УДК 004.056.55:512.6

ДИФЕРЕНЦІАЛЬНО-ОБЕРТАЛЬНИЙ КРИПТОАНАЛІЗ ARX-КРИПТОСИСТЕМ ЗА ОПЕРАЦІЄЮ МОДУЛЬНОГО ДОДАВАННЯ

Д. С. Кобець[1,а], С. В. Яковлєв[1,б]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

У даній роботі пропонується новий підхід до диференціально-обертального криптоаналізу, який використовує різниці за операцією модульного додавання. Введено поняття RA-диференціалу (по аналогії з RX-диференціалом), знайдено аналітичні вирази для імовірностей RA-диференціалів базових ARX-перетворень: модульного додавання та віднімання, циклічного зсуву, побітового додавання.

Ключові слова: ARX-криптосистеми, диференціальний аналіз, обертальний аналіз, циклічний зсув

Вступ

ARX-криптосистеми будуються на основі виключно простих операцій, доступних на рівні інструкцій обчислювальних процесорів: модульного додавання, побітового додавання, циклічних зсувів та, у розширеному розумінні, інших операцій логіки (ТА, АБО, нециклічних зсувів тощо). Через просту реалізацію та надвисоку швидкість роботи такі криптосистеми стали важливою частиною так званої «легкої криптографії» — напрямку, присвяченому розробці надійних алгоритмів для малоресурсних пристроїв та Інтернету речей.

Одним з основних інструментів аналізу ARX-криптосистем є диференціальний криптоаналіз, який у даному контексті можна розглядати як за операцією побітового додавання [1], так і за опреацією модульного додавання [2]. Алгебраїчна структура ARX-систем призвела до появи специфічного типу криптоаналізу так званого обертального криптоаналізу [3], який досліджує особливості зміни пар текстів, які відрізняються циклічним зсувом під час виконання обчислень. Обертальний криптоаналіз дозволяє будувати ефективні атаки на ARX-системи, тому захищеність від нього є однією з обов'язкових умов для надійних криптосистем даного типу.

У роботі [4] було запропоновано *диференціально-обертальний криптоаналіз*, який комбінує ідеї диференціального та обертального криптоаналізу. Диференціально-обертальний криптоаналіз досліджує проходження через криптосистему пар текстів, які відрізняються одночасно і циклічним зсувом, і деякою різницею, яка в оригінальній роботі розглядалась відносно операції побітового додавання.

У даній роботі буде запропоновано підхід до диференціально-обертального криптоаналізу, у якому різниці між текстами розглядаються за додаванням за модулем 2^n. Буде проаналізовано базові складові усіх ARX-криптосистем: функції модульного додавання та віднімання, циклічного зсуву, побітового додавання, — та знайдено імовірності проходження узагальнених диференціалів через зазначені функції, що дозволить оцінювати стійкість до даного методу криптоаналізу.

[а] denis.kobets8@gmail.com
[б] yasv@rl.kiev.ua

1. Узагальнений диференціал за модульним додаванням

Введемо необхідні в подальшому умовні позначення:

V_n — множина всіх бітових векторів довжини n;

$x \in V_n$ — довільний вектор, біти якого нумеруються так:

$$x = (x_{n-1}, \dots, x_0);$$

x^r — циклічний зсув вектора x на r позицій ліворуч, тобто

$$x^r = x \lll r = (x_{n-r-1}, \dots, x_0, x_{n-1}, \dots, x_{n-r}).$$

Для класичного диференціального криптоаналізу, що використовує різниці за операцією $\oplus$ [1], модульне додавання є складним нелінійним перетворенням. Альтернативним шляхом криптоаналізу ARX-систем є використання різниць за операцією модульного додавання $+$, завдяки чому вузли криптосистеми із модульним додаванням стають лінійними відносно цієї різниці [2]. Однак на нелінійні перетворюються вузли із операціями $\oplus$ та циклічними зсувами.

Нехай $F\colon V_n \times V_n \to V_n$. *Диференціалом* функції F називається довільна трійка векторів $(\alpha, \beta \to \gamma)$, де $\alpha, \beta, \gamma \in V_n$ розглядаються як різниці між значеннями вхідних аргументів або виходу функції. Якщо різниці розглядаються за операцією модульного до-

давання, то імовірність диференціалу $(\alpha, \beta \to \gamma)$ функції F визначається як [2]

$$adp^F(\alpha, \beta \to \gamma) = \\ = \Pr_{x,y}\{F(x+\alpha, y+\beta) = F(x,y) + \gamma\}.$$

У роботі [4] було введено поняття *узагальненого диференціалу*, або *RX-диференціалу* $(r; \alpha, \beta \to \gamma)$, де $0 \le r < n$ — величина циклічного зсуву між текстами, а $\alpha, \beta, \gamma \in V_n$ розглядались як різниці між проміжними текстами за операцією побітового додавання. Імовірність RX-диференціалу визначається як

$$xrp^F(r; \alpha, \beta \to \gamma) = \\ = \Pr_{x,y}\{F(x^r \oplus \alpha, y^r \oplus \beta) = (F(x,y))^r \oplus \gamma\}.$$

Введемо поняття *узагальненого диференціалу за операцією модульного додавання*, або просто *RA-диференціалу* $(r; \alpha, \beta \to \gamma)$ для функції F, де $0 \le r < n$ так само визначає величину циклічного зсуву між текстами, а $\alpha, \beta, \gamma \in V_n$ розглядаються як різниці між проміжними текстами за операцією додавання за модулем 2^n. Імовірність RA-диференціалу визначимо як

$$arp^F(r; \alpha, \beta \to \gamma) = \\ = \Pr_{x,y}\{F(x^r + \alpha, y^r + \beta) = (F(x,y))^r + \gamma\}.$$

Зауважимо, що поняття RA-диференціалу природним чином поширюється на функції від іншої кількості змінних; наприклад, для відображення $f\colon V_n \to V_n$ RA-диференціал має вид $(r; \alpha \to \beta)$, а його імовірність визначається як

$$arp^f(r; \alpha \to \beta) = \Pr_x\{f(x^r + \alpha) = (f(x))^r + \beta\}.$$

Для дослідження поведінки імовірностей RA-диференціалів корисною виявилась теорема Даума.

Теорема (Даум) [5]. Для довільних n-бітових векторів x, y та $x = x_{n-r} \cdot 2^r + x_r$, $y = y_{n-r} \cdot 2^r + y_r$, де $|x_{n-r}| = |y_{n-r}| = n - r$ та $|x_r| = |y_r| = r$, справедливі рівності

$$\begin{aligned} (x+y)^r - (x^r + y^r) &= (-c) \cdot 2^{n-r} + c_r, \\ (x-y)^r - (x^r - y^r) &= c' \cdot 2^{n-r} + c'_r, \end{aligned}$$

де $c = [x + y \ge 2^n]$, $c_r = [x_r + y_r \ge 2^r]$, $c' = [x < y]$, $c'_r = [x_r < y_r]$, тут [] позначають індикатор.

Іншими словами, c, c_r, c', c'_r — це біти переносу що можуть виникнути при проведені операцій над x та y.

Наслідок 1. Для довільного r, оскільки c, c_r можуть прийняти значення 0 або 1, значенням виразу $(x+y)^r - (x^r + y^r)$ буде одне з наступних: $\{0, 1, -2^{n-r}, -2^{n-r}+1\}$.

Наслідок 2. За аналогією до попереднього, для довільного r, оскільки c', c'_r також мають значення 0 або 1, значенням виразу $(x-y)^r - (x^r - y^r)$ буде одне з наступних: $\{0, 1, 2^{n-r}, 2^{n-r}+1\}$.

Наслідок 3. Імовірності появи кожного з можливих значень у теоремі Даума описуються імовірностями P_{c,c_r} (P_{c',c'_r}), де

$$\begin{aligned} P_{0,0} &= \frac{1}{4}\left(1 + 2^{-(n-r)} + 2^{-r} + 2^{-n}\right), \\ P_{0,1} &= \frac{1}{4}\left(1 - 2^{-(n-r)} - 2^{-r} + 2^{-n}\right), \\ P_{1,0} &= \frac{1}{4}\left(1 - 2^{-(n-r)} + 2^{-r} - 2^{-n}\right), \\ P_{1,1} &= \frac{1}{4}\left(1 + 2^{-(n-r)} - 2^{-r} - 2^{-n}\right). \end{aligned}$$

2. Імовірності RA-диференціалів базових перетворень ARX-криптосистем

У даному розділі ми розглянемо усі базові операції, які використовуються в ARX-криптосистемах, та знайдемо аналітичні вирази для імовірностей RA-диференціалів цих операцій.

Першою розглянемо операцію $F(x,y) = x + y$ — додавання за модулем 2^n. Імовірність RA-диференціалу буде описуватись так:

$$arp^+(r; \alpha, \beta \to \gamma) = \\ = \Pr_{x,y}\{(x^r + \alpha) + (y^r + \beta) = (x+y)^r + \gamma\}.$$

Рівність, яка описує подію для імовірності, можна перетворити таким чином:

$$\begin{aligned} x^r + \alpha + y^r + \beta &= (x+y)^r + \gamma, \\ (x+y)^r - x^r - y^r &= \alpha + \beta - \gamma. \end{aligned}$$

Ліва частина одержаної рівності описується теоремою Даума. Тоді для довільних α, β отримаємо усього чотири можливі різниці γ із ненульовими ймовірностями:

1) $\alpha + \beta - \gamma = 0$, тобто $\gamma = \alpha + \beta$;
2) $\gamma = \alpha + \beta - 1$;
3) $\gamma = \alpha + \beta + 2^{n-r}$;
4) $\gamma = \alpha + \beta + 2^{n-r} - 1$.

Відповідно, з наслідків 1 та 3 теореми Даума випливає, що

$$arp^+(r; \alpha, \beta \to \gamma) = \begin{cases} P_{0,0}, & \gamma = \alpha + \beta, \\ P_{0,1}, & \gamma = \alpha + \beta - 1, \\ P_{1,0}, & \gamma = \alpha + \beta + 2^{n-r}, \\ P_{1,1}, & \gamma = \alpha + \beta + 2^{n-r} - 1, \\ 0, & \text{при інших } \gamma. \end{cases}$$

Зауважимо, що у диференціальному та диференціально-обертальному аналізах, які розглядають різниці за операцію побітового додавання, такі різниці проходять через операцію побітового додавання з імовірністю 1 (тобто, вихідна різниця однозначно обчислюється через вхідну). У випадку модульного додавання навіть операція модульного додавання розщеплює імовірнісні переходи на чотири можливих альтернативи.

Для функції $F(x,y) = x - y$ усі кроки по знаходженню імовірностей RA-диференціалів будуть аналогічними. Імовірність RA-диференціалу визначається

такою рівністю, в якій ліва частина описана теоремою Даума:

$$(x-y)^r - x^r + y^r = \alpha + \beta - \gamma.$$

З наслідків 2 та 3 теореми Даума, аналогічно до попереднього випадку, випливає, що

$$arp^{-}(r;\alpha,\beta\to\gamma) = \begin{cases} P_{0,0}, & \gamma = \alpha+\beta, \\ P_{0,1}, & \gamma = \alpha+\beta-1, \\ P_{1,0}, & \gamma = \alpha+\beta-2^{n-r}, \\ P_{1,1}, & \gamma = \alpha+\beta-2^{n-r}-1, \\ 0, & \text{при інших } \gamma. \end{cases}$$

Таким чином, з точки зору поведінки RA-диференціалів, модульні додавання та віднімання ведуть себе дуже схожим чином.

Розглянемо тепер операцію циклічного зсуву $f(x) = x \lll s$. Імовірність RA-диференціалу буде дорівнювати

$$arp^{\lll s}(r;\alpha\to\beta) = \\ = \Pr_x\{(x^r+\alpha)\lll s = (x\lll s)^r + \beta\}.$$

Розглянемо співвідношення

$$\begin{aligned} (x^r+\alpha)\lll s &= (x\lll s)^r + \beta, \text{ або} \\ (x^r+\alpha)^s &= (x^s)^r + \beta. \end{aligned}$$

Оскільки циклічні зсуви комутують між собою, то можна праву частину подати як $(x^r+\alpha)^s = (x^r)^s + \beta$. Введемо заміну $y = x^r$ та одержимо рівність

$$(y+\alpha)^s = y^s + \beta.$$

Імовірність цієї події була знайдена Берсоном у роботі [6]. Використовуючи результати Берсона, одержуємо

$$arp^{\lll s}(r;\alpha\to\beta) = \\ = \begin{cases} \frac{1}{2^n}\cdot(2^s-\alpha_s)\cdot(2^{n-s}-\alpha_{n-s}), & \beta = \alpha_s\|\alpha_{n-s}, \\ \frac{1}{2^n}\cdot(2^s-\alpha_s)\cdot\alpha_{n-s}, & \beta = (\alpha_s-1)\|\alpha_{n-s}, \\ \frac{1}{2^n}\cdot\alpha_s\cdot(2^{n-s}-\alpha_{n-s}-1), & \beta = \alpha_s\|(\alpha_{n-s}+1), \\ \frac{1}{2^n}\cdot\alpha_s\cdot(\alpha_{n-s}+1), & \beta = (\alpha_s-1)\|(\alpha_{n-s}+1), \\ 0, & \text{для інших } \beta. \end{cases}$$

Тут α_{n-s} та α_s— вектори зі старших $n-s$ та молодших s бітів вектору α, а операції над ними відбуваються за модулями 2^{n-s} та 2^s відповідно.

Оскільки $x \ggg s = x \lll (n-s)$, диференціальні імовірності циклічних зсувів у різні боки пов'язані співвідношенням

$$arp^{\ggg s}(\alpha\to\beta) = arp^{\lll(n-s)}(\alpha\to\beta).$$

Цей факт дозволяє застосувати аналогічний для визначення імовірностей RA-диференціалів функції $x \ggg s$.

Окремо зауважимо, що для циклічного зсуву імовірності RA-диференціалів не залежать від значення r і, фактично, співпадають з імовірностями звичайних диференціалів за модульним додаванням.

Розглянемо тепер операцію побітового додавання $F(x,y) = x \oplus y$. Імовірність RA-диференціалу цієї операції буде такою:

$$arp^{\oplus}(r;\alpha,\beta\to\gamma) = \\ = \Pr_{x,y}\{(x^r+\alpha)\oplus(y^r+\beta) = (x\oplus y)^r + \gamma\}.$$

Оскільки операція $\oplus$ виконується побітово, то справедлива рівність $(x\oplus y)^r = x^r \oplus y^r$. Введемо заміну $u = x^r$, $v = y^r$; тоді

$$arp^{\oplus}(r;\alpha,\beta\to\gamma) = \\ = \Pr_{u,v}\{(u+\alpha)\oplus(v+\beta) = (u\oplus v)+\gamma\} = \\ = adp^{\oplus}(\alpha,\beta\to\gamma).$$

Це значення, зокрема, також не залежить від значення r.

Аналогічні міркування справедливі для будь якої побітово виконуваної функції $F(x,y)$, наприклад, для $F(x,y) = x\&y$, $F(x,y) = x\vee y$, тощо:

$$arp^{F}(r;\alpha,\beta\to\gamma) = adp^{F}(\alpha,\beta\to\gamma).$$

Висновки

У даній роботі було введено поняття диференціально-обертального аналізу за операцією модульного додавання. Було знайдено імовірності RA-диференціалів для усіх базових операцій ARX-криптосистем. Показано, що для додавання, віднімання є всього 4 можливих RA-диференціалів. Для циклічного зсуву та побітово обчислюваних операцій імовірності не залежать від величини цього зсуву і, фактично, співпадають з імовірностями звичайних диференціалів. Одержані результати дозволить в подальшому аналізувати більш складні перетворення, що комбінують декілька операцій.

Перелік використаних джерел

1. *Lipmaa H., Moriai S.* Efficient Algorithms for Computing Differential Properties of Addition // Fast Software Encryption / за ред. M. Matsui. — Springer Berlin Heidelberg, 2002. — С. 336—350.
2. *Lipmaa H., Wallén J., Dumas P.* On the Additive Differential Probability of Exclusive-Or // Fast Software Encryption. — 2004. — С. 317—331. — URL: https://iacr.org/archive/fse2004/30170316/30170316.pdf.
3. *Khovratovich D., Nikolic I.* Rotational Cryptanalysis of ARX. // Lecture Notes in Computer Science. — 2010. — С. 333—346.
4. *Ashur I., Liu Y.* Rotational Cryptanalysis in the Presence of Constants. — 2016. — URL: https://eprint.iacr.org/2016/826.pdf.
5. *Daum M.* Cryptanalysis of Hash Functions of the MD4-Family (PhD thesis). — 2005.
6. *Berson T.* Differential cryptanalysis mod 2^{32} with applications to MD5 // In Advances in Cryptology – Eurocrypt'92. — 1992. — С. 71—80.