісник Національного університету "Львівська політехніка". – 2014. – № 806. – С. 40-48.

8. Daniel J. Bernstein. Sphincs: practical stateless hash-based signatures. Cryptology ePrint Archive, Report 2014/795, 2014 / Daniel J. Bernstein, Daira Hopwood, Andreas Helsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Peter Schwabe, Zooko Wilcox O'Hearn. [Електронний ресурс]. – Режим доступу до ресурсу: http://eprint.iacr.org/- 24.07.2016 - Загол. з екрану.

9. Ray A. Perlner. Quantum resistant public key cryptography: a survey / Ray A. Perlner, David A. Cooper // In Proceedings of the 8th Symposium on Identity and Trust on the Internet (IDtrust '09), Kent Seamons, Neal McBurnett, and Tim Polk (Eds.). – New York, ACM, 2009. – P. 85-93.

10. Enhanced Lattice-Based Signatures on Recon gurable Hardware Extended Version [Електронний ресурс]. – Режим доступу до ресурсу: https://eprint.iacr.org/2014/254.pdf. – Загол. з екрану.

11. Богданов А.Ю. Квантовые алгоритмы и их влияние на безопасность современных классических криптографических систем / А.Ю. Богданов, И.С. Кижватов. – М.: РГГУ, 2005.

12. Finiasz M. Parallel-CFS - Strengthening the CFS McEliece-Based Signature Scheme / M. Finiasz // In A. Biryukov, G. Gong, D.R. Stinson, editors, Selected Areas in Cryptography, vol. 6544 of Lecture Notes in Computer Science. – Springer Berlin Heidelberg, 2011. – P. 159-170.

13. Берлекэмп Э. Алгебраическая теория кодирования / Э. Берлекэмп. – М.: Мир, 1971. – 234 с.

14. McEliece R.J. A Public-Key Criptosystem Based on Algebraic Theory / R.J. McEliece // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – P. 114-116.

15. Whyte W. IEEE P1363.1 Draft 10: Draft Standard for Public Key Crypto-graphic Techniques Based on Hard Problems over Lattices [Електронний ресурс] / N. Howgrave-Graham, J. Hostein, J. Pipher, J.H. Silverman. – Режим доступу до ресурсу: http://grouper.ieee.org/groups/1363/WorkingGroup/contact.html.

16. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer / P. Shor // SIAM J. Comput., 1997. – 26 (5), P. 1484-1509.

17. Grover L. A fast quantum mechanics algo- rithm for database search / L. Grover // Proceeding of the 28th ACM Symposium on Theory of Computation. – New York: ACM Press, 1996. – P. 212-219.

18. An Improved MITM Attack Against NTRU / Z. Xiong, J. Wang, Y. Wang, T. Zhang, L. Chen // International Journal of Security and Its Applications. – 2012. – Vol. 6, No. 2. – P. 269-274.

19. Wang H. An efficient quantum meet-in-the-middle attack against NTRU-2005 / H. Wang, M.A. Zhi, M.A. ChuanGui // Chinese Science Bulletin, 2013. – Vol. 58, No. 28-29. – P. 3514-3518.

20. Саати Т. Принятие решений. Метод анализа иерархий: пер. с англ. / Т. Саати. – М.: Наука, 1977. – 434 с.

Надійшла до редколегії 3.10.2016

Рецензент: д-р техн. наук проф. С.Г. Рассомахін, Харківський національний університет ім. В.Н. Каразіна, Харків.

АНАЛИЗ И СРАВНИТЕЛЬНЫЕ ИССЛЕДОВАНИЯ АЛГОРИТМОВ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ ДЛЯ ПОСТКВАНТОВОГО ПРИМЕНЕНИЯ

А.В. Шевцов, И.И. Сватовський, Т.Ю. Кузнецова

Анализируются постквантовые криптографические примитивы электронной цифровой подписи и обосновываются условия их применения в Украине для обеспечения безопасности информационных технологий на постквантовый период. Сравниваются кандидаты цифровых квантово-устойчивых подписей по выбранным критериям. Разрабатываются рекомендации по применению избранных криптопримитивов в зависимости от сферы использования.

***Ключевые слова**: постквантовая криптография, алгебраические решётки, электронная цифровая подпись, помехоустойчивые коды.*

ANALYSIS AND COMPARATIVE RESEARCH OF POSTQUANTUM DIGITAL SIGNATURE ALGORITHMS

O.V. Shevtsov, I.I. Svatovskij, T.U. Kuznetsova

In the paper post-quantum signatures are analyzed. Restrictions and conditions of implementation of cryptographic primitives in a post-quantum period are considered. We compare quantum-resistant signatures on defined criteria. As a result we propose recommendations for implementation of signature algorithms depending on application sphere.

***Keywords**: post-quantum cryptography, code-based cryptography, digital signature, algebraic lattice.*