УДК 003.026:004.056 **DOI:10.30837/rt.2021.1.204.06**

С.О. КАНДІЙ, Г.А. МАЛЄЄВА

АНАЛІЗ СКЛАДНОСТІ АТАК НА МУЛЬТИВАРІАТИВНІ КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ З ВИКОРИСТАННЯМ АЛГЕБРАЇЧНОЇ СТРУКТУРИ ПОЛЯ

Вступ

В останні роки інтерес до криптосистем, що ґрунтуються на багатовимірних квадратичних перетвореннях (MQ-перетвореннях), значно зріс. В першу чергу це пов'язано з конкурсом NIST PQC [1] та необхідністю у практичних схемах електронного підпису, що є стійкими до атак на квантових комп'ютерах. Незважаючи на те, що світовою спільнотою була проведена велика робота з криптоаналізу представлених схем, багато питань потребують подальшого уточнення. Спеціалісти NIST дуже обережно підходять до процесу стандартизації і закликають криптологів [4] у найближчі три роки провести всесторонній аналіз фіналістів конкурсу NIST PQC перед їх стандартизацією.

Одним з фіналістів є схема електронного підпису Rainbow [2]. Вона є узагальненням схеми UOV (Unbalanced Oil and Vinegar) [3]. Нещодавно на інше узагальнення цієї схеми – LUOV (Lifted UOV) [5] була знайдена атака [6], що за поліноміальний час здатна повністю відновити закритий ключ. Особливістю цієї атаки є використання алгебраїчної структури поля, над яким задане MQ-перетворення. Цей напрямок атак з'явився нещодавно і досі не зрозуміло чи можливо використовувати структуру поля у схемі Rainbow.

Метою цієї роботи є систематизація технік, що використовуються у атаках з використанням алгебраїчної структури поля для криптосистем на основі UOV та аналіз перешкод для їх узагальнення на схему Rainbow.

Схема UOV та її узагальнення

Нехай задано поле $GF(q_1)$ та його підполе $GF(q_2) \subseteq GF(q_1)$. В основі системи UOV лежить перетворення $F : GF^n(q_1) \to GF^m(q_1)$, яке задається n багатовимірними поліномами від m змінних:

$$F(X) = \begin{cases} f^{(1)}(X) = \sum\limits_{i=1}^{n}\sum\limits_{j=i}^{n} \alpha_{ij_1} x_i x_j + \sum\limits_{i=1}^{n} \beta_{i_1} x_i + \gamma_1 \\ f^{(2)}(X) = \sum\limits_{i=1}^{n}\sum\limits_{j=i}^{n} \alpha_{ij_2} x_i x_j + \sum\limits_{i=1}^{n} \beta_{i_2} x_i + \gamma_2 \\ \vdots \\ f^{(m)}(X) = \sum\limits_{i=1}^{n}\sum\limits_{j=i}^{n} \alpha_{ij_m} x_i x_j + \sum\limits_{i=1}^{n} \beta_{i_m} x_i + \gamma_m \end{cases},$$

де коефіцієнти $\alpha_{ij_k}, \beta_{i_k}, \gamma_k$ у загальному випадку належать полю $GF(q_2) \subseteq GF(q_1)$. Знаходження прообразу для цього перетворення є складною задачею, оскільки воно містить нелінійну частину $\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{n} \alpha_{ij_k} x_i x_j$. Надалі це перетворення маскується двома афінними перетвореннями $P = S \circ F \circ T$. Підпис є прообразом для повідомлення відносно цього фінально-

го перетворення. Виробити підпис можливо, якщо зафіксувати частину таким чином, щоб система рівнянь стала лінійною. Нелінійна частина у цьому випадку ділиться на дві незалежні частини. В схемі Rainbow цей поділ узагальнюється на більшу кількість незалежних частин. Детальний огляд змін наданий в специфікації Rainbow [2]. Як правило, в криптосистемах, що побудовані на схемі UOV, використовується поле $GF(2^r)$. Цей вибір обумовлений тим, що для цього поля, на відміну від інших відомих полів, можливо реалізувати швидкі та константні за часом алгоритми множення поліномів. Для поля $GF(p)$, де p-просте число, ці показники значно погіршуються.

Диференційні атаки на підполе

Основною проблемою криптосистем на MQ-перетвореннях є великі розміри ключів. У деяких криптосистемах [5] для вирішення цієї проблеми у якості поля $GF(q_2)$ використовують поле $GF(2)$. Це призвело до появи диференційних атак на підполе (subfield differential attack) [7]. Атака є можливою через наявність проміжних підполів між $GF(q_1)$ та $GF(q_2)$: існує поле $GF(2^d)$, таке що

$$GF(2) \subset GF(2^d) \subset GF(2^r). \tag{1}$$

Якщо таке поле існує, то можливо побудувати ізоморфізм

$$GF(2^r) \cong GF(2^d)[X]/(g(t)), \tag{2}$$

де $g(t)$ є незвідним поліномом степеня $s = r/d$. У цьому випадку компоненти рівнянь можливо перегрупувати за степенями t і створити нову систему рівнянь, яка містить меншу кількість нелінійних компонентів.

Ключова ідея атаки полягає у пошуку прообразу для довільного елемента $Y \in GF^n(2^r)$ в формі диференціалу $X = X' + \bar{X}$, де $X' \in GF^n(2^r)$ і $\bar{X} \in GF^n(2^d)$. При цьому X' обирається випадковим чином. Оскільки $\bar{X}$ належить до проміжного поля $GF(2^d)$, то множина рішень суттєво зменшується.

Розглянемо детальніше процес пошуку рішення. Якщо обчислити $P(X' + \bar{X})$, то матимемо:

$$P(X' + \bar{X}) = \begin{cases} p^{(1)}(X' + \bar{X}) = \sum_{i=1}^{n}\sum_{j=i}^{n} \alpha_{ij_1}(x_i' + \bar{x}_i)(x_j' + \bar{x}_j) + \sum_{i=1}^{n} \beta_{i_1}(x_i' + \bar{x}_i) + \gamma_1 \\ p^{(2)}(X' + \bar{X}) = \sum_{i=1}^{n}\sum_{j=i}^{n} \alpha_{ij_2}(x_i' + \bar{x}_i)(x_j' + \bar{x}_j) + \sum_{i=1}^{n} \beta_{i_2}(x_i' + \bar{x}_i) + \gamma_2 \\ \vdots \\ p^{(m)}(X' + \bar{X}) = \sum_{i=1}^{n}\sum_{j=i}^{n} \alpha_{ij_m}(x_i' + \bar{x}_i)(x_j' + \bar{x}_j) + \sum_{i=1}^{n} \beta_{i_m}(x_i' + \bar{x}_i) + \gamma_m \end{cases}$$

Після розкриття дужок та перегрупування невідомих маємо нову систему рівнянь відносно $\bar{X}$:

$$P(X'+\overline{X})=\begin{cases} p^{(1)}(X'+\overline{X})=\sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij_1}(x_j'\overline{x}_i+x_i'\overline{x}_j+x_i'x_j')+\sum_{i=1}^{n}\beta_{i_1}(\overline{x}_i+x_i')+\gamma_k+\sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij_1}\overline{x}_i\overline{x}_j \\ p^{(2)}(X'+\overline{X})=\sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij_2}(x_j'\overline{x}_i+x_i'\overline{x}_j+x_i'x_j')+\sum_{i=1}^{n}\beta_{i_2}(\overline{x}_i+x_i')+\gamma_k+\sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij_2}\overline{x}_i\overline{x}_j \\ \vdots \\ p^{(m)}(X'+\overline{X})=\sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij_m}(x_j'\overline{x}_i+x_i'\overline{x}_j+x_i'x_j')+\sum_{i=1}^{n}\beta_{i_m}(\overline{x}_i+x_i')+\gamma_k+\sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij_m}\overline{x}_i\overline{x}_j \end{cases}$$

У новій системі рівнянь можливо виділити лінійну частину $G_k(\overline{X}), k=1...m$:

$$G_k(\overline{X})=\sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij_2}(x_j'\overline{x}_i+x_i'\overline{x}_j+x_i'x_j')+\sum_{i=1}^{n}\beta_{i_2}(\overline{x}_i+x_i')+\gamma_k \tag{3}$$

Та квадратичну частину $Q_k(\overline{X}), k=1...m$:

$$Q_k(\overline{X})=\sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij_k}\overline{x}_i\overline{x}_j\ . \tag{4}$$

Оскільки існує ізоморфізм (2), то рішення системи можливо розглядати як поліном відносно деякої змінної t:

$$P(X'+\overline{X})=\sum_{i=0}^{s-1}w_{i_k}t^i\ . \tag{5}$$

При цьому частина матиме вигляд

$$G_k(\overline{X})=\sum_{i=1}^{s-1}g_{i_k}(\overline{X})t^i, \tag{6}$$

де $g_{i_k}(\overline{X})$ - нові лінійні поліноми. І квадратична частина, оскільки $\overline{X}\in GF^n(2^d)$, матиме вигляд

$$Q_k(\overline{X})=w_{0_i} \tag{7}$$

Такий простий вигляд зумовлений тим, що $\alpha_{ij_k}\in GF(2)$. Тож, якщо підсумувати (5) - (7), то отримуємо нову систему рівнянь:

$$P(X'+\overline{X})=\begin{cases} p^{(1)}(X'+\overline{X})=\sum_{i=1}^{s-1}g_{i_2}(\overline{X})t^i+Q_2(\overline{X})=\sum_{i=0}^{s-1}w_{i_2}t^i \\ p^{(2)}(X'+\overline{X})=\sum_{i=1}^{s-1}g_{i_2}(\overline{X})t^i+Q_2(\overline{X})=\sum_{i=0}^{s-1}w_{i_2}t^i \\ \vdots \\ p^{(m)}(X'+\overline{X})=\sum_{i=1}^{s-1}g_{i_m}(\overline{X})t^i+Q_m(\overline{X})=\sum_{i=0}^{s-1}w_{i_m}t^i \end{cases}.$$

Нова система є перевизначеною. Використовуючи метод [8], її можна звести до системи з $m-\left\lfloor (n-(s-1)m)/m \right\rfloor$ рівнянь та невідомих. Для більшості загальносистемних параметрів ця нова система буде суттєво меншою за оригінальну. У свою чергу, вирішення цієї системи матиме меншу складність.

Вкладені диференційні атаки на підполе

Ці атаки узагальнюють диференційні атаки. Замість пошуку прообразу у формі диференціалу $x'+\bar{x}=\sum_{i=0}^{s-1} w_i t^i+\bar{x}$ автори пропонують шукати його в формі

$$X = X_0 + X_1 t + X_2 t^2 \ldots , \tag{8}$$

де $X_0, X_1, X_2 \ldots$ шукаються ітеративно на основі попередніх значень. Для опису процедури пошуку необхідно ввести поняття s-відсічення. Процедура s-відсічення для елемента кільця $GF(2^r)$ (у поліноміальному представленні) полягає у відсіченні старших $r-s$ коефіцієнтів:

$$a=\sum_{i=0}^{r-1} a_i t^i \Rightarrow \bar{a}^s=\sum_{i=0}^{s} a_i t^i .$$

Відповідно для багатомірного полінома:

$$f(\bar{X})=\sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{ij}\bar{x}_i\bar{x}_j+\sum_{i=1}^{n}\beta_i\bar{x}_i+\gamma \Rightarrow$$

$$\Rightarrow \bar{f}^s(\bar{X})=\sum_{i=1}^{n}\sum_{j=i}^{n}\bar{\alpha}_{ij}^s\bar{x}_i\bar{x}_j+\sum_{i=1}^{n}\bar{\beta}_i^s\bar{x}_i+\bar{\gamma}^s .$$

І для системи рівнянь визначається наступним чином:

$$P(\bar{X})=\begin{cases} p_1(\bar{X}) \\ p_2(\bar{X}) \\ \vdots \\ p_m(\bar{X}) \end{cases} \Rightarrow \bar{P}^s(\bar{X})=\begin{cases} \bar{p}_1^s(\bar{X}) \\ \bar{p}_2^s(\bar{X}) \\ \vdots \\ \bar{p}_m^s(\bar{X}) \end{cases} .$$

Відповідно до введеної нотації змінні $X_0, X_1, X_2 \ldots$ знаходяться з наступних рівнянь:

X_0 - рішення рівняння $\bar{P}^0(X_0)=\bar{Y}^0$,

X_1 - рішення рівняння $\bar{P}^1(X_0+X_1 t)=\bar{Y}^1$,

X_{s-1} - рішення рівняння $\bar{P}^{s-1}(X_0+X_1 t+\ldots+X_{s-2}t^{s-2}+X_{s-1}t^{s-1})=\bar{Y}^{s-1}$.

Оскільки рішення знаходиться ітеративно, то серед цих рівнянь тільки $\bar{P}^0(X_0)=\bar{Y}^0$ є нелінійним:

$$\bar{P}^0(X_0)=\begin{cases} Q_1(X_0) \\ Q_2(X_0) \\ \vdots \\ Q_m(X_0) \end{cases},$$

де $Q_k(X_0)$ визначається за формулою (7). Для всіх інших випадків до рівняння буде додаватися лінійний член. Так для $0<s<r$ система рівнянь матиме вигляд:

$$\bar{P}^s(X_s)=\begin{cases} \sum_{i=1}^{s-1} g_{i_1}(X_i)t^i + Q_1(X_0) + g_{s_1}(X_s) \\ \sum_{i=1}^{s-1} g_{i_2}(X_i)t^i + Q_2(X_0) + g_{s_2}(X_s) \\ \vdots \\ \sum_{i=1}^{s-1} g_{i_m}(X_i)t^i + Q_m(X_0) + g_{s_m}(X_s) \end{cases}.$$

Оскільки нелінійна частина знаходиться на першому кроці, то вирішити всі системи, окрім першої, можливо за поліноміальний час. Тож, складність атаки визначається складністю вирішення системи для випадку $s=0$.

Аналіз атак та перспективи розвитку

Розглянуті атаки ґрунтуються на декількох припущеннях:

- поле, над яким визначена система рівнянь, має нетривіальні підполя. Пошук прообразу відбувається в одному з таких підполів;
- можливо знайти представлення елементів поля як поліномів з коефіцієнтами з підполя в аналітичному вигляді;
- ймовірність того, що існує рішення, яке лежить у підполі, є достатньо великою.

Для оцінки ймовірності існування рішення в диференційній атаці на підполе можливо скористуватися наступною лемою [7].

Лемма 1. Нехай A та B є двома множинами, на яких задано відображення $L: A \to B$. Тоді ймовірність того, що для будь-якого елемента $b \in B$ відображення $L^{-1}(b)$ є не пустою множиною складає $1-\exp\left(\frac{|A|}{|B|}\right)$.

У випадку коли $GF(q_1)=GF(2^r)$ і $GF(q_2)=GF(2^d)$ маємо

$$1-\exp\left(\frac{|GF^n(2^d)|}{|GF^m(2^r)|}\right) \approx 2^{-2^{d*n-r*m}}. \quad (9)$$

Це співвідношення встановлює мінімальний розмір підполя, яке може містити рішення системи з достатньо великою ймовірністю. Виходячи з виразу (9), можна сказати, що якщо використовується поле $GF(2^r)$, то мінімальне підполе $GF(2^d)$ повинно задовольняти співвідношенню

$$d > \frac{r*m}{n}.$$

Необхідність у наявності представлення елементів поля як поліномів з коефіцієнтами з підполя в аналітичному вигляді є умовою, яка суттєво обмежує застосування таких атак. Фактично вони працюють тільки коли коефіцієнти належать полю $GF(2)$. У цьому випадку при поліноміальному представленні маємо

$$\alpha * \overline{x} = \alpha * \sum_{i=0}^{s-1} w_i t^i$$

Фактично, у цьому випадку α є індикаторною величною. А коефіцієнти поліному будуть однозначно визначатися з ізоморфізму (2). Якщо використовується інше підполе, то маємо

$$\alpha * \overline{x} = \sum_{i=0}^{s-1} v_i t^i * \sum_{i=0}^{s-1} w_i t^i = \sum_{i=0}^{s-1} z_i t^i$$

де z_i нелінійно залежить як від α, так від $\overline{x}$. Тож, навіть якщо вдасться вирішити нову систему рівнянь, то відновити $\overline{x}$ з рішення буде складною задачею. В цілому, точний аналіз складності відновлення $\overline{x}$ в відкритих публікаціях відсутній. Це є предметом подальших досліджень. Наразі вирішення цієї задачі вважається достатньо складним, щоб можливо було застосовувати такі атаки на криптосистеми як Rainbow. Тож, для захисту від існуючих атак достатньо, щоб хоча б одна з умов зазначених вище не виконувалася.

Висновки

Незважаючи на те, що криптосистеми на MQ-перетвореннях були запропоновані ще у 80-х роках, вплив поля, над яким задані системи рівнянь, на безпеку схем почав досліджуватися нещодавно. Наразі відомі атаки для випадку, коли коефіцієнти багатовимірних поліномів лежать у $GF(2)$.

Для захисту від існуючих атак достатньо обрати у якості поля для рівнянь $GF(p)$, де p є простим числом. Для оптимізації розміру ключів можливо використовувати поле , що є розширенням $GF(p)$ і має групу Галуа S_n, а коефіцієнти багатовимірних поліномів обирати з $GF(p)$. У цьому випадку не існуватиме проміжних полів і значення p значно зменшиться. Такий вибір дасть гарантований захист від будь-яких атак, що використовують структуру поля. Проте ціною такого вибору є значне погіршення швидкодії системи і складності програмної реалізації.

Для випадків, коли коефіцієнти багатовимірних поліномів лежать у довільному підполі, наразі не має оцінок складності атаки через складність аналізу. Вважається, що атаки є неефективними для цього випадку. Наразі залишається ймовірність узагальнення цих атак на інші криптосистеми, такі як Rainbow. Оскільки він претендує на стандартизацію, то виникає потреба у аналізі атак з використанням структури поля для випадку довільних підполів. Такий аналіз є предметом подальших досліджень.

Список літератури:

1. NIST Web site/ Електронне посилання: https://csrc.nist.gov/projects/post-quantum-cryptography
2. Rainbow Web site / Електронне посилання: https://www.pqcrainbow.org/
3. Wolf, Christopher: Multivariate Quadratic Polynomials in Public Key Cryptography, DIAMANT/EIDMA symposium 2005
4. NISTIR 8309
5. Rainbow Web site / Електронне посилання https://www.esat.kuleuven.be/cosic/pqcrypto/luov/
6. 6 Jintai Ding and Joshua Deaton and Vishakha and Bo-Yin Yang The Nested Subset Differential Attack: A Practical Direct Attack Against LUOV which Forges a Signature within 210 Minutes / Електронне посилання: https://eprint.iacr.org/2020/967.pdf

7. Jintai Ding, Zheng Zhang, Joshua Deaton, Kurt Schmidt, FNU Vishakha New Attacks on Lifted Unbalanced Oil Vinegar, Електронне посилання: https://csrc.nist.gov/CSRC/media/Events/Second-PQC-Standardization Conference/documents/accepted-papers/ding-new-attacks-luov.pdf

8. Enrico Thomae and Christopher Wolf. Solving underdetermined systems of multivari-ate quadratic equations revisited. In Public Key Cryptography- PKC2012-15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May21-23, 2012. Proceedings, pages 156–171. Springer, 2012

Надійшла до редколегії 07.02.2021

Відомості про авторів:

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

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