УДК 003.026:004.056 **DOI:10.30837/rt.2021.2.205.08**

Г.А. МАЛЄЄВА

АНАЛІЗ ЗАХИЩЕНОСТІ ПОСТКВАНТОВОГО АЛГОРИТМУ ЕЛЕКТРОННОГО ПІДПИСУ RAINBOW ВІД ПОТЕНЦІЙНИХ АТАК

Вступ

Багатовимірна криптографія на основі відкритого ключа є кандидатом для постквантової криптографії, і це дозволяє генерувати особливо короткі підписи та швидку перевірку. Схема підписів Rainbow, запропонована Дж. Діном та Д. Шмідтом, є такою багатовимірною криптосистемою і вважається захищеною від усіх відомих атак. Ця схема підпису може бути реалізована просто та ефективно за допомогою лінійних методів алгебри над невеликим кінцевим полем і, зокрема, створює коротші підписи, ніж ті, що використовуються в RSA та інших постквантових підписах схеми [1]. У другому раунді NIST PQC пропонуються захищені набори параметрів Rainbow і проаналізовано кілька атак на них [1]. Зокрема, атака Rainbow-Band-Separation (RBS) [2] є найкращою серед відомих атак на Rainbow з певним набором параметрів і є важливою. Метою статті є спроба зрозуміти точну безпеку Rainbow від атаки RBS за допомогою F_4.

1. Порівняльний аналіз ЕП на основі MQ-перетворень за критерієм стійкість – складність

При порівняльному аналізі згідно [3] використані системи безумовних та умовних критеріїв оцінки та порівняльного аналізу електронних підписів (ЕП) на основі MQ-перетворень. Причому, якщо відповідні ЕП задовольняють безумовним критеріям, то в подальшому вони оцінюються та порівнюються за умовними критеріями. Таким чином, спочатку для алгоритмів ЕП обчислюються сукупності часткових безумовних критеріїв та інтегральні критерії для кожного з них. Потім для тих ЕП, що пройшли випробовування на першому етапі, обчислюються сукупності часткових умовних критеріїв та інтегральні умовні критерії для кожного з ЕП. Далі ранжування здійснюється з використанням безумовних та умовних інтегральних критеріїв. Перевага віддається алгоритмам ЕП, що пройшли відбір за безумовними критеріями, а також, що мають кращі показники щодо інтегральних умовних критеріїв. Таку методику запропоновано називати раціональною, тобто не оптимальною. Зрозуміло, що окремо ЕП на основі MQ-перетворень оцінюються щодо захищеності від атак сторонніми каналами. Після цього приймається рішення щодо переваг певного алгоритму ЕП на основі MQ-перетворення.

Для порівняння ЕП використані наступні характеристики та відповідні показники:

1) $I_{ст.}$ – рівень стійкості ЕП щодо класичних та квантових атак стійкості;
2) $l_{в.к.}$ – розмір відкритого ключа ЕП (байтів);
3) $l_{о.к.}$ – розмір особистого ключа ЕП (байтів);
4) $l_{рез.}$ – розмір підсумкового ЕП (байтів);
5) $T_{кл.}$ – швидкість (складність) створення ключової пари ЕП (тактів роботи);
6) $T_{пр.}$ – швидкість (складність) вироблення ЕП (тактів);
7) $T_{зв.}$ – швидкість (складність) перевірки ЕП (тактів).

Необхідно відмітити, що при необхідності число характеристик та відповідно показників може бути розширено.

Для визначення важливості тієї чи іншої характеристики (показника) використовуються експертні оцінки. При цьому, при порівнянні, певною перевагою та об’єктивністю є врахування та порівняння усієї множини кандидатів. В цьому якраз полягає сутність та особливість методу ранжування та застосування експертних оцінок.

У табл. 1 наведено експертні оцінки для вказаних характеристик, які були отримані від спеціалістів-криптологів.

Таблиця 1

Експертні оцінки характеристик криптографічних алгоритмів методом ранжування

Показники / Експерти	$I_{ст.}$	$l_{в.к.}$	$l_{о.к.}$	$l_{рез.}$	$T_{кл.}$	$T_{пр.}$	$T_{зв.}$
1	7	5	3	2	1	4	6
2	6	7	1	3	2	4	5
3	5	6	1	2	3	4	7
4	5	6	1	4	2	3	7
5	6	2	1	4	3	5	7
W	0,207	0,186	0,05	0,107	0,079	0,143	0,228

Із табл. 1 видно, що стійкість дійсно є важливою характеристикою для експертів, а реально це інтегральний безумовний критерій. Вона приймається за умови, що відповідні алгоритми ЕП пройшли відбір за інтегральним безумовним критерієм. Також враховано, що вона легко коригується за допомогою вибору параметрів. Крім того, видно, що складність (час) зворотного криптографічного перетворення, тобто час перевірки підпису, є більш важливою характеристикою.

Нижче наводяться результати аналізу та оцінки кожного із алгоритмів ЕП за допомогою методу ранжування та визначається алгоритм, що має найкращу модифікацію для кожного із алгоритмів, а також наводиться вибір більш перспективного алгоритму ЕП на основі MQ-перетворення. Відповідні дані наведені в табл. 2 і обрані найперспективніші кандидати.

Варто зазначити, що для характеристик 2) – 5) чим менше їх значення, тим краще, а для характеристик 1), 6) та 7) чим воно більше, тим краще, оскільки тим більш захищеним є алгоритм і більша швидкодія вироблення та перевірки ЕП.

Для аналізу було прийнято рішення провести порівняльний аналіз відповідно до кожного алгоритму, тобто обрати модифікації з найбільшою перевагою, і порівняти безпосередньо модифікації.

У табл. 2 представлено зведені характеристики щодо обраних модифікацій.

На рис. 1 зображено зведену гістограму відносної переваги алгоритмів ЕП на основі MQ-перетворень.

Таблиця 2

Зведені характеристики кращих модифікацій механізмів ЕП на базі MQ-перетворень другого етапу конкурсу NIST PQC

Характеристики / Модифікація	$I_{ст.}$	$l_{в.к.}$	$l_{о.к.}$	$l_{рез.}$	$T_{кл.}$	$T_{пр.}$	$T_{зв.}$
8-63-256	2	15,872	32	319	39,421,493	26,714,796	15,123,202
Ia	1	152,064	100,250	64	1,302,000,000	601,000	350,000
31-48	2	62	32	32,882	2,957,276	266,840,340	191,666,288
128	1	417,408	14,208	48	1,398,800,000	3,172,000,000	19,656,000

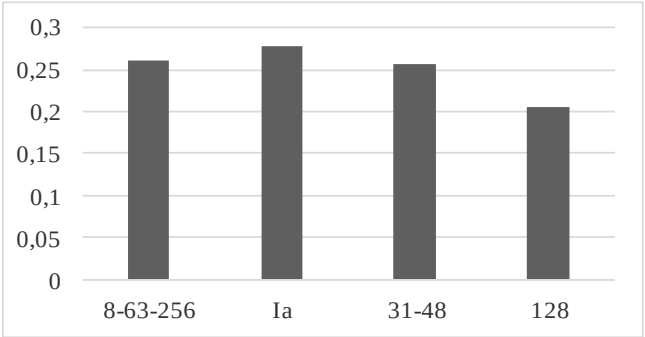

Рис. 1. Відносна перевага механізмів ЕП конкурсу NIST PQC за методом ранжування (серпень 2019, другий семінар)

Таким чином, беручи до уваги результати, які були поданими у [3], можна зробити висновок, що Rainbow та LUOV мають значну перевагу над іншими алгоритмами, як за умови надання мінімального рівня захисту, так і максимального. Ці два алгоритми ЕП в обмеженій групі лише MQ-перетворень можна розглядати щодо використання у постквантовий період як найбільш перспективні. Але необхідно відмітити, що як Rainbow, так і LUOV алгоритми можуть забезпечити обмежені рівні безпеки. Як правило обмеження пов'язані з забезпеченням максимум п'ятого рівня безпеки – мається на увазі 256 біт захищеності від класичних атак та 128 біт квантових атак.

2. Атака RAINBOW-BAND-SEPARATION (RBS)

Атака Rainbow-Band-Separation відновлює секретний ключ Rainbow, розв'язуючи певні системи квадратичних рівнянь, а його складність оцінюється за відомим показником, який називається ступенем регулярності. Однак, як правило, ступінь регулярності більша, ніж ступінь розв'язання в експериментах, і точної оцінки отримати неможливо. Попередні методи оцінки [1, 4] для складності атаки RBS використовують ступінь регулярності як її показник за припущенням, що система квадратичних рівнянь, розв'язана в атаці, є напіврегулярною. Для напіврегулярної системи ступінь регулярності задається як ступінь D_{reg} першого члена, коефіцієнт якого не позитивний у ряді потужностей

$$\frac{(1-t^2)^m}{(1-t)^n}, \qquad (1)$$

де m і n – числа рівнянь і змінних відповідно. Оскільки загальноприйнята квадратична система, що вирішується в прямій атаці, часто є напіврегулярною, то при оцінці складності прямої атаки використовується ступінь регулярності [1].

У роботі [5] запропоновано новий показник складності атаки Rainbow-Band-Separation за допомогою алгоритму F_4, який дає більш точну оцінку порівняно з показником, що використовує ступінь регулярності. Цей показник виводиться двома змінними рядами потужності

$$\frac{\prod_{i=1}^{m}(1-t_1^{d_{i1}}t_2^{d_{i2}})}{(1-t_1)^{n_1}(1-t_2)^{n_2}}, \qquad (2)$$

що збігається з однозмінним рядом потужностей при $t_1=t_2$, виводячи ступінь регулярності. Крім того, показано залежність між атакою Rainbow-Band-Separation за допомогою гібридного підходу та атакою HighRank. Розглядаючи це відношення та показник, ми отримали нову оцінку складності для атаки Rainbow-Band-Separation. Отже, завдяки цьому, можна зрозуміти точну безпеку Rainbow від атаки Rainbow-Band-Separation за допомогою алгоритму F_4.

3. Опис атаки RBS на схему підпису RAINBOW

Нехай m і n – натуральні числа. Позначимо через F кінцеве поле порядку q. Елемент $(f_1, ..., f_m)$ F $[x_1, ..., x_n]^m$ називається поліноміальною системою і дає відображення $F^n \to F^m$ на $a \to (f_1(a),...,f_m(a))$, яке називають поліноміальним відображенням (картою).

Багатовимірна схема підпису відкритого ключа складається з наступних трьох алгоритмів.

Генерація ключів: будуються дві обернені лінійні карти $S:F^n \to F^n$ і $T:F^m \to F^m$ випадковим чином і легко обернена квадратична карта $F: F^n \to F^m$, яку називають центральною картою, а потім обчислюється $P:=T \circ F \circ S$. Відкритий ключ подається у вигляді P. Кортеж (T, F, S) – секретний ключ.

Генерація підписів: для повідомлення $b \in F^m$ обчислюємо $b'=T^{-1}(b)$. Далі ми можемо обчислити елемент a' з $F^{-1}(\{b'\})$, оскільки F легко обернений. Отже, ми отримуємо підпис

$$a=S^{-1}(a') \in F^n.$$

Перевірка: перевіряється, чи $P(a)=b$ має місце. Для натуральних чисел v, o_1 і o_2, нехай $x=\{x_1, ..., x_v\}$, $y=\{y_1, ..., y_{o1}\}$ і $z=\{z_1, ..., z_{o2}\}$ будуть трьома змінними множинами і $n=v+o_1+o_2$, і $m=o_1+o_2$. Центральна карта $F=(f_1, ..., f_m)\in F[x, y, z]^m$ Rainbow

$$\begin{cases} f_1 = g^{(1)}(\mathbf{x}) + \sum_{i=1}^{o_1} l_i^{(1)}(\mathbf{x}) y_i, \\ \quad\vdots \\ f_{o_1} = g^{(o_1)}(\mathbf{x}) + \sum_{i=1}^{o_1} l_i^{(o_1)}(\mathbf{x}) y_i, \\ f_{o_1+1} = g^{(o_1+1)}(\mathbf{x},\mathbf{y}) + \sum_{i=1}^{o_2} l_i^{(o_1+1)}(\mathbf{x},\mathbf{y}) z_i, \\ \quad\vdots \\ f_{o_1+o_2} = g^{(o_1+o_2)}(\mathbf{x},\mathbf{y}) + \sum_{i=1}^{o_2} l_i^{(o_1+o_2)}(\mathbf{x},\mathbf{y}) z_i, \end{cases} \tag{3}$$

де $g^{(j)}$ та $l^{(j)}_i$ – випадковим чином обрані квадратичні многочлени та лінійні многочлени відповідно. Тоді за алгоритмом генерації підписів, наведеним вище, ми можемо легко обчислити елемент a' у попередньому зображенні будь-якого елемента $b'=(b'_1, ..., b'_{o1+o2})$ у F^m під F наступним чином.

1. Випадково обрати $a_v{}' = (a_1', ..., a_v')$ як x.
2. Вирішити систему лінійних рівнянь

$$f_1(\mathbf{a}'_v, \mathbf{y}) = b'_1, \ldots, f_{o_1}(\mathbf{a}'_v, \mathbf{y}) = b'_{o_1}.$$

Нехай $\mathbf{a}'_{o_1} = (a'_{v+1}, \ldots, a'_{v+o_1})$ є одним із її рішень, якщо воно існує. В іншому випадку повернутись до кроку 1.

3. Вирішити систему лінійних рівнянь

$$f_{o_1+1}(\mathbf{a}'_v, \mathbf{a}'_{o_1}, \mathbf{z}) = b'_{o_1+1}, \ldots, f_{o_1+o_2}(\mathbf{a}'_v, \mathbf{a}'_{o_1}, \mathbf{z}) = b'_{o_1+o_2}.$$

Нехай $\mathbf{a}'_{o_2} = (a'_{v+o_1+1}, \ldots, a'_{v+o_1+o_2})$ є одним із її рішень, якщо воно існує. В іншому випадку повернутись до кроку 1.

4. Отримати елемент $\mathbf{a}' = (a'_1, \ldots, a'_{v+o_1+o_2})$ у попередньому зображенні b'.

Нехай (v, o_1, o_2) – набір параметрів Rainbow, покладемо $n=v+o_1+o_2$ і $m=o_1+o_2$. Для відкритого ключа Rainbow $P=(p_1, ..., p_m)$ атака RBS відновлює свій секретний ключ (T, F, S) наступним чином. За визначенням (3) центральної карти $F=(f_1, ..., f_m)$ кожна матриця, відповідна f і має такий вигляд:

$$M_{f_i} = \begin{cases} \begin{pmatrix} *_{v\times v} & *_{v\times o_1} & 0_{v\times o_2} \\ *_{o_1\times v} & 0_{o_1\times o_1} & 0_{o_1\times o_2} \\ 0_{o_2\times v} & 0_{o_2\times o_1} & 0_{o_2\times o_2} \end{pmatrix} \text{ if } 1 \le i \le o_1, \\ \begin{pmatrix} *_{v\times v} & *_{v\times o_1} & *_{v\times o_2} \\ *_{o_1\times v} & *_{o_1\times o_1} & *_{o_1\times o_2} \\ *_{o_2\times v} & *_{o_2\times o_1} & 0_{o_2\times o_2} \end{pmatrix} \text{ if } o_1+1 \le i \le o_1+o_2. \end{cases} \tag{4}$$

Тут $*_{k\times l}$ означають k на l матриці над F. Аналогічно, матриці, відповідні S і T, можна записати наступним чином.

Матриці M_{p1}, ..., M_{pm}, що відповідають відкритим поліномам p_1, ..., p_m, задаються як

$$(M_{p_1}, \ldots, M_{p_m}) = (M_S M_{f_1}{}^t M_S, \ldots, M_S M_{f_m}{}^t M_S) M_T. \tag{5}$$

Існує вектор n на 1 $s=(\lambda_1, ..., \lambda_{v+o1}, 0, ..., 0,1)$ такий, що $s\cdot M_S=(0,...,0,1)$ Тоді для $i=1,...,m$, маємо

$$\mathbf{s} \cdot M_S M_{f_i}{}^t M_S \cdot {}^t\mathbf{s} = (0, \ldots, 0, 1) \cdot M_{f_i} \cdot {}^t(0, \ldots, 0, 1) = 0.$$

Оскільки кожен M_{pk} є лінійною комбінацією $M_S M_{f1}{}^t M_S{}^t;:::; M_S{}^t M_S M_{fm}{}^t$, отримуємо

$$\mathbf{s} \cdot M_{p_k} \cdot {}^t\mathbf{s} = 0, \quad k = 1, \ldots, m. \tag{6}$$

Існує вектор m на 1 $t=(1,0 ...,0, \lambda_{v+o1+1}, ..., \lambda_{v+o1+o2})$ такий, що $M_T \cdot {}^t t = {}^t(1,0, ..., 0)$. Потім,

помноживши рівняння (5) на ${}^t t$, отримаємо

$$M_{p_1} + \sum_{i=1}^{o_2} \lambda_{v+o_1+i} M_{p_{o_1+i}} = M_S M_{f_1} {}^t M_S. \quad (7)$$

де e_k це n на 1 вектор (0;...;0;1;0;...;0). Тут вилучаємо випадок $k=n$, оскільки рівняння (7) для $k=n$ випливає з рівняння (6).

Оскільки s = (λ_1, ..., λ_{v+o1}, 0, ..., 0,1), зрозуміло, що рівняння (6) і (7) є $n+m-1$ квадратичними рівняннями в n змінних $\lambda_1,...,\lambda_n$ і будуються з відкритого ключа $p_1,...,p_m$. Вирішивши ці квадратичні системи, зловмисник може відновити частину секретного ключа S і T, а сааме – s і t. Атака RBS може відновити S і T, повторюючи подібні обговорення, як описано вище (детальніше див. [2]).

Оскільки складність розв'язання квадратичної системи домінує в одній з атаки RBS, достатньо оновити лише систему. Квадратична система, що складається з рівнянь (6) та (7), називається домінуючою системою RBS.

З досліджень [5] можна зробити висновок, що домінуюча система RBS є нерегулярною та дворівневою.

4. Показник складності розв'язання дворівневої системи поліномів

Для дворівневої поліномічної системи $(h_1,...,h_m)$ у $F[x_1,...,xn_1,y_1,...,y_{n2}]^m$, де $deg\ Z^2_{\geq 0}\ h_i=(d_{i1}, d_{i2})$,

$$\sum_{(d_1,d_2)\in\mathbb{Z}^2_{\geq 0}} a_{(d_1,d_2)} t_1^{d_1} t_2^{d_2} = \frac{\prod_{i=1}^{m}(1-t_1^{d_{i,1}} t_2^{d_{i,2}})}{(1-t_1)^{n_1}(1-t_2)^{n_2}}, \quad (8)$$

і $D_{bgd}=D_{bqd}(h_1,...,h_m)$ визначається як мінімальне значення наступного набору, якщо воно існує, – $\{d_1+d_2 \mid a_{(d_1,d_2)} < 0\}$.

Двохзмінний ряд у (8) розглядається як двозначна версія гільбертового ряду.

Зауваження 1. Для дворівневої системи зазначимо, що однозмінний ряд потужності

$$\frac{\prod_{i=1}^{m}(1-t^{\deg f_i})}{(1-t)^n}. \quad (9)$$

що виводить D_{reg}, збігається з двома змінними рядами потужності (8), коли $t=t_1=t_2$. Отже, якщо ми визначимо D'_{bgd} як мінімальне значення набору $\{d_1+d_2 \mid a_{(d_1,d_2)} \leq 0\}$, де a (d_1, d_2) – коефіцієнт ${t^{d1}}_1 {t^{d2}}_2$ у ряді (8) і він існує, тоді $D'_{bgd} \leq D_{reg}$. D'_{bgd} часто менший, ніж ступінь вирішення для деяких наборів параметрів Rainbow. Таким чином, ми не використовуємо D'_{bgd} як відповідний показник. З іншого боку, термін t^{Dreg} у ряді (9) часто має від'ємний коефіцієнт, який виводить один із ${t^{d1}}_1 {t^{d2}}_2$ у ряді (8), де $d_1+d_2=D_{reg}$. А саме, відношення $D_{bgd} \leq D_{reg}$ часто дотримується (див. табл. 3 та 4).

Виходячи з цього, можна побачити, що введений показник D_{bgd} щільно наближає ступінь розв'язання домінуючої системи RBS, ніж ступінь регулярності. Показник D_{bgd} для домінуючої системи RBS з набором параметрів (v,o_1,o_2) задається мінімальною сумарною мірою показників, коефіцієнт яких від'ємний у двовимірній потужності

$$\frac{(1-t_1t_2)^{v+o_1+o_2-1}(1-t_1^2)^{o_1+o_2}}{(1-t_1)^{v+o_1}(1-t_2)^{o_2}}. \quad (10)$$

У табл. 3 порівнюється показник D_{bgd} та ступінь регулярності D_{reg} для домінантних систем RBS з $v=o_i$ та $v \lesssim 2o_i$.

Таблиця 3

D_{bgd} проти D_{reg} для домінуючої системи RBS

q=256	Експеримент			Теорія	
(v; o_i)	d_{slv}	d_{tim}	d_{mem}	D_{bgd}	*Невеликий залишок*
(4; 3)	4	4	4	4	4
(5; 3)	4	4	4	4	5
(6; 3)	4	4	4	4	5
(6; 4)	4	4	4	4	5
(7; 4)	4	4	4	4	6
(8; 4)	4	4	4	5	6
(8; 5)	5	5	5	5	6
(9; 5)	5	5	5	5	6
(10; 5)	5	5	5	5	7
(10; 6)	6	6	6	6	7
(11; 6)	6	6	6	6	7
(12; 6)	6	6	6	6	7
q=16	Експеримент			Теорія	
(v; o_i)	d_{slv}	d_{tim}	d_{mem}	D_{bgd}	*Невеликий залишок*
(3; 3)	3	3	3	3	4
(4; 4)	4	4	4	4	5
(5; 5)	4	4	4	4	5
(6; 6)	5	5	5	5	6
(7; 7)	5	5	5	5	6
(8; 8)	5	6	6	6	7
(9; 9)	6	6	6	6	7

Експериментальні ступені d_{slv}, d_{mem} і d_{tim} в алгоритмі F_4 та теоретичних ступенях D_{bgd} (із серії (10)) та D_{reg} (при k=0) для домінантної системи RBS з $v \lesssim 2o_i$ або $v=o_i$ (i=1,2). Запропонований показник D_{bgd} збігається з d_{slv} у випадках, за винятком (q, v, o_i) = (256,8,4), (16,8,8). Ступінь регулярності D_{reg} завжди більша, ніж d_{slv}, за винятком (q, v, o_i) = (256,4,4).

Експериментальні ступені d_{slv}, d_{mem} і d_{tim} в алгоритмі F_4 та теоретичних ступенях D_{bgd} та D_{reg} гібридного підходу щодо домінуючих систем RBS у змінних $\{\lambda_1, ..., \lambda_{v+o1+o2}\}$ для (q,v,o_1,o_2)=(256,10,5,5) і (16,8,8,8). Цілі числа k_1 і k_2 – це кількість змінних, зафіксованих гібридним підходом у $\{\lambda_1, ..., \lambda_{v+o1}\}$ і $\{\lambda_{v+o1+1}, ..., \lambda_{v+o1+o2}\}$ відповідно. Ступінь регулярності D_{reg} завжди більша, ніж ступінь вирішення d_{slv}. Пропонований показник D_{bgd} щільно наближає d_{slv}, ніж D_{reg}, і є верхньою межею d_{slv}.

Крім того, у табл. 4 порівнюється показник D_{bgd} та ступінь регулярності D_{reg} для гібридного підходу при атаці RBS проти наборів параметрів Rainbow (q,v,o_1,o_2)=(256,10,5,5) та (16,8,8,8). Тут k_1 і k_2 – це кількість змінних, зафіксованих гібридним підходом у $\{\lambda_1, ..., \lambda_{v+o1}\}$ і $\{\lambda_{v+o1+1}, ..., \lambda_{v+o1+o2}\}$, де $\lambda_1, ..., \lambda_{v+o1+o2}$ – змінні домінуючої системи RBS (див. вирази (6) та (7)). Тоді показник D_{bgd} задається мінімальною сумарною мірою показників, коефіцієнт яких від'ємний у двох змінних рядах потужності

$$\frac{(1-t_1t_2)^{v+o_1+o_2-1}(1-t_1^2)^{o_1+o_2}}{(1-t_1)^{v+o_1-k_1}(1-t_2)^{o_2-k_2}}. \qquad (11)$$

Таблиця 4

D_{bgd} проти D_{reg} для гібридного підходу в домінантній системі RBS

(256; 10; 5; 5)		Експеримент			Теорія	
k_1+k_2	$(k_1; k_2)$	d_{slv}	d_{tim}	d_{mem}	D_{bgd}	*Невеликий залишок*
0	(0; 0)	5	5	5	5	7
1	(1; 0)	5	5	5	5	6
	(0; 1)	4	4	4	5	6
2	(2; 0)	4	5	5	5	6
	(1; 1)	4	4	4	4	6
	(0; 2)	4	4	4	4	6
3	(3; 0)	4	4	4	4	6
	(2; 1)	4	4	4	4	6
	(1; 2)	3	4	4	4	6
	(0; 3)	3	3	3	3	6
4	(4; 0)	4	4	4	4	5
	(3; 1)	3	4	4	4	5
	(2; 2)	3	3	3	3	5
	(1; 3)	3	3	3	3	5
	(0; 4)	2	2	2	2	5
(16; 8; 8; 8)		Експеримент			Теорія	
k_1+k_2	$(k_1; k_2)$	d_{slv}	d_{tim}	d_{mem}	D_{bgd}	*Невеликий залишок*
0	(0; 0)	5	6	6	6	7
1	(1; 0)	5	5	5	5	6
	(0; 1)	5	5	5	5	6
2	(2; 0)	5	5	5	5	6
	(1; 1)	5	5	5	5	6
	(0; 2)	5	5	5	5	6
3	(3; 0)	4	5	5	5	6
	(2; 1)	4	5	5	5	6
	(1; 2)	4	5	5	5	6
	(0; 3)	4	4	4	5	6
4	(4; 0)	4	4	4	4	6
	(3; 1)	4	4	4	5	6
	(2; 2)	4	4	4	4	6
	(1; 3)	4	4	4	4	6
	(0; 4)	4	4	4	4	6

Зауваження 2. Як правило, перший доданок, що має від'ємний коефіцієнт у ряді потужностей (9), дає комплекс Кошу, якщо вона існує. Отже, очікується, що D_{bgd} надає комплекс

Кошу, а саме алгоритми на основі підпису, які повертають генератори модуля сизигії, повинні обчислювати до ступеня D_{bgd}.

Атака RBS за допомогою гібридного підходу при $k_2=o_2$ стає схожою на атаку HighRank [6]. Оскільки центральна карта Rainbow має матриці низького рангу M_{f1}, ..., M_{fo1} (див. вираз (4)), можна отримати квадратичний многочлен нижчого рангу, знайшовши лінійну комбінацію $M_{p1},...,M$. Для матриць o_2+1 з $M_{p1},...,M_{pm}$ атака HighRank відновлює такий квадратичний многочлен, знаходячи лінійну комбінацію, підпростір ядра якого має розмір одиниці. З іншого боку, атака RBS з використанням гібридного підходу при $k_2=o_2$ фіксує o_2 значення λ_{v+o1+1}, ..., $\lambda_{v+o1+o2}$ для отримання лінійної комбінації

$$M_{p_1} + \sum_{j=1}^{o_2} \lambda_{v+o_1+j} M_{p_{a_1+j}}$$

матриць o_2 +1 $M_{p1},M_{po1+1},...,M_{po1+o\,2}$ і розв'язує систему лінійних рівнянь (7) в $v+o_1-k_1$ змінних. Отже, атака має квадратичний поліном нижчого рангу і схожа на атаку HighRank.

Висновки

1. При порівнянні ЕП перевага віддається алгоритмам ЕП, що пройшли відбір за безумовними критеріями, а також, що мають кращі показники щодо інтегральних умовних критеріїв, оскільки така методика є більш раціональною.

3. При порівнянні рекомендується використовувати наступні характеристики та відповідні показники: $I_{ст.}$ – рівень стійкості ЕП щодо класичних та квантових атак стійкості; $l_{в.к.}$ – розмір відкритого ключа ЕП (байтів); $l_{о.к.}$ – розмір особистого ключа ЕП (байтів); $l_{рез.}$ – розмір підсумкового ЕП (байтів); $T_{кл.}$ – швидкість (складність) створення ключової пари ЕП (тактів роботи); $T_{пр.}$ – швидкість (складність) вироблення ЕП (тактів); $T_{зв.}$ – швидкість (складність) перевірки ЕП (тактів). Ранжування за цими показниками необхідне для визначення переваг певного алгоритму ЕП на основі MQ-перетворень.

4. Для наведених характеристик 2) – 5) у табл. 1, чим менше їх значення, тим краще, а для характеристик 1), 6) та 7), чим воно більше, тим краще, оскільки тим більш захищеним є алгоритм і більша швидкодія вироблення та перевірки ЕП.

5. Алгоритми ЕП Rainbow та LUOV в класі MQ-перетворень мають значну перевагу над іншими алгоритмами, як за умови надання мінімального рівня захисту, так і максимального. Ці два алгоритми ЕП в обмеженій групі лише MQ-перетворень можна розглядати щодо використання у постквантовий період як найбільш перспективні.

6. Необхідно відмітити, що як Rainbow, так і LUOV алгоритми можуть забезпечити обмежені рівні безпеки. Як правило, обмеження пов’язані з забезпеченням максимум п’ятого рівня безпеки. Мається на увазі 256 біт захищеності від класичних атак та 128 біт квантових атак.

7. Оскільки атака Rainbow-Band-Separation (RBS) відновлює секретний ключ Rainbow, розв’язуючи певну дворівневу багаточленну систему, можна використовувати D_{bgd} для оцінки складності цієї атаки.

8. Згідно з експериментами [5], що використовують F_4 для зменшених наборів параметрів Rainbow у другому раунді NIST PQC, показник D_{bgd} більше наближає ступінь розв'язання, ніж ступінь регулярності D_{reg}, який використовувався раніше. Тоді відношення $D_{bgd} \leq D_{reg}$ дотримується завжди.

9. Крім того, атака RBS може звести отриману поліномну систему до лінійної системи, використовуючи гібридний підхід із спеціальними налаштуваннями. Тоді ця атака стає схожою на атаку HighRank.

Список літератури:

1. Ding J., Chen M.-S., Petzoldt A., Schmidt D., Yang B. Y. Rainbow – Algorithm Specification and Documentation. Specification document of NIST PQC 2nd round submission package (2019)

2. Ding J., Yang B.-Y., Chen C.-H. O., Chen M.-S. and Cheng C.-M. New differential-algebraic attacks and reparametrization of Rainbow // Bellovin, S.M., Gennaro, R., Keromytis, A.D., Yung, M. (eds.) ACNS 2008, LNCS, vol. 5037, pp. 242–257. Springer (2008).

3. Кудряшов І. С., Малєєва Г. А. Аналіз властивостей електронних підписів на базі MQ перетворень / Ін-т кібернетики імені В. М. Глушакова НАН України ; Кам'янець-Подільський нац. ун-т імені Івана Огієнка // Математичне та комп'ютерне моделювання / Кам'янець-Подільський нац. ун-т імені Івана Огієнка. Кам'янець-Подільський, 2019. (Технічні науки: зб. наук праць; 19). С. 69-74.

4. Thomae E. A Generalization of the Rainbow Band Separation Attack and its Applications to Multivariate Schemes // IACR Cryptology ePrint Archive (2012). https://eprint.iacr.org/2012/223.

5. Nakamura S., Ikematsu Y., Wang Y., Ding J., Takagi T. New Complexity Estimation on the Rainbow-Band-Separation Attack. Specification document of NIST PQC.

6. Coppersmith D., Stern J., Vaudenay S. Attacks on the birational signature scheme // Stinson D.R. (ed.) CRYPTO 1994, LNCS vol. 773, pp. 435–443. Springer (1994).

Надійшла до редколегії 05.03.2021

Відомості про автора:

Малєєва Ганна Андріївна – Харківський національний університет радіоелектроніки, аспірант кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління; Україна; e-mail: hanna.malieieva@nure.ua