УДК 004.056.55 **DOI:10.30837/rt.2021.1.204.02**

М.В. ЄСІНА, канд. техн. наук, С.О. КАНДІЙ, Є.В. ОСТРЯНСЬКА,
І.Д. ГОРБЕНКО, д-р техн. наук

ГЕНЕРАЦІЯ ЗАГАЛЬНОСИСТЕМНИХ ПАРАМЕТРІВ ДЛЯ СХЕМИ ЕЛЕКТРОННОГО ПІДПИСУ RAINBOW ДЛЯ 384 ТА 512 БІТ БЕЗПЕКИ

Вступ

Наразі спостерігається стрімкий прогрес у створенні квантових комп'ютерів щодо вирішення різних обчислювально складних задач та для різних цілей. При цьому особливі зусилля докладаються до створення такого квантового комп'ютера, що зможе вирішувати задачі криптоаналізу існуючих криптосистем – асиметричних шифрів, протоколів інкапсуляції ключів, електронних підписів тощо. Попередження таких загроз може бути досягнуто засобом розробки таких криптографічних систем, що будуть захищені як від квантових, так і від класичних атак, а також зможуть взаємодіяти з протоколами і мережами зв'язку, що вже існують. Також є суттєва необхідність захисту від атак сторонніми каналами.

На даний момент значні зусилля криптологів зосереджені на відкритому конкурсі NIST PQC [1]. Основною ідеєю конкурсу є визначення математичних методів, на основі яких можуть бути розроблені стандарти на асиметричні криптоперетворення, в першу чергу електронного підпису (ЕП), а також асиметричні шифри та протоколи інкапсуляції ключів. За підсумками другого етапу фіналістами третього етапу конкурсу NIST PQC стали три схеми ЕП – Crystals-Dilithium, Falcon та Rainbow [1]. Наразі всесторонній аналіз фіналістів є важливою задачею для усієї світової криптоспільноти. Переважна більшість схем, що стали фіналістами, ґрунтується на проблемах з теорії алгебраїчних решіток [2 – 4]. Також особлива увага була приділена схемі ЕП Rainbow, що ґрунтується на основі багатовимірних перетворень [1].

Схема ЕП Rainbow значно відрізняється від інших кандидатів конкурсу NIST, оскільки заснована на багатовимірних перетвореннях. Вона є узагальненням структури UOV [5], що забезпечує ефективну параметризацію алгоритму ЕП за рахунок додаткової алгебраїчної структури. Теоретична безпека Rainbow ґрунтується на тому, що вирішення набору випадкових багатовимірних квадратичних систем є NP-складною проблемою [6]. Авторами методу Rainbow заявлено досягнення EUF-CMA моделі безпеки, що засновано на використанні геш-конструкції з випадковим чи псевдовипадковим ключем сеансу (сіллю). Також запропоновано дуже малі ЕП, буквально лише в кілька сотень бітів (лише 528 біт (66 байт) для I рівня безпеки NIST). У порівнянні з іншими кандидатами конкурсу NIST на постквантову схему ЕП вони є набагато коротшими. Крім того, оскільки Rainbow використовує лише прості операції над невеликими скінченими полями, то процеси вироблення та перевірки підпису є надзвичайно ефективними [6]. Крім того, спектр параметрів Rainbow дозволяє оптимізувати їх застосування у широкому діапазоні випадків. Схема ЕП Rainbow також вивчалась в інших контекстах та має певні переваги, у тому числі, наприклад, у малоресурсних додатках.

Показано, що для гарантованого забезпечення криптографічної стійкості ЕП Rainbow необхідно обґрунтувати вимоги та побудувати набори загальносистемних параметрів, за яких забезпечується стійкість до класичних і квантових атак. При визначенні вимог до системних параметрів схеми Rainbow NIST у рамках конкурсу зупинився на загальносистемних параметрах, що забезпечать 256 біт стійкості проти класичного та до 128 біт проти квантового криптоаналізу. Дані обмеження, на нашу думку, в тому числі пов'язані зі складністю обчислення загальносистемних параметрів, а також із суттєвим впливом їх збільшення на швидкодію електронного підпису. Проте, зважаючи на нинішнє застосування симетричних криптоперетворень на рівні стійкості у 512 біт, вважаємо, що уже наразі необхідно розглянути та реалізувати на основі схеми Rainbow ЕП зі стійкістю включно до 512 бітів. Але для цього необхідно обґрунтувати основні положення та вимоги до загальносистемних параметрів таких довжин, а також безпосередньо їх побудувати. При цьому повинна бути забезпечена

криптографічна стійкість від класичних та квантових атак відповідних значень, а також захист від атак сторонніми каналами.

Метою цієї статі є попередній аналіз існуючих атак щодо перспективного електронного підпису Rainbow, визначення вимог до загальносистемних параметрів для забезпечення криптографічної стійкості включно не менше 512 біт проти класичного та 256 біт проти квантового криптоаналізу, а також розроблення та практична реалізація щодо Rainbow алгоритмів генерації загальносистемних параметрів для 512 біт проти класичного та 256 біт проти квантового криптоаналізу.

1. Сутність механізму ЕП Rainbow

Розглянемо основні складові перетворень Rainbow – генерування загальносистемних параметрів та безпосередньо криптоперетворення. Схема ЕП Rainbow заснована на багатовимірних перетвореннях. Для багатовимірних схем з відкритим ключем відкритий ключ задається набором нелінійних багатовимірних поліномів над скінченим полем. Загалом, ключ багатовимірної криптосистеми з відкритим ключем – це система багатовимірних квадратичних поліномів з *n* змінними та *m* рівняннями [6, 7]:

$$\begin{aligned} p^{(1)}\left(x_1,\ldots,x_n\right) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(1)}\cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)}\cdot x_i + p_0^{(1)} \\ p^{(2)}\left(x_1,\ldots,x_n\right) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(2)}\cdot x_i x_j + \sum_{i=1}^{n} p_i^{(2)}\cdot x_i + p_0^{(2)} \\ &\vdots \\ p^{(m)}\left(x_1,\ldots,x_n\right) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(m)}\cdot x_i x_j + \sum_{i=1}^{n} p_i^{(m)}\cdot x_i + p_0^{(m)} \end{aligned} . \tag{1}$$

Усі коефіцієнти та змінні походять з F_q – скінченого поля з q елементами. По суті сукупність загальновідомих поліномів

$$\mathrm{P}\left(x_1,\ldots,x_n\right) = \left(p^{(1)}\left(x_1,\ldots,x_n\right),\ldots,p^{(m)}\left(x_1,\ldots,x_n\right)\right) \tag{2}$$

математично являє собою відображення F_q^n до F_q^m. Операції зашифрування повідомлення або верифікації підпису полягають у простому оцінюванні $\mathrm{P}\left(x_1,\ldots,x_n\right)$ з використанням відкритого ключа. Процес розшифрування зашифрованого тексту, а також вироблення ЕП зводиться до здійснення «інверсії» відображення $\mathrm{P}\left(x_1,\ldots,x_n\right)$ з використанням секретного (особистого) ключа. Ці складові еквівалентні вирішенню проблеми стійкості MQ-перетворення.

Схему ЕП Rainbow [7] з u рівнями можна описати наступним чином. Нехай F_q – скінчене поле з q елементами, а $\upsilon_1 < \upsilon_2 < \cdots < \upsilon_u < \upsilon_{u+1} = n$ – цілі числа. Обираємо $V_i = \{1,\ldots,\upsilon_i\}$, $o_i = \upsilon_{i+1} - \upsilon_i$ та $O_i = \{\upsilon_i,\ldots,\upsilon_{i+1}\}$, де $(i = 1,\ldots,u)$. Таким чином отримаємо $|V_i| = \upsilon_i$ і $|O_i| = o_i$, де $(i = 1,\ldots,u)$.

Центральне відображення F Rainbow складається з $m = n - \upsilon_1$ багатовимірних квадратичних поліномів $f^{(\upsilon_1+1)},\ldots,f^{(n)}$ виду

$$f^{(k)}(\mathbf{x}) = \sum_{i,j\in V_\ell} \alpha_{ij}^{(k)} x_i x_j + \sum_{i\in V_\ell,\, j\in O_\ell} \beta_{ij}^{(k)} x_i x_j + \sum_{i\in V_\ell\cup O_\ell} \gamma_i^{(k)} x_i + \eta^{(k)}, \tag{3}$$

де $\ell \in \{1,\ldots,u\}$ – єдине ціле число, таке, що $k \in O_\ell$.

Зауважимо, що в кожному поліномі $f^{(k)}$ при $k \in O_\ell$ немає квадратного члена $x_i x_j$, де i та j знаходяться в O_ℓ. Цей факт використаний авторами [7] для вироблення ЕП. Такі поліноми називали поліномами Oil-Vinegar, коли пропонувались схеми OV [5].

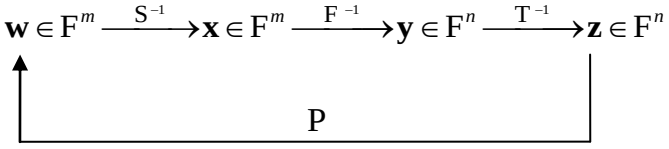
Щоб приховати структуру F у відкритому ключі, його складають з двома оберненими афінними або лінійними відображеннями $S : F^m \to F^m$ та $T : F^n \to F^n$. Отже, відкритий ключ Rainbow має вигляд $P = S \circ F \circ T : F^n \to F^m$, секретний ключ складається з трьох відображень S, F і T, а, отже, дозволяє інвертувати відображення відкритого ключа.

Щоб виконати ЕП для повідомлення $\mathbf{w} \in F^m$, необхідно виконати наступні три кроки.

1. Обчислити $\mathbf{x} = S^{-1}(\mathbf{w}) \in F^m$.
2. Обчислити попереднє відображення $\mathbf{y}$ з $\mathbf{x}$ під центральним відображенням F, використовуючи алгоритм інверсії, тобто $\mathbf{y} = F^{-1}(\mathbf{x}) \in F^n$.
3. Обчислити підпис $\mathbf{z} \in F^n$, $\mathbf{z} = T^{-1}(\mathbf{y})$.

Для підтвердження того, що $\mathbf{z} \in F^n$ є дійсним підписом для повідомлення $\mathbf{w} \in F^m$, необхідно обчислити $\mathbf{w}' = P(\mathbf{z})$. Якщо виконується рівність $\mathbf{w}' = \mathbf{w}$, підпис є дійсним. Процес генерації підпису та верифікації зображено на рис. 1.

Генерація підпису



Верифікація підпису

Рис. 1. Процес генерації та верифікації підпису Rainbow

2. Атаки на Rainbow

Нижче розглянуто низку атак на схему ЕП Rainbow, а саме пряму атаку, атаку MinRank та HighRank, атаку UOV та атаку «Rainbow Band Separation» (RBS) [1].

Хоча атаки прямої та грубої сили є атаками підробки підпису, які потрібно виконувати для кожного повідомлення окремо, атаки RBS та UOV є ключовими атаками відновлення. Після відновлення секретного ключа Rainbow за допомогою однієї з цих атак криптоаналітик може виробляти підписи так само, як законний користувач.

2.1. Прямі атаки

Найбільш прямолінійною атакою на багатовимірну схему Rainbow є пряма алгебраїчна атака, в якій загальновідоме рівняння $P(\mathbf{z}) = \mathbf{h}$ розглядається як проблема MQ. Оскільки Rainbow – це невизначена система з $n \approx 1.5 \cdot m$ рівнянь, найефективнішим способом вирішення цієї системи є фіксація *n–m* змінних для створення детермінованої системи. Можна очікувати, що отримана детермінована система має рівно одне рішення. У деяких випадках отримують ще кращі результати, коли відгадують додаткові змінні перед вирішенням системи (гібридний підхід) [8]. Складність вирішення такої системи з *m* квадратних рівнянь у *m* змінних можна оцінити за допомогою рівності (4):

$$\text{Complexity}_{\text{direct;classical}} = \min_k \left(q^k \cdot 3 \cdot \binom{m-k+d_{reg}}{d_{reg}}^2 \cdot \binom{m-k}{2} \right) \tag{4}$$

множень у полі, де d_{reg} – це так званий ступінь регулярності системи.

Ступінь регулярності системи можна оцінити як найменше ціле число d, для якого коефіцієнт t^d в

$$\frac{\left(1-t^2\right)^m}{\left(1-t\right)^{m-k}} \tag{5}$$

не є додатним.

За наявності квантових комп'ютерів додатковий крок вгадування гібридного підходу може бути прискорений алгоритмом Гровера. Застосовуючи такий підхід, можливо оцінити складність квантової прямої атаки наступним чином.

$$\text{Complexity}_{\text{direct;quantum}} = \min_k \left(q^{k/2} \cdot 3 \cdot \binom{m-k+d_{reg}}{d_{reg}}^2 \cdot \binom{m-k}{2} \right) \tag{6}$$

множень у полі.

2.2. MinRank атака

Під час атаки MinRank криптоаналітик намагається знайти лінійну комбінацію загальновідомих поліномів мінімального рангу. У випадку з Rainbow така лінійна комбінація рангу υ_2 відповідає лінійній комбінації центральних поліномів першого рівня. Таким чином, знаходячи o_1 цих лінійних комбінацій низького рангу, можна ідентифікувати центральні поліноми першого рівня та відновити еквівалентний секретний ключ Rainbow.

На сьогодні найбільш ефективний метод вирішення проблеми MinRank було запропонований у [9]. У цьому варіанті розглядається розкладання матриці низького рангу Q на $Q = S \cdot C$, де S – це $n \times r$, а C – це $r \times n$ матриці, що представляють простір рядків матриці Q. Визначається матриця $C'_j = \begin{pmatrix} r_j \\ C \end{pmatrix}$ і приймаються за нуль $r+1$ мінорів цих C_j матриць. Оскільки отримана система має набагато більше рівнянь, ніж змінних, ми можемо вирішити її шляхом лінеаризації за допомогою алгоритму Відемана.

Зокрема, кількість рівнянь у системі задається як $m \cdot \binom{n}{r+1}$, де $\binom{n}{r+1}$ – це кількість $r+1$ мінорів матриці C'_j. Кількість змінних у системі дорівнює $\left(o_2+1\right) \cdot \binom{n}{r}$. Отже, якщо нерівність

$$\left(o_2+1\right) \cdot \binom{n}{r+1} \geq \left(o_2+1\right) \cdot \binom{n}{r} - 1 \tag{7}$$

справедлива, то можливо розв’язати систему за допомогою алгоритму Відемана. Тому складність вирішення цієї системи задається як

$$\text{Complexity}_{\text{MinRank}} = 3 \cdot \left(\left(\left(o_2+1\right) \cdot \binom{n'}{r} \right)^2 \cdot \left(r+1\right) \cdot \left(o_2+1\right) \right). \tag{8}$$

Ретельний аналіз показав, що не потрібно розглядати всі *n* рядків матриці C'_j, щоб мати можливість вирішити систему. Число n' у (8) позначає найменше число, для якого виконується нерівність (7).

2.3. Атака HighRank

Метою атаки HighRank [10] є виявлення (у лінійному представленні) змінних, що з'являються найменшу кількість разів у центральних поліномах (вони відповідають Oil-змінним останнього рівня Rainbow, тобто змінним x_i з $i \in O_u$).

Складність цієї атаки можна оцінити як

$$\text{Complexity}_{\text{HighRank; classical}} = q^{o_u} \cdot \frac{n^3}{6}. \tag{9}$$

За наявності квантових комп'ютерів можна прискорити крок пошуку за допомогою алгоритму Гровера. Таким чином отримаємо

$$\text{Complexity}_{\text{HighRank; quantum}} = q^{o_u/2} \cdot \frac{n^3}{6} \tag{10}$$

множень у полі.

2.4. UOV атака

Оскільки Rainbow можна розглядати як продовження добре відомої схеми підпису Oil та Vinegar [5], її можна атакувати, використовуючи всі відомі атаки UOV [11].

Можна розглядати Rainbow як екземпляр UOV з $\upsilon = \upsilon_1 + o_1$ та $o = o_2$. Метою даної атаки є пошук попереднього відображення так званого Oil підпростору O афінного перетворення T, де $\mathrm{O} = \left\{ \mathbf{x} \in \mathrm{F}^n : x_1 = \cdots = x_\upsilon = 0 \right\}$. Знаходження цього простору дозволяє відокремити Oil від змінних Vinegar та відновити закритий ключ.

Складність цієї атаки можна оцінити як

$$\text{Complexity}_{\text{UOV-Attack; classical}} = q^{n-2o_2-1} \cdot o_2^4 \tag{11}$$

множень у полі. Використовуючи алгоритм Гровера, цю складність можна зменшити до

$$\text{Complexity}_{\text{UOV-Attack; quantum}} = q^{\frac{n-2o_2-1}{2}} \cdot o_2^4 \tag{12}$$

множень у полі.

2.5. Атака RBS

Атака RBS [12] спрямована на пошук лінійних відображень S і T, що перетворюють загальновідомі поліноми в поліноми форми Rainbow (тобто значення $\mathrm{Oil} \times \mathrm{Oil}$ повинні бути нульовими). Для цього криптоаналітик повинен вирішити кілька нелінійних багатовимірних систем. Складність цього кроку визначається складністю вирішення першої (і найбільшої) з цих систем, яка складається з $n + m - 1$ квадратних рівнянь з n змінними. Однак поліноми в цій системі не є випадковими квадратичними поліномами, але існують дві групи змінних X і Y, такі, що поліноми є білінійними в X і Y.

Зокрема, отримуємо два набори змінних X та Y розміром $|X| = n_x = \upsilon_1 + o_1$ та $|Y| = n_y = o_2$. Маємо $m_x = x$ поліномів, які є квадратичними у змінних X, а $m_y = n - 1$ рівняння білінійні у змінних X та Y. Отже, складність атаки RBS можна оцінити як

$$Compl_{RBS} = \min_{\alpha,\beta} 3 \cdot \mathrm{M}_{\alpha,\beta}(t,s)^2 \cdot (n_x + 1) \cdot (n_y + 1), \tag{13}$$

де $\mathrm{M}_{\alpha,\beta}$ позначає кількість одночленів (α, β).

3. Генерація параметрів для 384, 512 біт стійкості

У цьому підрозділі наведено вибір (генерацію) параметрів для 384 та 512 біт стійкості над полем GF(256). Під час вибору параметрів керувалися такими умовами:

– кількість рівнянь, що нам необхідна, залежить від складності прямої атаки та атаки на геш-функцію;
– кількість змінних залежить від складності атак RBS, UOV та HighRank.

Тож, якщо підсумувати сказане вище, то знайти параметри υ_1, o_1, o_2 при $q = 256$, тобто $GF(q) = GF(256)$, можливо з умов (4) – (13). На основі цього було розроблене програмне забезпечення, з використанням якого було згенеровано параметри υ_1, o_1 та o_2 для ЕП Rainbow для 384 та 512 біт безпеки, що наведені в табл. 1.

Таблиця 1

Основні загальносистемні параметри Rainbow
для 384, 512 біт безпеки

Безпека	υ_1	o_1	o_2	$GF(q)$
384	192	48	136	$GF(256)$
512	272	120	128	$GF(256)$

При таких параметрах отримуємо наступні розміри ключів, гешування та підписів для трьох версій Rainbow: класичної (Classic), циклічної (CZ-Rainbow), та стисненої (Compressed), що наведені в табл. 2 – 4 відповідно.

Таблиця 2

Розміри ключів та підписів Classic Rainbow

Безпека	Набір параметрів $(\mathrm{F}, \upsilon_1, o_1, o_2)$	Розмір відкритого ключа (байтів)	Розмір закритого ключа (байтів)	Розмір гешу (байтів)	Розмір підпису (байтів)
384	$(GF(256), 192, 48, 136)$	13041184	9752288	64	392
512	$(GF(256), 272, 120, 128)$	33594080	24752480	64	536

Таблиця 3

Розміри ключів та підписів CZ-Rainbow

Безпека	Набір параметрів $(\mathrm{F}, \upsilon_1, o_1, o_2)$	Розмір відкритого ключа (байтів)	Розмір закритого ключа (байтів)	Розмір гешу (байтів)	Розмір підпису (байтів)
384	$(GF(256), 192, 48, 136)$	3337344	9752288	64	392
512	$(GF(256), 272, 120, 128)$	8939840	24752480	64	536

Таблиця 4

Розміри ключів та підписів Compressed Rainbow

Безпека	Набір параметрів $(\mathrm{F}, \upsilon_1, o_1, o_2)$	Розмір відкритого ключа (байтів)	Розмір закритого ключа (байтів)	Розмір гешу (байтів)	Розмір підпису (байтів)
384	$(GF(256), 192, 48, 136)$	3337344	64	64	392
512	$(GF(256), 272, 120, 128)$	8939840	64	64	536

Швидкодія при заданих параметрах для трьох версій Rainbow, що представлена в тактах процесора, наведена в табл. 5 – 7 відповідно.

Таблиця 5

Швидкодія Classic Rainbow

Набір параметрів	Генерація ключів	Генерація підпису	Верифікація підпису
384	4658727146	16484356	2645458
512	16999329532	43986312	8165628

Таблиця 6

Швидкодія CZ-Rainbow

Набір параметрів	Генерація ключів	Генерація підпису	Верифікація підпису
384	4658375168	16799206	2927814
512	16900406374	52017328	10617618

Таблиця 7

Швидкодія Compressed Rainbow

Набір параметрів	Генерація ключів	Генерація підпису	Верифікація підпису
384	4631048528	16288184	2398794
512	16694833556	44923458	7611730

Висновки

1. Однією із важливих проблем сучасної криптографії є створення стандартів асиметричних криптографічних перетворень ЕП, які були б безпечними у постквантовий період. Вирішення цієї проблеми здійснюється в процесі міжнародного конкурсу NIST США, завданням якого є розробка такого механізму ЕП, який би був стійким як до квантових, так і до класичних атак.

2. Фіналістами конкурсу NIST США на схему ЕП стали: Crystals-Dilithium, Falcon та Rainbow. Переважна більшість схем, що стали фіналістами, ґрунтується на проблемах з теорії алгебраїчних решіток. Також особлива увага була приділена схемі електронного підпису Rainbow, що ґрунтується на основі багатовимірних перетворень.

3. Схема електронного підпису Rainbow значно відрізняється від інших кандидатів конкурсу NIST, оскільки заснована на багатовимірних перетвореннях. Вона є узагальненням структури UOV, що забезпечує ефективну параметризацію за рахунок додаткової алгебраїчної структури. Теоретична безпека Rainbow базується на тому, що вирішення набору випадкових багатовимірних квадратичних систем є NP-складною проблемою. Щодо проекту Rainbow заявлено EUF-CMA безпечність, вказане досягається на основі використання гешконструкції з випадковим ключем сеансу (сіллю).

4. Процес вироблення ЕП Rainbow складається з простих операцій лінійної алгебри, таких як множення матричних векторів та вирішення лінійних систем над малими скінченими полями. Також Rainbow забезпечує малі, у порівнянні з іншими підписи, по суті лише в кілька сотень бітів.

5. Основним недоліком ЕП Rainbow є великий розмір відкритих ключів. Тому його застосування рекомендується у системах, де можуть бути використаними відкриті ключі значних розмірів. Розміри загальносистемних параметрів та ключів для випадку забезпечення 384 та 512 біт безпеки наведені в табл. 2 – 4.

6. Також із табл. 5 – 7 видно, що процес верифікації ЕП CZ-Rainbow значно повільніший, ніж у стандартній схемі Rainbow. Однак необхідно зазначити, що це спричинене використанням криптографічно захищеного PRNG на базі AES, що постачається OpenSSL (що є таким самим, що і у NIST), для створення «фіксованих» частин відкритого ключа. Використовуючи швидший потоковий шифр або навіть генеруючи відкритий ключ, використовуючи регістр лінійного зворотного зсуву (LFSR), цього уповільнення можна уникнути майже повністю.

7. Було розглянуто низку атак на схему ЕП Rainbow, а саме – пряму атаку, атаку MinRank та HighRank, атаку UOV та атаку «Rainbow Band Separation» (RBS). Хоча пряма атака є атакою підробки підпису, яка повинна виконуватися для кожного повідомлення окремо, атаки MinRank, HighRank, UOV та RBS є ключовими атаками відновлення. Після відновлення секретного ключа Rainbow за допомогою однієї з цих атак криптоаналітик може виробляти підписи так само, як законний користувач.

Обґрунтовані та обчислені загальносистемні параметри можуть бути використані для забезпечення підвищених рівнів безпеки ЕП Rainbow включно до 384 та 512 біт безпеки відпо-

відно з параметрами, що в цій статті обґрунтовані, а саме: $(GF(256),192,48,136)$ та $(GF(256),272,120,128)$ відповідно.

Список літератури:

1. PQC Standardization Process: Third Round Candidate Announcement. July 22, 2020. [Electronic resource]. Access mode: https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement.

2. Craig Gentry, Chris Peikert, Vinod Vaikuntanathan Trapdoors for hard lattices and new cryptographic constructions // Richard E. Ladner and Cynthia Dwork, editors, 40th ACM STOC, pages 197–206. ACM Press, May 2008.

3. Damien Stehlé, Ron Steinfeld Making NTRU as secure as worst-case problems over ideal lattices // Kenneth G. Paterson, editor, EUROCRYPT 2011, volume 6632 of LNCS, pages 27–47, Tallinn, Estonia, May 15–19, 2011. Springer, Heidelberg, Germany.

4. Thomas Prest Gaussian Sampling in Lattice-Based Cryptography. Theses, École Normale Supérieure, December 2015.

5. A. Kipnis, J. Patarin, L. Goubin Unbalanced Oil and Vinegar schemes // EUROCRYPT 1999, LNCS vol. 1592, pp. 206-222. Springer, 1999.

6. Rainbow Signature / Ding J. and other.2020. P. 16-22. Access mode: https://www.pqcrainbow.org/.

7. J. Ding, D. Schmidt Rainbow, a new multivariable polynomial signature scheme // ACNS 2005, LNCS vol. 3531, pp. 164-175. Springer, 2005.

8. J. Bonneau, I. Mironov Cache-Collision Timing Attacks Against AES. CHES 2006, LNCS vol. 4249, pp. 201-215. Springer, 2006.

9. Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray A. Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, Javier A. Verbel Algebraic attacks for solving the Rank Decoding and MinRank problems without Groebner basis. CoRR abs/2002.08322 (2020).

10. D. Coppersmith, J. Stern, S. Vaudenay Attacks on the birational signature scheme. CRYPTO 1994, LNCS vol. 773, pp. 435-443. Springer, 1994.

11. A. Kipnis, A. Shamir Cryptanalysis of the Oil and Vinegar signature scheme. CRYPTO 1998, LNCS vol. 1462, pp. 257-266. Springer, 1998.

12. J. Ding, B.-Y. Yang, C.-H. O. Chen, M.-S. Che, C.-M. Cheng: New differential-algebraic attacks and reparametrization of Rainbow // ACNS 2008, LNCS vol. 5037, pp. 242-257. Springer, 2008.

13. J. Ding, Z. Zhang, J. Deaton, K. Schmidt, F. Visakha New attacks on lifted unbalanced oil vinegar. The 2nd NIST PQC Standardization Conference, 2019.

14. A. Kipnis, A. Shamir Cryptanalysis of the Oil and Vinegar signature scheme. CRYPTO 1998, LNCS vol. 1462, pp. 257-266. Springer, 1998.

15. A. Petzoldt, S. Bulygin, J. Buchmann Cyclic Rainbow – a Multivariate Signature Scheme with a Partially Cyclic Public Key. INDOCRYPT 2010, LNCS vol. 6498, pp. 33 – 48. Springer, 2010.

16. A. Petzoldt: Efficient Key Generation for the Rainbow Signature Scheme. PQCrypto 2020.

17. E. Thomae C. Wolf: Solving Underdetermined Systems of Multivariate Quadratic Equations Revisited. PKC 2012, LNCS vol. 7293, pp. 156-171. Springer, 2012.

18. W. Beullens, B. Preneel, A. Szepieniec, F. Vercauteren LUOV signature scheme proposal for NIST PQC project (Round 2 version), 2019.

Надійшла до редколегії 05.02.2021

Відомості про авторів:

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, старший викладач кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна; e-mail: rinayes20@gmail.com; ORCID: https://orcid.org/0000-0002-1252-7606

Кандій Сергій Олегович – АТ «Інститут інформаційних технологій», технік-конструктор, Україна; e-mail: sergeykandy@gmail.com

Острянська Єлизавета Вадимівна – АТ «Інститут інформаційних технологій», аналітик з систем захисту інформації, Україна; e-mail: antelizza@gmail.com

Горбенко Іван Дмитрович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, АТ «Інститут інформаційних технологій», головний конструктор; Україна; e-mail: GorbenkoI@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-4616-3449