УДК 003.26:004/056

КВАНТОВІ КРИПТОГРАФІЧНІ АЛГОРИТМИ ЕЛЕКТРОННОГО ПІДПИСУ НА ОСНОВІ МУЛЬТИВАРІАТИВНИХ КВАДРАТИЧНИХ ПЕРЕТВОРЕНЬ

Д. В. ГАРМАШ, О. О. БАКЛИКОВ, Н.В. ФІЛАТОВА, І.Д.ГОРБЕНКО

Наводяться вимоги до постквантових алгоритмів асиметричних криптоперетворень. Вказується на актуальність та необхідність пошуку, дослідження, стандартизації та застосування криптографічного примітиву типу електронний підпис (ЕП). Розглядається сутність та можливості застосування мультиваріативних квадратичних перетворень в ході реалізації ЕП, робиться попередній аналіз їх властивостей та наводиться практичний приклад.

Ключові слова: вимоги до постквантових електронних підписів, електронний підпис, квантове криптоперетворення, математичні основи мультиваріативних перетворень, мультиваративне квадратичне перетворення для електронного підпису.

ВСТУП

У 2016 році у США та ЄС розпочалися активні роботи щодо підготовки до проведення конкурсів відносно методів та на їх основі майбутніх кандидатів квантово-захищених алгоритмів криптографічних перетворень. Підтвердженням цьому є заяви АНБ США та технічний звіт NIST США [1,2], розпочаті широкі попередні дослідження та підтримка провідних криптографів проблем постквантової криптографії[1]. Так АНБ та NIST ініціювали роботи щодо організації конкурсу на нові стандарти квантвозахищених криптографічних алгоритмів. Необхідно відмітити значне число досліджень в ЄС[3] та публікацій на міжнародному рівні і в Україні [4,5].

У лютому 2016 року свої плани NIST анонсував на VII Міжнародній конференції з постквантової криптографії, що проходила у Японії [3,4]. У подальшому планується підготувати вимоги та оголосити у 2017 конкурс на кращі криптопримітиви для застосування у постквантовий період. Також планується протягом 3 – 5 років провести їх аналіз та порівняння, а потім у 2020 – 2022 роках прийняти нові криптографічні постквантові стандарти.

Серед множини криптографічних примітивів важливе значення мають електронні підписи (ЕП), що пояснюється їх широким застосування та можливостями великих втрат у фінансовій сфері та економіці, зрозуміло у випадку компрометації сьогодні існуючих стандартизованих ЕП [1 – 5].

Зважаючи на актуальність та необхідність створення постквантових алгоритмів ЕП у цьому напрямі уже розпочаті дослідження, певною мірою визначено математичні основи, на яких можуть бути побудовані постквантові алгоритми ЕП та асиметричного шифрування. За результатами вказаної VII міжнародній конференції [4] в основному визначені шляхи створення постквантових алгоритмів ЕП. Основними з них є дослідження, що грунтуються на використанні [1 – 10]:

- мультиваріативного квадратичного криптоперетворення (multivariate-quadratic-equations cryptography) на основі запропонованого Matsumoto та Imai підходу[6];
- перетворення на основі геш-дерева Меркеля (Merkle), у свою чергу побудованого з використанням ідеї Lamport та Die про підпис одного повідомлення [7];
- криптоперетворення у фактор кільці, стійкість якого доводиться на основі використання математичного апарату алгебраїчних решіток (Lattice-based cryptography). Найбільший інтерес у цьому класі є схема асиметричного шифрування Hoffstein-Pipher–Silverman “NTRU”, згідно з якою прийнято та застосовується стандарт США X9.98[8];
- криптоперетворення на основі застосування кодів (Code-based cryptography), класичним прикладом якого є схема асиметричного шифрування та ЕП Mc Eliece з кодами Гоппи (Goppa) [9];
- криптоперетворення та основі використання математичного апарату ізогеній еліптичних кривих[10].

Наш попередній аналіз дозволив зробити висновок, що усі названі криптоперетворення можуть бути використані для побудови постквантових ЕП, тому вони заслуговують відповідної уваги.

Метою цієї статі є узагальнення вимог до постквантових алгоритмів ЕП та попередній аналіз сутності, можливостей та властивостей криптографічного перетворення типу ЕП на основі використання мультиваріативного квадратичного перетворення.

1. ВИМОГИ ДО ПОСТКВАНТОВИХ ЕП

Аналіз показав, що уже сьогодні США на рівні NIST, Європейський Союз на рівні ETSI, Японія та Германія розпочали активну роботу з формування вимог до квантово-захищених криптоалгоритмів. Так, до кінця 2026 року планується в основному розробити та розпочати відкрите обговорення квантово-захищених алгоритмів [1 – 4]. За результатами вказаних робіт усі вимоги можна поділити на безумовні

або цільові, тобто відносно криптографічної стійкості, техніко-економічні та техніко-експлуатаційні.

Як мінімальні вимоги до можливих кандидатів можна віднести [5]:

- безумовне доведення криптостійкості проти квантового криптоаналізу;
- забезпечення однієї з функцій криптоперетворення, наприклад ЕП;
- відкритість алгоритму ЕП для криптографічного аналізу криптографічною спільнотою;
- можливість реалізації та застосування ЕП у широкому діапазоні платформ.

Продовжується подальший розгляд вимог до постквантових примітивів, їх конкретизація здійснюється, як уже вказувалось вище, у трьох напрямках:

-вимоги відносно стійкості до криптографічного аналізу, причому вони визнаються безумовними, тобто повинні кандидатом виконуватись безумовно;

- техніко-економічні вимоги в основному в частині часової та просторової складностей (складність обчислень та витрати на пам'ять); технічні характеристики реалізації алгоритмів;

- техніко-експлуатаційні вимоги в частині простоти реалізації та використання.

Сьогодні вказані вимоги уточнюються та деталізуються, ми в подальшому покладемо в ході аналізу за основу та посилатимемося на необхідні в подальшому.

2. МАТЕМАТИЧНІ ОСНОВИ МУЛЬТИВАРІАТИВНИХ КВАДРАТИЧНИХ ПЕРЕТВОРЕНЬ

Механізм (схема) мультиваріативних квадратичних перетворень Т. Мацумото і Х. Імаі представили на конференції Eurocrypt у 1988 р [6]. Пізніше в цьому напрямі французом Жаком Патарином були досліджені "мономіальні криптосистеми приховування інформації» [4,6,11]. Вони засновані на розширенні поля $i(t)$ (у поліноміальні формі). Пізніше Ж. Патарин розробив інші механізми (схеми) перетворень. У співпраці з Евиадом Кипнісом і Луї Губіном в 1997 році він представив перетворення "Balanced Oil and Vinegar", а у 1999 "Unbalanced Oil and Vinegar". У подальшому запропоновані перетворення практичної реалізації не отримали. Але з часом, коли з'явились постквантові загрози, увага була звернута і на мультиваріативні квадратичні перетворення. Сьогодні ці перетворення розглядаються криптологами як реальні кандидати на постквантовий ЕП.

Мультиваріативні перетворення грунтуються на використанні кінцевого поля [6,11 – 13]

$$k - \frac{GF[2]}{x^2 + x + 1}, \qquad (1)$$

в якому 2^2 елементів. Для спрощення вони позначаються множиною чисел $\{0,1,2,3\}$. Причому 0 є нулем у полі k, 1 є одиницею, 2 є поліномом x, а 3 є поліномом 1+x. По суті, коефіцієнти квадратичних поліномів приймають значення над полем $4=2^2$. Як квадратичні поліноми вибираються такі:

$$G_0 = (x_1, x_2, x_3) =$$
$$= 1 + x_2 + 2x_0x_2 + 3x_1^2 + 3x_1x_2 + x_2^2;$$
$$G_1 = (x_1, x_2, x_3) =$$
$$= 1 + 3x_0 + 2x_1 + x_2 + x_0^2 + x_0x_1 + 3x_0x_2 + x_1^2;$$
$$G_2(x_1, x_2, x_3) =$$
$$= 3x_2 + x_0^2 + 3x_1^2 + x_1x_2 + 3x_2^2.$$

Вважається, що наведені поліноми є багато вимірними поліномами над кінцевим полем та вони можуть застосовуватися у багатофакторній криптографія під час розробки асиметричних криптографічних примітивів.

Механізм (схема) Мацумото та Імаі (MIA). Для цієї схеми використовується центральне рівняння над полем розширення E ступеня n. Воно має вигляд

$$P(x') := x^{'q^\lambda + 1} \qquad (2)$$

для $q := |F|$ та деякого $\lambda \in N$.

Також між F^n та E, в процесі перетворення використовується коефіцієнт бієкції. Нехай вектор $a \in F^n$ подається у вигляді $(a_1, \ldots, a_n)$, причому $a_i \in F$, нехай також $b \in E$ та має вигляд $b_{n-1}t^{n-1} + \ldots + b_1t + b_0$ з $b_i \in F$, а $i(t)$ є визначальним многочленом E. Далі, нехай $x^{'q^\lambda}$ є лінійним рівнянням над F для будь-якого $\lambda \in N$, а x' призводить до квадратних рівнянь над F. Причому вказана бієкція справджується, якщо $\gcd(q^n - 1,\ q^\lambda + 1) = 1$.

Рівняння приховування в полі. Використовується та сама ідея, як у MIA, але для влаштування люку використовується інша ідея. Як і для MIA, використовуються центральні рівняння над полем розширення E зі ступенем n. Вони мають вигляд:

$$P'(x') := \sum_{\substack{0 \le ij \le d \\ q^i + q^j \le d}} C'_{i,j} x^{'q^i + q^j} + \sum_{\substack{0 \le k \le d \\ q^k \le d}} B'_k x^{'q^k} + A', \qquad (3)$$

де $\begin{cases} C'_{i,j} x^{q^i + q^j} \text{ для } C'_{i,j} \in E - \text{квадратичні члени} \\ B'_k x^{q^k} \text{ для } B'_k \in E - \text{лінійні члени} \\ A' \text{для } A' \in E - \text{константа} \end{cases}$

для $i, j \in N$ та деякого $d \in N$.

Базові класи. Ґрунтуються на незбалансованій схемі Оіла та Вінежера (UOV). Використовуються значення vinegar та oil (v та o). Мається $n = v + o$ та потрібно

$v = 2o \ldots 3o$ для безпечної схеми. Крім того, є $o = m$. При цьому центральні поліноми мають вигляд:

$$p_i'\left(x_1', \ldots, x_n'\right) := \sum_{j=1}^{v}\sum_{k=1}^{n}\gamma_{i,j,k}' x_j' x_k' + \sum_{j=1}^{n}\beta_{i,j}' x_j' + a_i' \quad (4)$$

для $1 \le i \le m$ та коефіцієнтів

$$\alpha_i', \beta_{i,j}', \gamma_{i,j}' \in F$$

Примітка: ці рівняння стають лінійними, якщо значення присвоюються до значень Віженера $x_1', \ldots, x_v'$.

Далі застосовуються поетапні трикутні системи (STS). В них система P має такий вигляд:

$$\text{Крок1}\begin{cases} p_1' & \left(x_1', \ldots, x_r'\right) \\ & \vdots \\ p_r' & \left(x_1', \ldots, x_r'\right) \end{cases} \quad (5)$$

$$\text{Крок } l\begin{cases} p_{(l-1)r+1}' & \left(x_1', \ldots, x_r', \ldots, x_{(l-1)r+1}', \ldots, x_{lr}'\right) \\ & \vdots \\ p_{lr}' & \left(x_1', \ldots, x_r', \ldots, x_{(l-1)r+1}', \ldots, x_{lr}'\right) \end{cases}.$$

3. КЛЮЧОВІ ДАНІ ТА БАЗОВІ ПОЗНАЧЕННЯ

Мультиваріативні квадратичні перетворення є криптографічними, якщо під час його виконання застосовуються спеціальні дані – асиметричний ключ. Він складається з відкритого ключа $K_в$ та особистого (таємного) K_o. Основною вимогою до асиметричної пари ($K_в$, K_o) є вимога, щоб

$$Kв \ne Ko \quad (6)$$

та щоб при знанні одного із них – наприклад, як на практиці – відкритого, визначення таємного було експоненційно складним. Як мінімум у деяких випадках – субекспоненційно складним.

Відкритий ключ $K_в$ будується із поліномів скінченного поля P. На практиці це завжди сукупність коефіцієнтів $p_i's$, що складаються (розміщаються) у певному порядку. Це робиться з метою зменшення складності обчислень. Оскільки $K_в$ є відкритий ключ, то $P(0)$ завжди дорівнюється нулю.

Таємний ключ складається з інформації, що міститься в $S, T\, i\, Q$. Тобто, складається з $\left(M_S^{-1}, c_S\right), \left(M_T^{-1}, c_T\right)$ та усіх параметрів, які існують в Q. Теоретично, один з c_S та c_T може бути зайвим, але він зберігається у будь-якому випадку [4,6].

Для того, щоб перевірити підпис або зашифрувати інформацію [5,6], застосовується відкритий ключ у вигляді

$$z = P(w). \quad (7)$$

Для того, щоб підписати або розшифрувати, застосовується таємний ключ у вигляді

$$y = T^{(-1)}(z),\ x = Q^{-1}(y) \text{ і } w = S^{-1}(x), \quad (8)$$

але потрібно зважити на те, що це може бути тільки один з багатьох прообразів, який не обов'язково є зворотною функцією у змісті криптографічного перетворення.

Необхідно відмітити, що навіть якщо ми обмежимося криптосистемами, для яких відкритий ключ є набором поліномів $P = (p_1, \ldots, p_m)$ у змінних $w = (w_1, \ldots, w_n)$, де всі змінні і коефіцієнти знаходяться в $K=F_q$, шлях, який приховує перетворення (можливо лазівку) не є унікальним.

Проте, повідомлення завжди можна захистити за допомогою афінних перетворень S,T. Тобто, $P = T\,o\,Q\,o\,S : K^n \to K^m$, або

$$P: w=(w_1,..,w_n) \to x=M_S w+c_S \to y \to z=M_T y+c_T=(z_1,..,z_m) \quad (9)$$

Також необхідно відмітити, що у будь-якому перетворенні головне перетворення Q належить до певного класу квадратичних відображень, при чому для нього зворотне перетворення з точки зору складності виконання є поліноміально складним. При цьому таємні відображення S та T є афінними (можливо навіть лінійними) та повного рангу. В цьому випадку x_j називається центральною змінною, а пполіноми y_j та x називаються центральними поліномами. Далі, коли необхідно знайти різницю між змінною та значенням, то її позначають як $y_i = q_i(x)$. При цьому ключ K_C є основою такого механізму.

Також наведемо позначення, які використовуються далі. Розмір блоку шифру або набору повідомлень – m елементів F_q. Блок відкритого тексту або розмір підпису – n елементів у скінченному полі F_q. Розмір відкритого ключа $\frac{mn(n+3)}{2}$,

F_q – елементи, які зберігаються.

Розмір таємного ключа оцінюється як

$$\left(n^2 + m^2 + [\#\text{параметри в } Q]\right), \quad (10)$$

де F_q – елементи, які зберігаються у відповідному форматі.

Складність таємного перетворення оцінюється як

$$\left(n^2 + m^2\right). \quad (11)$$

Складність відкритого перетворення з наближенням можна оцінити як

$$mn^2 / 2F^q. \quad (12)$$

Трудомісткість (складність) генерації ключа - n^2 в полі F оцінюється в інтервалі

$$(O(n^4) - O(n^5)). \quad (13)$$

Попередній аналіз дозволив виявити основний недолік мультиваріативних перетворень – суттєве збільшення, порівняно з традиційними криптосистемами RSA, DSA або ECC, довжини ключів. Але вказане, як і інші питання властивостей мультиваріативного перетворення та умов його застосування, вимагають непростих досліджень.

4. КРИПТОСИТЕМА ЕП НА ОСНОВІ МУЛЬТИВАРІАТИВНОГО КВАДРАТИЧНОГО ПЕРЕТВОРЕННЯ

Відкритий ключ у такій системі є послідовністю [4,6]

$$P_1, P_2, \ldots, P_{2b} \hat{I} F_2[w_1, \ldots, w_{4b}]. \quad (14)$$

Із *2b* поліномів з *4b* змінних. $w_1, \ldots, w_{4b}$ з коефіцієнтами у полі $F_2 \in \{0,1\}$. Кожний поліном має мати ступінь не більше 2 та без квадратичних термів, та поданий як послідовність

$$1, w_1, \ldots, w_{4b}, w_1w_2, w_1w_3, \ldots, w_{4b-1}w_{4b}. \quad (15)$$

У цілому, відкритий ключ має довжину $16b^3 + 4b^2 + 2b$ бітів. Наприклад, для *b=128*, розмір відкритого ключа складатиме 4 Mbyte. Для інших b дані наведено в таблиці 1.

Таблиця 1

Параметри відкритого ключа залежно від b

Значення b	$16b^3 + 4b^2 + 2b$ бітів	Відкритий ключ
128	$16*128^3 + 4*128^2 + 2*128$	33620224 бітів
256	$16*256^3 + 4*256^2 + 2*256$	268698112 бітів
512	$16*512^3 + 4*512^2 + 2*512$	2148533248 бітів

Значною перевагою підпису на основі MQ-криптографії можна вважати те, що підпис є коротким. Інші MQ-підписи з більш коротшими відкритими ключами мають підписи ще у більшості випадків ще коротші. Для здійснення атаки зловмиснику необхідно знайти послідовність з $4b$ $w_1, \ldots, w_{4b}$ бітів, що породжує 2b зазначених вище вихідних бітів, це і є головною проблемою для нього.

У таблиці 2 наведені значення ймовірностей вгадування послідовності із *4b* бітів

$$(P_1(w_1, \ldots, w_{4b}), \ldots, P_{2b}(w_1, \ldots, w_{4b}))$$

В таблиці 3 наведені значення складності вгадування послідовності із *4b* бітів для більш досконалих атак, таких як «XL» -атаки.

Таблиця 2

Ймовірності вгадування послідовності із 4b бітів

Значення b	2^{-2b}	Ймовірність вгадування
128	$2^{-2\times128}$	$8.636168555094445e-78$
256	$2^{-2\times256}$	$7.458340731200207e-155$
512	$2^{-2\times512}$	$5.562684646268003e-309$

Таблиця 3

Значення складності вгадування послідовності із *4b* бітів для «XL» -атаки.

Значення b	2^{2b}	Кількість операцій
128	$2^{2\times128}$	$1.157920892373162e+77$
256	$2^{2\times256}$	$1.3407807929942597e+154$
512	$2^{2\times512}$	$1,797693134862315907729305190789e+308$

Але для більшості квадратичних поліномів $P_1,\ldots, P_{2b}c\ 4b$ змінними на даний момент можуть бути зроблені невідомі атаки за 2^{2b} операцій. Ця проблема вирішується вже тривалий час.

Важливою перевагою підпису на основі MQ-криптографії над HB - підписом є те, що підпис є коротким. Інші MQ-системи мають ще коротші підписи і, у більшості випадків, більш короткий відкритий ключ.

Алгоритм електронного підпису. Розглянемо як здійснюється електронний підпис під час застосування мультиваріативного перетворення [4,6].

Підписувач генерує відкритий ключ $P_1,\ldots, P_{2b}$ з таємною структурою, більш конкретно, з HFE^{v-} структурою, яка дозволяє підписувачу вирішити вищенаведену проблему за прийнятний час. Можливо, що зловмисник зможе розкрити HFE^{v-}структуру у відкритому ключі або у відкритому ключі разом із послідовністю легітимних підписів. Але така атака поки ще не відома.

Нехай зафіксовано стандартний незвідний поліном $\phi\in F_2(t)$ ступеню $3b$. Визначимо *L* як поле $F2(t)\big/\varphi$ розмірністю 2^{3b}. Критичним кроком під час формування підпису є пошук кореня таємного одномірного (uniraviate) поліному малого ступеня над L, а саме, поліному в L[x] зі ступенем не більше ніж *2b*. Існує декілька стандартних алгоритмів для вирішення цієї задачі за час $b^{O(1)}$.

Таємний поліном обирається так, щоб мати всі ненульові експоненти вигляду 2^i+2^j або 2^i.

Якщо елементи $x\in L$ продані у вигляді

$$x_0+x_1t_1+\ldots+x_{3b-1}, \text{ де } x_i\in F_2, \qquad (15)$$

тоді

$$x_2=x_0+x_1t^2+\ldots+x_{3b-1}t^{6b-2}$$
$$x_4=x_0+x_1t^4+\ldots+x_{3b-1}t^{12b-4}$$

і т. д.

Таким чином, $x^{2i}+^{2j}$ є квадратичним поліномом зі змінними $x_0,\ \ldots, x_{3b-1}$.

Деякі прості перетворення приховують структуру цього поліному і породжують відкритий ключ.

Таємний ключ підписувача має три компоненти.

1. Оборотна матриця *S* розмірністю $4b\times4b$ з коефіцієнтами в F_2.
2. Поліном $Q\in L[x,n_1,n_2,\ \ldots,n_b]$, де кожний терм має одну з шести можливих форм:
3. $$lx^{(2^i+2^j)},$$
$$\text{де } lL,2^i<2^j,2^i+2^j2b;$$
$$\text{де } lx^{(2^i)}j,$$
$$\text{де } l\in L,2^i\le2b \qquad (16)$$

$$lv_iv_j$$
$$lx^{(2^i)}$$
$$ln_j$$
$$l$$

Якщо $b=128$, то ми маємо *944b* можливих термів, кожний з яких має 384-бітний коефіцієнт *l*, а загальний об'єм складатиме 443 Kbytes.

4. Матрицю *T* розмірністю $2b\times3b$ рангу *2b* з коефіцієнтами у F_2.

В цьому випадку підписувач обчислює відкритий ключ

$$(x_0,x_1,\ \ldots,x_{3b-1},v_1,v_2,\ldots,v_b) \qquad (17)$$

як S раз вектор $(w_1,\ \ldots,w_{4b})$ всередині фактор-кільця

$$L\left[\omega_1,\ldots,\omega_{4b}\right]/\left(\omega_1^2-\omega_1,\ldots,\omega_{1b}^2-\omega_{4b}\right).$$

Далі необхідно обчислити

$x=\sum x_it^i$ та $y=Q\left(x,V_1,V_2,\ldots,V_b\right)$

та подати у вигляді

$$Y_0 + Y_1 t + \ldots + Y_{3b-1} t^{3b-1}$$

де кожний $Y_i F_2 \left[\omega_1, \ldots, \omega_{4b}\right]$.

Потім обчислити $(P_1, P_2, \ldots, P_{2b})$ як T раз вектор-стовпчик

$$(Y_0, Y_1, \ldots, YP_{3b-1}).$$

Безпосередньо підписування здійснюється у зворотному напрямку з використанням тих самих конструкцій.

1. Починаємо з величини $P_1, P_2, \ldots, P_{2b}$. Спочатку для того, щоб отримати значення $(Y_0, Y_1, \ldots, Y_{3b-1})$ розв'язується таємне лінійне рівняння

$$T\left(Y_0, Y_1, \ldots, YP_{3b-1}\right) = \left(P_1, P_2, \ldots, P_{2b}\right). \quad (17)$$

При цьому існує 2^b можливих варіантів розв'язання $(Y_0, Y_1, \ldots, Y_{3b-1})$. Обираємо випадковим чином одне із них.

2. Обираємо випадково значення $V_1, V_2, \ldots, V_{b1} \in F_2$ і підставляємо його у таємний поліном $Q\left(x, V_1, V_2, \ldots, V_b\right)$, отримуючи поліном $Q\left(x\right) \in L\left[x\right]$.

3. Обчислюємо

$$Y = Y_0 + Y_1 t + \ldots + Y_{3b-1} t^{3b-1} \in L$$ і

вирішуємо $Q\left(x\right) = Y$, внаслідок чого отримуємо $x \in L$. У випадку, коли існує декілька коренів, процес починається з початку.

4. Запишемо x як

$$x_0 + x_1 t + \ldots + x_{3b-1} t^{3b-1},$$

де $x_0, x_1, x_{3b-1} \in F_2$.

Розв'язуємо таємне рівняння

$$S(\omega_1, \ldots, \omega_{4b} = \left(x_0, \ldots, x_{3b-1}, v_1, \ldots, v_b\right) \quad (18)$$

та отримуємо підпис.

Цей приклад є прикладом з класу *HFE*^{v} – конструкцій, що запропоновані Potanin у 1996 році. В ньому *HFE*- приховане рівняння в полі $Q\left(x\right) = Y$. «–» означає пропуск декількох бітів. Тобто $Q\left(x\right) = Y$ є еквівалентом 3b рівнянь, але публікується тільки 2b рівнянь. «v» – означає «vinegar» змінні $v_1, v_2, \ldots, v_b$.

Безпосереднє (чисте) HFE перетворення, тобто без пропусків бітів та без v-змінної може бути атаковано за $2^{(lgb)^2}$ операцій атакою Grobner але *HFE*^{v}-перетворення протистоятиме такій атаці. В таблиці 4 наведено оцінки складності такої атаки.

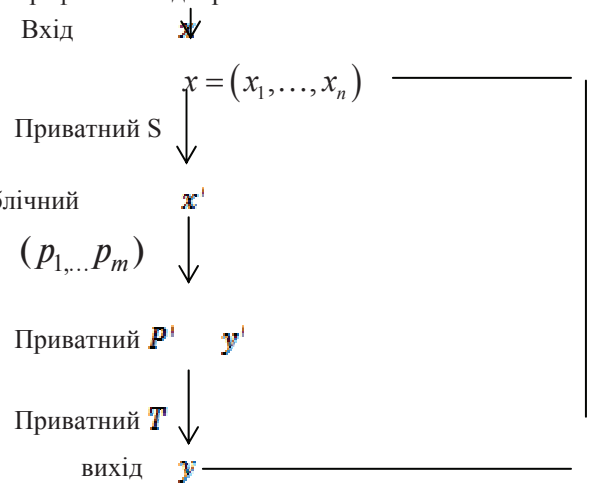
Таблиця 4

Складність атаки на *HFE*^{v}- перетворення

Значення b	$2^{(lgb)^2}$	Відкритий ключ
128	$2^{(lg128)^2}$	216974
256	$2^{(lg256)^2}$	556559
512	$2^{(lg512)^2}$	1618688

5. ОСОБЛИВОСТІ ПОЛОЖЕНЬ МУЛЬТИВАРІАТИВНИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Генерування ключів можна подати у вигляді такого графічного відображення



Далі використовуються многочлени над малими кінцевими полями F, наприклад, GF (2), GF (128) або GF (256), що орієнтовано, в тому числі, на 8-бітні мікропроцесори. За деяких умов можуть використовуватися розширення полів E розмірності *n* над полем F.

У результаті маємо:

- таємний ключ:

$$(S, P', T) \in AGL_n\left(F\right) \times MQ_m\left(F^n\right) \times AGL_m\left(F\right) \quad (19)$$

- *відкритий (публічний) ключ:*
-

$$P \in MQ_m\left(F^n\right), P = T\, o\, P' o\, S \quad (20)$$

- *рівняння для відкритого ключа:*

$$P_i\left(x_1, \ldots, x_n\right) = \sum_{1 \le j \le k \le n} \gamma_{ij,k} x_j x_k + + \sum_{j=1}^{n} \beta_{ij} x_j + a_i \text{ для } 1 \le i \le m \quad (21)$$

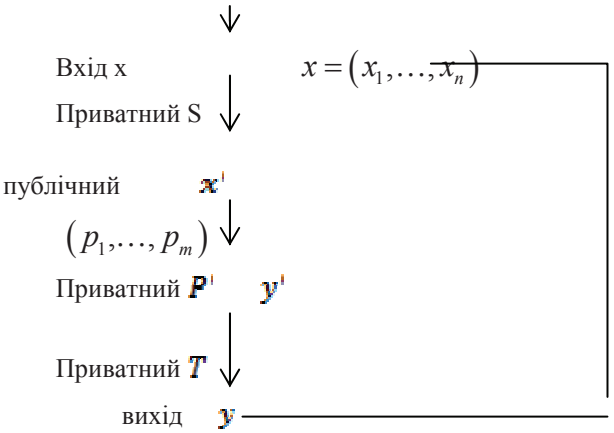
Причому коєфіцієнти $a_i, \beta_{ij}, \gamma_{ij,} k \in F\ a$

$$P(x) = \left(p_1(x_1,\ldots,x_n),\ldots,p_m(x_1,\ldots,x_n)\right)$$

У загальному випадку при прямому перетворенні (електронному підписі чи за шифруванні) робиться обчислення $y \in F^m$ для даного $x \in F^n$ шляхом оцінки $y = P(x).$

Перевірка підпису може здійснюватись таким чином.

Дана пара $(x, y) \in F^n \times F^m$. Перевірити рівняння $y = P(x)$.



Важливою властивістю є можливість інверсії для афінних перетворень. Нехай

$$S(x) = M_s x + v_s,$$

$M_s \in F^{n\times n}, v_s \in F^n$. Потрібно, щоб M_S було зворотним, після цього можна обчислити $S^{-1}(x') = M_S^{-1}(x' - v_s)$ Далі можна інвертувати $T(y') = y$ для даного y.

Генерування підпису. Необхідно для даного $y \in F^m$ зробити інверсію на кожному кроці та опублікувати відповідний x як підпис y.

Аналіз показує, що унікальна інверсія P' не може бути можливою, якщо є надмірність $\mathrm{H} = \mathrm{h}(\mathrm{x}),$ навіть якщо використовується з $\mathrm{h}(\bullet)$ криптографічно безпечною геш-функція.

Наведемо приклад та зробимо аналіз ключів. У криптосистемі мультиваріативного перетворення існують таємні та відкриті ключі. Таємний ключ складається з двох афінних перетворень, S і T, а також дозволяє легко інвертувати квадратичне відображення $P' : F^m \to F^n$. Позначимо через матрицю n афінних ендоморфізмів. $S : F^m \to F^n$ через M_S і вектор зсуву $v_s \in F^n$ і аналогічно для $T : F^m \to F^n$. В результаті отримуємо

$$S(x) = M_s x + v_s\, i$$

$$T(y) = M_T y' + v_T. \qquad (22)$$

В (22) параметри $\left(S^{-1},\ p^{t-1},\ T^{-1}\right)$ – це особисті ключі (ще їх називають люками). Публічний ключ є поєднанням $P = S \circ P' \circ T$ і його важко інвертувати, якщо люк є невідомим.

6. ПРИКЛАД МУЛЬТИВАРІАТИВНОГО КВАДРАТИЧНОГО ПЕРЕТВОРЕННЯ

Нехай x_1 і x_2 мають спільний PDF [15]

$$fx_1, x_2(x_1, x_2) = 2,\ 0 < x_1 < x_2 < 1,$$

і нуль в іншому випадку. Потрібно підрахувати спільний PDF випадкових величин

$$y_1 = \frac{x_1}{x_2},\ y_2 = x_2.$$

Розв'язок у загальному випадку.

1. Зважаючи на те, що
2. $x(2) = \{(x_1, x_2) : 0 < x_1 < x_2 < 1\}$ і

$$g_1(t_1, t_2) = \frac{t_1}{t_2}, g_2(t_1, t_2) = t_2;$$

3. Зворотні перетворення

$Y_1 = \dfrac{X_1}{x_2}, Y_2 = X_2 \leftrightarrow X_1 = Y_1 Y_2, X_2 = Y_2$ і тому

$g_1^{-1}(t_1, t_2) = t_1, t_2, g_2^{-1}(t_1, t_2) = t_2$

4. Діапазон: знайти Y(2). Розглянемо точку перетворення з $X^{(2)}$ в $Y^{(2)}$. Для пари точок $(x_1, x_2) \in X^{(2)}\ u\ (y_1, y_2) \in Y^{(2)}$, пов'язаних між собою перетворенням, маємо

$0 < x_1 < x_2 < 1 \leftrightarrow 0 < y_1 y_2 < y_2 < 1$ і, отже, можна отримати нерівності:

$$0 < y_2 < 1 \text{ і } 0 < y_1 < 1$$
$$Y^{(2)} = (0,1) \times (0,1)$$

5. Якобіан для точок $(y_1, y_2) \in Y^{(2)}$ знаходиться з

$$D_y = \begin{bmatrix} \frac{\partial x_1}{\partial y_1} & \frac{\partial x_1}{\partial y_2} \\ \frac{\partial x_2}{\partial y_1} & \frac{\partial x_2}{\partial y_2} \end{bmatrix} = \begin{bmatrix} y_2 & y_1 \\ 0 & 1 \end{bmatrix} \rightarrow$$

$$\rightarrow \left| J(y_1, y_2) \right| = \left| \det D_y \right| = \left| y_2 \right| = y_2$$

Запишемо це для $(x_1, x_2) \in X^{(2)}$

$$D_x = \begin{bmatrix} \frac{\partial y_1}{\partial x_1} & \frac{\partial y_1}{\partial x_2} \\ \frac{\partial y_2}{\partial x_1} & \frac{\partial y_2}{\partial x_2} \end{bmatrix} = \begin{bmatrix} \frac{1}{x_2} & \frac{x_1}{x_2^2} \\ 0 & 1 \end{bmatrix} \rightarrow$$

$$\rightarrow \left| J(x_1, x_2) \right| = \left| \det D_x \right| = \left| \frac{1}{x_2} \right| = \frac{1}{x_2}$$

Перевіримо, що $\left| J(y_1, y_2) \right| = \frac{1}{\left| J(x_1, x_2) \right|}$.

Нарешті, ми маємо

$$fY_1, Y_2(y_1, y_2) = 3y_2,$$

$0 < y_1 < 1, 0 < y_2 < 1$ і нуль в іншому випадку

7. АНАЛІЗ ВЛАСТИВОСТЕЙ МУЛЬТИВАРІАТИВНИХ КВАДРАТИЧНИХ ПЕРЕТВОРЕНЬ

Вважається, що мультиваріативні квадратичні перетворення з точки зору знаходження таємного ключа є експоненційно складними, що і є їх важливою перевагою. Приклад параметрів захищеності наведено в таблиці 5[4,11 – 13].

Таблиця 5

Параметри захищеності мультиваріативного перетворення

Розмір [біт]	Параметри	MQ-система [кілобайти]	Оцінка
259	$q = 128,\ m = n = 37$	23	< 1
569	$q = 128,\ m = n = 67$	134	< 1

Однією з основних вимог до ЕП є вимога, щоб процедури генерування та перевірки підпису були не складними – не вище за поліноміально складні. Тобто генерувати та перевіряти підпис потрібно швидко. Також достатньо великі відкриті ключі можна не змінювати часто, тому що це не є проблемою. Але треба звернути увагу на суттєве розширення ЕП, навіть, якщо пропускна здатність повідомлень є високою.

Наведені в таблиці 6 параметри були взяті з ЕП Quartz (– схема підпису в європейському проекті NESSIE). Потрібно звернути увагу на низьку швидкість розширення підпису. Проте, час генерації йде до 5 секунд (екстраполяція з кварцу).

Таблиця 6

Параметри ЕП Quartz

Геш [біти]	Параметри	Секретний ключ [кілобайти]	Публічний ключ [кілобайти]	Підпис	Перевірка	Розширення [біти]
160	q=128 n=67 r=11	7.8	112.3	<1	<1	237
Повідомлення [біти]	Параметри		Публічний ключ [кілобайти]	Підпис	Перевірка	Розширення
173	q=2 n=173 r=10		310.2	5,000	<5	10

Таблиця 7

Параметри для безпечної зміни ЕП Quartz.

Параметри	Секретний ключ [кілобайти]	Публічний ключ [кілобайти]	Підпис	Перевірка	Підпис
q=2 n=107 r=7	3	71	10,000	<1	128

У цілому наведені в таблицях 1 – 7 дані дозволяють зробити попередні висновки, що мультиваріативні криптоперетворення можуть розглядатися як кандидати на постквантові криптографічні перетворення типу ЕП.

8. ЗАГАЛЬНІ ВИМОГИ ДО ЕП

Однією із важливих проблемних задач, які потрібно вирішити на першому етапі розробки методів побудування постквантових алгоритмів ЕП, є обгрунтування загальних та спеціальних вимог до них. У цьому напрямі отримано ряд результатів. Серед них необхідно відмітити [4,11 – 14]. В таблицях 8 та 9 наведено вимоги, що висунуті NIST США [14] та ETSI “ЕС [12-13].

Таблиця 8

Вимоги з безпеки NIST США до постквантових ЕП

Модель безпеки для цифрового підпису	Модель безпеки EUF-CMA. Умови безпеки: доступ зловмисника менше, ніж до 2^{64} обраних повідомлень.
Вимоги до стійкості	1) 128 біт класичної безпеки / 64 біт квантової захищеності (запас стійкості AES-128) 2) 128 біт класичної безпеки / 80 біт квантової захищеності (запас стійкості SHA-256/ SHA3-256) 3) 192 біт класичної безпеки / 96 біт квантової захищеності (запас стійкості AES-192) 4) 192 біт класичної безпеки / 128 біт квантової захищеності (запас стійкості SHA-384/ SHA3-384) 5) 256 біт класичної безпеки / 128 біт квантової захищеності (запас стійкості AES-256)
Додаткові властивості безпеки	«perfect forward secrecy». (удосконалена випереджаюча безпека). Стійкість до атак сторонніми каналами. Стійкість до мультиключових атак. Стійкість до відмов.
Інші вимоги	Прозорі математичні розв’язання. Обгрунтованість стійкості

Таблиця 9

Вимоги з безпеки ETSI ЄС до постквантових ЕП

Вимоги безпеки: – Проходження громадського контролю та визнання науковим співтовариством. – Надійне підтвердження стійкості. – Актуальність моделі безпеки. – Висока складність можливих атак. – Можливість використання в безпечному протоколі розподілу ключів. – Можливість поєднання кількох функцій безпеки (наприклад, встановлення ключів і схеми автентифікації). – Зручність кількісної оцінки заявлених класичних і квантових рівнів безпеки. – Визначеність рекомендованих ключових розмірів для заданого рівня безпеки (наприклад, 80-біт, 112 біт, 128 біт або 256 біт).	
Класична безпека	Стійкість проти класичних атак.
Квантова безпека	Стійкість проти «квантових» атак. Зокрема, стійкість до алгоритму Гровера (подвоєння розміру ключа).

Продовження таблиці 9

Доказова безпека	Базування на задачах, які мають високу складність обчислення. Можливе ігнорування зниження рівня складності, за умови, що практична стійкість не зміниться.
Довгострокова безпека	Можливість використання у протоколів типу TLS 1.3 з підтримкою forward secure cipher suites.
Активна безпека	Стійкість проти атак з адаптивним підбором.
Ефективність	Використання рекомендованих параметрів розмірів для заданого рівня безпеки. Незалежність швидкодії та кількості раундів перетворень від платформи реалізації. Швидкість генерації ключів і часу, необхідного для поширення нового ключа. Інші практичні вимоги (наприклад, стійкість до відмов).

Крім наведених вимог з криптографічної стійкості висунуті також техніко-економічні та техніко-експлуатаційні вимоги [14]. Очевидно в найближчі 3 – 4 роки вони будуть покладені в основу під час розробки постквантових стандартів ЕП.

ВИСНОВКИ

1.У зв'язку з можливістю появи квантового комп'ютера актуальними є завдання створення постквантових алгоритмів ЕП. У цьому напрямі уже розпочаті дослідження, певною мірою визначено математичні основи, на яких можуть бути побудовані постквантові алгоритми ЕП.

2. Реалізація квантово-захищених алгоритмів вимагає великих матеріально-технічних ресурсів. Вказане пов'язане з великими довжинами ключів і загальних параметрів. Сучасний рівень розвитку техніки дозволяє оптимістично ставитися до можливості ефективної реалізації квантово-захищених алгоритмів.

3.Мультиваріативні квадратичні перетворення можуть бути застосованими у стандарті ЕП. Вони були використані для побудови схем підпису, але всі спроби побудувати надійну схему шифрування не увінчалися успіхом.

4. Попередній аналіз показав, що мультиваріативні квадратичні перетворення можуть вирішити проблему захищеності від атак на основі квантових комп'ютерів, але для цього ще потрібно провести величезний обсяг досліджень та робіт, а також вкласти значні ресурси.

5. Попередній аналіз показує, що розміри загальних параметрів та ключів не викликають сумнівів відносно криптографічної стійкості стандарту, розробленого на основі мультиваріативного квадратичного перетворення. Але залишається проблема просторової складності, яка пов'язана зі значними довжинами загальних параметрів та ключів.

Література

[1] A riddle wrapped in an enigma Neal koblitz and Alfred j.menezes.https://www.google.com.ua/search?q=a+riddle+wrapped+in+an+enigma+neal+koblitz+and+alfred+j.+menezes

[2] *Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody*, *Rene Peralta, Ray Perlner, Daniel Smith-Tone*. Report on Post – Quatum Cryptography. Nistir 8105 (draft). https://www.google.com.ua/search?

[3] Інтернет-ресурс. Режим доступу http://www.nkj.ru/archive/articles/5309/

[4] Інтернет-ресурс. Режим доступу http://www.win.tue.nl/diamant/symposium05/abstracts/wolf.pdf

[5] *Горбенко І.Д.* Аналіз проблем криптографічного захисту інформації у пост-квантовий період та можливі шляхи їх вирішення/ Горбенко І.Д. Кузнєцов О.О., Олійников Р.В., Потій О.В, Горбенко Ю.І., Ганзя Р.С., Пономар В.І. // Матеріали V-ої міжнародної науково-технічної конференції «Захист інформації і безпеки інформаційних систем». – Львів, 2016 (02-.06 – 03.06). – С. 52.

[6] *Reinier Broker*. Constructing supersingular elliptic curves. J. Comb. Number Theory, (3): pp. 269–273, 2009.

[7] *McGrew D., Curcio M*. Hash-Based Signatures draft-mcgrew-hash-sigs-00[Электронный ресурс] / D. McGrew, M. Curcio - Режим доступа: https://tools.ietf.org/html/draft-mcgrew-hash-sigs-00

[8] *Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal.* NTRU Prime, https://ntruprime.cr.yp.to/ntruprime-20160511.pdf.

[9] *D. J. Bernstein*. Grover vs. McEliece. In N. Sendrier, editor, Post-Quantum Cryptography, Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010. Proceedings, volume 6061 of Lecture Notes in Computer Science, pages 73–80. Springer, 2010.

[10] *Steven D. Galbraith*. Constructing isogenies between elliptic curves over Finite Fields. LMS J. Comput. Math, 2: pp. 118–138 (electronic), 1999.

[11] *Moody D.* Post-Quntum Cryptography: NIST's Plan for the Future. The Seventh International Conference on Post-Quntum Cryptography, Japan, 2016. Режим доступу: [https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf].

[12] ETSI GR QSC 001 V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework

[13] ETSI White Paper №8: Quntum safe cryptography and security. – 2015

[14] Proposed Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-for-proposals-draft-aug-2016.pdf

Гармаш Дмитро Васильович, студент факультету комп'ютерних наук, кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Наукові інтереси: електронний цифровий підпис, криптографічний захист інформації.

Бакликов Олександр Олександрович, інженер зі створення комплексних систем захисту інформації. Наукові інтереси: криптографічний захист інформації.

Філатова Наталія Вадимівна, студентка факультету комп'ютерних наук, кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Наукові інтереси: електронний цифровий підпис, криптографічний захист інформації.

Горбенко Іван Дмитрович, доктор технічних наук, професор, Харківський національний університет ім. В.Н.Каразіна, професор кафедри безпеки інформаційних систем і технологій.

УДК 003.26:004/056

Квантовые криптографические алгоритмы электронной подписи на основе мультивариативных квадратических переобразований / Д.В. Гармаш, О.О. Бакликов, Н.В. Филатова, И.Д. Горбенко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2016. – Том 15, № 3. – С. 215 – 225.

Приводятся требования к постквантовым алгоритмам асимметрических криптопреобразований. Указывается актуальность и необходимость поиска, исследования, стандартизации и применения криптографического примитива типа электронной подписи (ЭП). Рассматривается сущность и возможности применения мультивариативных квадратических преобразований при реализации ЭП, делается предварительный анализ их свойств и приводится практический пример.

Ключевые слова: требования к постквантовым электронным подписям, электронные подписи, квантовое криптопреобразование, математические основы мультивариативных преобразований, мультивариативное квадратическое преобразование для электронной подписи.

Табл.: 09. Библиогр.: 14 назв.

UDC 003.26:004/056

Quantum cryptographic algorithms of electronic signature based on multivariative quadratic transformations / D.V. Garmash, O.O. Baklykov, N.V. Filatova, I.D.Gorbenko // Applied Radio Electronics: Sci. Joum. – 2016. – Vol. 15, № 3. – P. 215 – 225.

The paper provides the requirements for postquantum algorithms of asymmetric cryptotransformations. The urgency and need to search for, research, standardize and use the crypotographic primitive of the type of electronic signatures (ES) are indicated. The essence and possibilities of applying multivariative quadratic transformations in implementing the ES are considered, a preliminary analysis of their properties is performed and a practical example is provided.

Keywords: requirements for postquantum electronic signatures, electronic signatures, quantum cryptotransformation, mathematical foundations of multivariative transformations, multivariative quadratic transformation for electronic signature.

Tab.: 09. Ref.: 14 items.