УДК 003.026:004.056 **DOI:10.30837/rt.2022.2.209.06**

Г.А. МАЛЄЄВА

АНАЛІЗ АТАКИ ЧАСТКОВОГО ВІДНОВЛЕННЯ КЛЮЧА НА МУЛЬТИВАРІАТИВНІ КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ З ВИКОРИСТАННЯМ РАНГОВИХ СИСТЕМ

Вступ

Схема підпису Rainbow [1], запропонована Дінгом і Шмідтом у 2005 році, є однією з найстаріших і найбільш вивчених схем підпису в багатовимірній криптографії. Rainbow заснована на схемі підпису (unbalanced) Oil and Vinegar [2, 3], яка за правильно обраних параметрів мала необхідну криптостійкість починаючи з 1999 року. В останнє десятиліття збільшився інтерес до багатоваріантної криптографії, оскільки вважається, що вона є квантово стійкою.

Криптоаналіз Rainbow та його попередників активно розвивався на початку 2000-х років. Атаки з цієї епохи включають атаку MinRank, атаку HighRank, атаку Білле – Гілберта, атака погодження UOV та атака розподілу смуги Rainbow [4 – 8]. Після 2008 року криптоаналіз, здавалося, припинився, аж до участі Rainbow у проєкті NIST PQC, що послугувало мотиватором до продовження криптоаналізу. Під час другого раунд NIST, Бардет та інші запропонував новий алгоритм для розв'язування задачі MinRank [9]. Це різко підвищило ефективність атаки MinRank хоча й недостатньо, щоб загрожувати параметрам, поданим до NIST. Менш витратну з точки зору пам’яті версію цього алгоритму запропонувала Баена та ін. [10]. Перлнер і Сміт-Тон глибше проаналізували атаку розподілення смуги Rainbow, що показала, що атака була ефективнішою, ніж до цього вважалося[11]. Це спонукало команду Rainbow дещо збільшити параметри для третього туру. Під час третього раунду Белленс представив нову атаку [12], які знизили рівень безпеки Rainbow у 2^{20} разів для параметрів SL 1. Команда Rainbow стверджувала, що, незважаючи на нові атаки, параметри Rainbow все ще відповідають вимогам NIST [13].

У статті представлені дві нові атаки (часткового) відновлення ключа.

Розв’язування багатовимірних систем

Наші атаки використовують (у режимі чорної скриньки) процедуру, що задана однорідним багатовимірним квадратичним відображенням $\mathcal{P}: F_q^n \to F_q^m$, і знаходить ненульовий розв’язок *x* такий, що $\mathcal{P}(x) = 0$, якщо такий розв’язок існує. Ми розробили цю процедуру за допомогою блокового алгоритму Відемана XL [14 – 17]. Цей алгоритм будує велику, але дуже розріджену систему лінійних рівнянь і вирішує його за допомогою блокового алгоритму Відемана, використовуючи перевагами розрідженості системи.

Для експериментальної перевірки наших атак ми використали оптимізовану реалізацію блокового алгоритму Відеман XL авторів Cheng, Chou, Niederhagen та Yang [17]. Складність цього алгоритму на екземплярі з m випадкових однорідних рівнянь в n змінних можна оцінити як складність

$$3\binom{n-1+D}{D}^2\binom{n+1}{2}$$

множення поля, де D – *робочий ступінь* XL, який обирається найменшим цілим числом, коефіцієнт члена t^D у розкладанні степеневого ряду

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

є недодатним.

Приклад 1. Припустимо, що необхідно знайти розв'язок системи з 63 однорідних квадратних рівнянь з 31 змінною. Маємо

$$\frac{(1-t^2)^{63}}{(1-t)^{31}} = 1 + 31t + 433t^2 + 3503t^3 + 17081t^4 + 41447t^5 - 44919t^6 + O(t^7),$$

тож ми можемо запустити XL на ступені D = 6 з орієнтовною складністю

$$3\binom{31-1+6}{6}^2\binom{31+1}{2} \approx 2^{52.3}$$

множень поля.

Проста атака

Нехай $(pk = \mathcal{P}, sk = (O_1, O_2, W))$ – пара ключів Rainbow. Для будь-якого вектора $x \in F_q^n$, і будь-якого вектора $o_2 \in O_2$, за побудовою маємо, що $\mathcal{P}'(x, 2) \in W$. Отже, для будь-якого x ми розглянемо диференціал

$$D_x : F_q^n \to F_q^m : y \to \mathcal{P}'(x, y),$$

яка є лінійним відображенням з F_q^n до F_q^m, що, крім того, надсилає O_2 до W. Для будь-якого фіксованого відмінного від нуля x диференціал $D_x|O_2$, обмежений O_2, є рівномірно випадковим лінійним відображенням O_2 до W (по випадкових бітах алгоритму генерації ключа). Зазначимо що $dim(O_2) = dim(W) = o_2$, тому ймовірність того, що D_x має вектор ядра у O_2 – це саме ймовірність того, що випадкова матриця o_2 на o_2 над F_q є сингулярною. Матриця є не сингулярною, якщо перший рядок відмінний від нуля, і для кожного $i < o_2$, $i + 1 -$ й рядок не знаходиться в проміжку перших i рядків (що трапляється з імовірністю q^{i-1-o_2}), тому ймовірність бути сингулярною для матриці становить

$$1 - \prod_{i=0}^{o_2}\left(1 - q^{i-o_2}\right),$$

що близько до 1/q для достатньо великого q, незалежно від o_2. Наприклад, з q = 16, o_2 = 32, ймовірність приблизно 1/15,06.

Цільова атака тепер полягає в тому, щоб просто обрати випадковий (не нульовий) x, і сподіватися, що ядро D_x перетинає O_2 нетривіально, а потім спробувати знайти вектор o в цій інтерсекції. Оскільки $\mathcal{P}(o) = 0$ для всіх $o \in O_2$, запропоновано зробити це, розв'язавши наступну систему

$$\begin{cases} D_x o = 0 \\ \mathcal{P}(o) = 0 \end{cases}$$

Це система з m однорідних лінійних рівнянь і m однорідних квадратних рівнянь у n змінних o. Якщо ми використовуємо m лінійних рівнянь для усунення m змінних з квадратних рівнянь, ми отримуємо систему m однорідних рівнянь у $n - m$ змінних. Конкретно, нехай $B \in F_q^{n\times(n-m)}$ це матриця, стовпці якої утворюють основу для $ker(D_x)$, то ми шукаємо рішення $x \in F_q^{n-m}$ до $\tilde{\mathcal{P}}(x) = 0$, де $\tilde{\mathcal{P}}(x) := \mathcal{P}(Bx)$.

Атака в полях непарної характеристики. Коли q непарне, $\tilde{\mathcal{P}}$ поводиться як випадкова система з m однорідних квадратне рівняння в $n - m$ змінних в алгоритмі XL. Ранги XL системи точно відповідають рангам XL систем випадкових квадратичних рівнянь на кожному ступені операції D. Зокрема, якщо розв'язок $\mathcal{P}(x) = 0$ існує, ми можемо знайти його з орієнтовною вартістю

$$3\binom{n-m-1+D}{D}^2\binom{n-m+1}{2}$$

множення поля, де D – найменше натуральне число, таке, що t^D коефіцієнт розкладання по степеневому ряду $\frac{(1-t^2)^m}{(1-t)^{m-n}}$.

Атака в полях парної характеристики. Для парних q ранг систем XL не збігається з рангом випадкових систем, і застосування XL як у випадку непарної характеристики іноді не вдається. Причина полягає в тому, що $\mathcal{P}'(x,x) = 2\mathcal{P}(x)$ звертається до нуля в характеристиці 2, тому $x \in ker(D_x)$. Це означає існує $\tilde{x} \in F_q^{n-m}$(відомий зловмиснику) такий, що $\tilde{\mathcal{P}}(\tilde{x} + y) = \tilde{\mathcal{P}}(\tilde{x}) + \mathcal{P}(y)$ для всіх $y \in F_q^{n-m}$, що зазвичай не відбувається для випадкового $\tilde{\mathcal{P}}$. Добре, що це не становить проблеми для атаки, ми навіть можемо використовувати цю властивість, щоб зробити атаку трохи ефективнішою: необхідно знайти x такий, що $\tilde{\mathcal{P}}(x) = 0$. Нехай $Y \subset F_q^{n-m}$ будь-який підпростір розмірності $n - m - 1$, що не містить $\tilde{x}$, такий, що $\langle \tilde{x} \rangle + Y = F_q^{n-m}$. Тоді достатньо знайти $y \in Y$ таке, що $\tilde{\mathcal{P}}(y) = \alpha\tilde{\mathcal{P}}(\tilde{x})$ для деякого $\alpha \in F_q$, оскільки тоді $x = \tilde{x} + \alpha^{-1/2}y$ є рішення $\tilde{\mathcal{P}}(x) = 0$, (нагадаємо, що кожен елемент має квадратний корінь у полях характеристика 2, то $\alpha^{-1/2}$ існує), тому що

$$\tilde{\mathcal{P}}(\tilde{x} + \alpha^{-1/2}y) = \tilde{\mathcal{P}}(\tilde{x}) + \alpha^{-1}\tilde{\mathcal{P}}(y) = 0 .$$

Щоб знайти це $y \in Y$, ми обмежуємо $\tilde{\mathcal{P}}$ до Y і шукаємо рішення для $m - 1$ однорідних квадратних рівнянь

$$\hat{\mathcal{P}} := \{\tilde{p}_1 a_i - \tilde{p}_i a_1\}_{i=2}^{m} ,$$

де $a = \tilde{\mathcal{P}}(\tilde{x})$, і з втратою загальності припустимо, що $a_1 \neq 0$.

Обмеживши Y, ми видалимо проблемний вектор $\tilde{x}$, тому не дивно, що наші рангові експерименти показують, що нова система $\hat{\mathcal{P}}$ веде себе як система $m - 1$ випадкових однорідних квадратних рівнянь з $n - m - 1$ змінною. Тому, якщо рішення існує, можемо знайти його з орієнтовною вартістю

$$3\binom{n-m-2+D}{D}^2\binom{n-m}{2}$$

множення поля, де D – найменше натуральне число, таке, що t^D коефіцієнт розкладання по степеневому ряду $\frac{(1-t^2)^{m-1}}{(1-t)^{m-n-1}}$.

Виконання атаки. Як тільки вектор O_2 буде знайдено, другий шар Rainbow можна видалити, а безпека Rainbow зводиться до безпеки меншої системи UOV $m' = m - o_2$ рівнянь в $n' = n - o_2$ змінних (див. розділ 5.3 [12]). Для єдиного вектора o $\in O_2$ можна спочатку обчислити

$$\langle \mathcal{P}'(o, e_1), \ldots, \mathcal{P}'(o, e_n) \rangle \subset W ,$$

що з великою ймовірністю буде рівнянням. Нехай V — це зміна змінних, яка надсилає W до останніх o_2 координат F_q^m , і розбиває $V \circ \mathcal{P}$ як

$$V \circ \mathcal{P}(x) = \begin{cases} \mathcal{P}_1(x) \\ \mathcal{P}_2(x) \end{cases}$$

де $\mathcal{P}_1 : F_q^n \to F_q^{m-o_2}$ складається з перших $m - o_2$ координат $V \circ \mathcal{P}$ і $\mathcal{P}_2 : F_q^n \to F_q^{o_2}$ решти координат o_2. Тоді O_2 можна знайти як ядро лінійного відображення

$$o \to \begin{pmatrix} \mathcal{P}`_1(e_1, o) \\ \ldots \\ \mathcal{P}`_1(e_n, o) \end{pmatrix}.$$

Простір O_2 знаходиться в цьому ядрі, оскільки $\mathcal{P}`(x, o) \in W$ для всіх x $\in F_q^n$ і з великою долею ймовірності, маємо що ядро в точності дорівнює O_2. Тепер нехай U – зміна змінних, яка надсилає останні o_2 координати F_q^n до O_2, і нехай

$$V \circ \mathcal{P} \circ U(x) = F(x) = \begin{cases} F_1(x) \\ F_2(x) \end{cases},$$

де знову F_1 складається з перших $m - o_2$, а F_2 – з решти o_2 координат $V \circ \mathcal{P} \circ U$. Тоді F_1 залежить лише від перших $n - o_2$ записів x: нехай y – вектор, перші $n - o_2$ записів якого дорівнюють нулю, тоді $U(y) \in O_2$, тому $F_1(x + y) = F_1(x) + \mathcal{P}`_1 (U(x), U(y)) + \mathcal{P}(U(y)) = F_1(x)$. Крім того, F_1 звертається в нуль на $U^{-1} O_1$, оскільки $\mathcal{P}(O_1) \in W$. Отже, ігноруючи останні координати o_2, F_1 має структуру відкритого ключа UOV з $n' = n - o_2$ змінних і масляним простором розмірності $m' = m - o_2$.

Пошук прообразів для $\mathcal{P}$ еквівалентний пошуку прообразів для F, оскільки вони відрізняються трансформацією змінних, відомих зловмиснику. Тепер необхідно довести, що пошук прообразів для F зводиться до пошуку прообразів для F_1: припустимо, дано t = (t_1,t_2) і ми хочемо знайти *x* таке, що $F_1(x) = t_1$ і $F_2(x) = t_2$. Діємо наступним чином:

1. Знайти x таке, що $F_1(x) = t_1$ з деякою атакою на UOV з параметрами $(n', m') = (n - o_2, m - o_2)$,

2. Розв'яжіть для $o \in F_q^n$, у якого перших $n - o_2$ записів дорівнюють нулю так, що $F_2(x + o) = t2$. Це система o_2 лінійних рівнянь у o_2 змінних, оскільки $F_2(x + o) = F_2(x) + F'_2(x, o)$ є лінійною по o, тому o можна ефективно знайти.

3. Вихід $x + o$. Зверніть увагу, що $F_1(x + o) = F_1(x) = t_1$, оскільки F_1 залежить лише від перших $n - o_2$ змінних. Отже, $x + o$ дійсно є рішенням.

П р и м і т к а . Саме так працює справжній алгоритм підписання, за винятком того, що справжній підписувач володіє знаннями про O_1, що дозволяє йому ефективно виконувати перший крок.

Для наборів параметрів SL 1 у другому та третьому раундах NIST, F_1 є відображенням UOV, параметри якої (n', m') = (64,32) і (68,32) відповідно. У цих випадках атака Кіпніса – Шаміра [4], яка виконується за час $q^{n'-2m'} \cdot poly(n')$, може дуже ефективно відновити O_1, тому ми маємо повну атаку відновлення ключа. Для набору параметрів SL 3 і 5 екземпляри UOV можуть протистояти відомим атакам відновлення ключів, тому повна атака відновлення ключів здається недосяжною. Однак, оскільки $m' = m - o_2$ є відносно малим, ми все ще можемо вирішити $F_1(x) = t_1$, тому можливо підробити підписи без відновлення O_1. Для параметрів, поданих до NIST, вартість вирішення $F_1(x) = t_1$ за допомогою алгоритму Відемана XL нижча, ніж складність пошуку O_2 і W, тому складність атаки підробки переважає вартість пошуку O_2 і W .

Приклад 2. Набір параметрів SL1 другого раунду подання NIST дорівнює $q = 16, n = 96, m = 64, o_2 = 32$. Щоб знайти O_2 і W для цього набору параметрів, нам потрібно розв'язати системи $m - 1$ = 63 однорідні квадратні рівняння з $n - m - 1$=31 змінною, тому орієнтовна вартість розв'язання кожної системи становить 252,3 множення (див. приклад 1). У середньому нам потрібно перевірити 15,06 систем. Якщо вартість одного F_{16}-множення становить 36 процедур, то можемо оцінити, що загальна середня вартість елемента пошуку O_2 і W становить 252,3 · 15,06 · 36 ≈ 261,4. Після того як ми знайшли O_2 і W, у нас залишився відкритий ключ UOV з m′ = 32 рівняннями і n′ = 64 змінними. Отже, O_1 можна знайти за поліноміальний час з атакою Кіпніса – Шаміра[4]. У складності атаки переважає перший крок, який має складність ≈ 261,4, як зазначено в табл. 1.

Таблиця 1

Огляд вартості запропонованих атак у порівнянні з відомими атаками для шести наборів параметрів Rainbow які були подані до другого раунду та фіналу NIST PQC. Складність атак наведено у вигляді $\log_2$ прогнозуємої кількості операції. Складності відомих атак взяті з [12]. Для параметрів SL I наведено атаку відновлення ключа (позначено $*$), інші атаки є атаками підробки

Набір параметрів		q, n, m, o_2	Проста атака	Комбінована атака	Відомі атаки
Другий раунд	SL 1	(16, 96, 64, 32)	61*	93*	123*
	SL 3	(256, 140, 72, 36)	186	131	151
	SL 5	(256, 188, 96, 48)	246	164	191
Фіналісти	SL 1	(16, 100, 64, 32)	69*	99*	127*
	SL 3	(256, 148, 80, 48)	160	157	177
	SL 5	(256, 196, 100, 64)	257	206	226

Рангові експерименти

Проста атака. Для деяких наборів параметрів Rainbow над F_{31} створюємо певні $\tilde{\mathcal{P}}(x) = 0$ системи, як наведено у означеній простій атаці, і обчислюємо ранги матриці Маколея цих систем різного ступеня. Ці ранги відображаються в табл. 2. Аналогічно для деяких параметрів веселки над F_{16} ми будуємо певні $\hat{\mathcal{P}}(x) = 0$ системи, і відображаємо ранги матриць Маколея в табл. 3. Ми спостерігаємо в обох випадках, що ранги ідентичні рангам системи рівномірно випадкових квадратних рівнянь відповідних розмірів.

Тобто, якщо $\tilde{\mathcal{P}}(x)$ (або$\hat{\mathcal{P}}(x)$) має m рівнянь і n змінних, то ранг його Матриця Маколея на ступені D дорівнює коефіцієнту t^D в степеневому ряді розширення

$$(1 - t)^n(1 - (1 - t^2)^m),$$

якщо цей коефіцієнт додатний. Інакше система має ядро розмірності 1, що відповідає одномірному простору розв'язків. Це є свідченням того, що системи $\tilde{\mathcal{P}}(x) = 0$ і $\hat{\mathcal{P}}(x) = 0$ не мають конкретних відмінностей, які роблять їх легшими або складнішими для розв'язування в порівнянні з випадковими системами.

Комбінована атака. Табл. 4 надає інформацію про деякі з наших рангових експериментів для комбінованої атаки. Для деяких невеликих наборів параметрів Rainbow була виконана комбінована атака з розділу 4 для отримання екземпляра MinRank $n - m$ матриць з $n - 1$ рядками і m стовпцями (з яких ми зберігаємо m'). Потім були побудовані лінеаризовані системи, як вони рахуються в алгоритмі розв'язування MinRank за авторством Барде та ін. на кількох ступенях (b, 1), і обчислені їхні ранги. Виявилось для непарних характеристик ранг матриць Маколея завжди відповідає випадковим екземплярам MinRank з відповідними параметрами. Натомість, були виявлені невеликі дефекти рангів в двох характеристиках (підкреслені в табл. 4).

Таблиця 2

Ранг і кількість стовпців матриць Маколея для $\tilde{\mathcal{P}}(x) = 0$ система рівнянь простої атаки над F_{31}. Ранги матриці Маколея ступеня *D* виділено жирним шрифтом, якщо систему можна розв'язати на цьому ступені

Параметри Rainbow			Розмір $\tilde{\mathcal{P}}$			Ранг матриці Маколея ступеня *D*		
n	*m*	o_2	*m*	*n*		*D = 2*	*D = 3*	*D = 4*
30	20	10	20	10	Ранг Стовпички	20 55	200 220	**714** 715
45	30	15	30	15	Ранг Стовпички	30 120	450 680	**3059** 3060
60	40	20	40	20	Ранг Стовпички	40 210	800 1540	7620 8855

Таблиця 3

Ранг і кількість стовпців матриць Маколея для $\hat{\mathcal{P}}(\mathrm{x}) = 0$ система рівнянь простої атаки над F_{16} . Ранги матриці Маколея ступеня *D* виділено жирним шрифтом, якщо систему можна розв'язати на цьому ступені

Параметри Rainbow			Розмір $\hat{\mathcal{P}}$			Ранг матриці Маколея ступеня *D*		
n	*m*	o_2	*m*	*n*		*D = 2*	*D = 3*	*D = 4*
30	20	10	19	9	Ранг Стовпички	19 45	**164** 165	
36	24	12	23	11	Ранг Стовпички	23 66	253 286	**1000** 1001
42	28	14	27	13	Ранг Стовпички	27 91	351 455	**1819** 1820

Таблиця 4

Ранг і кількість стовпців матриць Маколея для проблеми MinRank внаслідок комбінованої атаки над F_{31} і F_{16}. Ранги матриці Маколея на бі-ступені (b, 1) виділені жирним шрифтом, якщо систему можна розв'язати на цьому ступені

Параметри Rainbow			Параметри MinRank			Ранг матриці Маколея бі-ступеня (*b*, 1)		
n	*m*	o_2	*k*	*m`*		*b = 1*	*b = 2*	*b = 3*
15	10	5	5	8	Ранг F_{31} Ранг F_{16} Стовпички	**279** **279** 280		
15	10	5	5	7	Ранг F_{31} Ранг F_{16} Стовпички	98 98 105	**314** **314** 315	
14	6	4	8	6	Ранг F_{31} Ранг F_{16} Стовпички	78 78 120	533 527 540	**1799** **1799** 1800

Результати та висновок

1. Вартість і ймовірність успіху атаки на практиці відповідають тому, що передбачає теорія. Очікується, що атака відновлення ключа проти набору параметрів SL 1, що подані Rainbow в третьому раунді, буде складніша лише на коефіцієнт 2^8, що хоч і вимагає від зловмисника більшої, проте все ще помірної кількості ресурсів.

2. Можливо було б перейти до більших параметрів для захисту від атаки, що представлена в цій статті, ціною більшого розміру ключів і підпису. Наприклад, параметри SL 3 подання третього раунду, схоже, забезпечують достатній рівень безпеки для SL 1, але ці параметри мають в 2,5 та 4,4 рази довший підпис та відкритий ключ порівняно з параметрами SL 1. Проте, схоже, також є потенціал для покращення атак, тому необхідно більше досліджень, перш ніж зможемо мати впевненість в безпеці Rainbow. Більше того, отримана схема підпису Rainbow була менш ефективною, ніж схема «Oil and Vinegar».

Список літератури:

1. Jintai Ding and Dieter Schmidt. Rainbow, a new multivariable polynomial signature scheme. In John Ioannidis, Angelos Keromytis, and Moti Yung, editors, ACNS 05, volume 3531 of LNCS, pages 164–175. Springer, Heidelberg, June 2005. 1.
2. Jacques Patarin. The oil and vinegar signature scheme. In Dagstuhl Workshop on Cryptography September, 1997, 1997. 1, 5.
3. Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In Jacques Stern, editor, EUROCRYPT'99, volume 1592 of LNCS, pages 206–222. Springer, Heidelberg, May 1999. 1.
4. Aviad Kipnis and Adi Shamir. Cryptanalysis of the oil & vinegar signature scheme. In Hugo Krawczyk, editor, CRYPTO'98, volume 1462 of LNCS, pages 257–266. Springer, Heidelberg, August 1998. 1, 3, 4.
5. Bo-Yin Yang and Jiun-Ming Chen. Building secure tame-like multivariate public-key cryptosystems: The new TTS. In Colin Boyd and Juan Manuel Gonz´alez Nieto, editors, ACISP 05, volume 3574 of LNCS, pages 518–531. Springer, Hedelberg, July 2005. 1.
6. Olivier Billet and Henri Gilbert. Cryptanalysis of Rainbow. In Roberto De Prisco and Moti Yung, editors, SCN 06, volume 4116 of LNCS, pages 336–347. Springer, Heidelberg, September 2006. 1
7. Louis Goubin and Nicolas Courtois. Cryptanalysis of the TTM cryptosystem. In Tatsuaki Okamoto, editor, ASIACRYPT 2000, volume 1976 of LNCS, pages 44–57. Springer, Heidelberg, December 2000. 1.
8. Jintai Ding, Bo-Yin Yang, Chia-Hsin Owen Chen, Ming-Shing Chen, and Chen-Mou Cheng. New differential-algebraic attacks and reparametrization of Rainbow. In Steven M. Bellovin, Rosario Gennaro, Angelos D. Keromytis, and Moti Yung, editors, ACNS 08, volume 5037 of LNCS, pages 242–257. Springer, Heidelberg, June 2008. 1, 2.
9. Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray A. Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier A. Verbel. Improvements of algebraic attacks for solving the rank decoding and MinRank problems. In Shiho Moriai and Huaxiong Wang, editors, ASIACRYPT 2020, Part I, volume 12491 of LNCS, pages 507–536. Springer, Heidelberg, December 2020. 1, 2, 4, 5.
10. John Baena, Pierre Briaud, Daniel Cabarcas, Ray Perlner, Daniel Smith-Tone, and Javier Verbel. Improving support-minors rank attacks: applications to GeMSS and rainbow. Cryptology ePrint Archive, Report 2021/1677, 2021. https://eprint.iacr.org/2021/1677. 1
11. Ray Perlner and Daniel Smith-Tone. Rainbow band separation is better than we thought. Cryptology ePrint Archive, Report 2020/702, 2020. https://eprint.iacr.org/2020/702. 1
12. Ward Beullens. Improved cryptanalysis of UOV and rainbow. In Anne Canteaut and Fran¸cois-Xavier Standaert, editors, EUROCRYPT 2021, Part I, volume 12696 of LNCS, pages 348–373. Springer, Heidelberg, October 2021. 1, 1, 1, 2, 2, 3, 4, 5 14 Ward Beullens.
13. Response to recent paper by Ward Beullens. https://troll.iis.sinica.edu.tw/by-publ/recent/response-ward.pdf, 2020. 1.
14. Daniel Lazard. Gr¨obner bases, Gaussian elimination and resolution of systems of algebraic equations. In European Conference on Computer Algebra, pages 146– 156. Springer, 1983. 2.
15. Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In Bart Preneel, editor, EUROCRYPT 2000, volume 1807 of LNCS, pages 392–407. Springer, Heidelberg, May 2000. 2.
16. Wael Said Abdelmageed Mohamed, Jintai Ding, Thorsten Kleinjung, Stanislav Bulygin, and Johannes Buchmann. Pwxl: A parallel wiedemann-xl algorithm for solving polynomial equations over gf (2). In Conference on Symbolic Computation and Cryptography, page 89, 2010. 2.
17. Chen-Mou Cheng, Tung Chou, Ruben Niederhagen, and Bo-Yin Yang. Solving quadratic equations with XL on parallel architectures. In Emmanuel Prouff and Patrick Schaumont, editors, CHES 2012, volume 7428 of LNCS, pages 356–373. Springer, Heidelberg, September 2012. 2, 5.

Надійшла до редколегії 02.06.2022

Відомості про автора:

Малєєва Ганна Андріївна – аспірант кафедри безпеки інформаційних технологій, Харківський національний університет радіоелектроніки,Україна, e-mail: hanna.malieieva@nure.ua