

АНАЛІТИЧНІ ВИРАЗИ ІМОВІРНОСТЕЙ ДИФЕРЕНЦІАЛІВ СКЛАДОВИХ ШИФРІВ NORX ТА CHACHA

Корж Н. С.¹, Яковлев С. В.¹

*¹Національний технічний університет України
«Київський політехнічний інститут імені Ігоря
Сікорського», м. Київ, Україна,
nik.korzh.ita@gmail.com, yasv@rl.kiev.ua*

У роботі знайдено нові аналітичні вирази для імовірностей диференціалів чвертьраундових перетворень шифрів ChaCha та NORX. Одержані вирази не ґрунтуються на припущеннях про незалежність окремих складових таких перетворень, а тому дозволяють оцінювати імовірності диференціалів більш точно, ніж у опублікованих раніше оцінках для імовірностей диференціалів зазначених шифрів.

Ключові слова: симетрична криптографія, диференціальний криптоаналіз, ChaCha, NORX.

Вступ

Диференціальний криптоаналіз [1] розглядає імовірності подій, що вхідні повідомлення із заданою різницею перейдуть у шифротексти із заданою різницею. У контексті ARX-шифрів (ChaCha [2], NORX [3]) зазвичай розглядають різниці за операцією побітового додавання.

У роботі [4] були запропоновані аналітичні вирази для імовірностей диференціалів окремих перетворень шифру ChaCha. Однак ці результати використовували припущення про незалежність появи диференціалів на окремих операціях раундових перетворень, які, взагалі кажучи, нічим не обґрунтовані.

У даній роботі наводяться точні формули для імовірностей раундових перетворень шифрів ChaCha та

NORX, які не використовують припущення про незалежність складових операцій.

Структура шифрів ChaCha та NORX

Шифр ChaCha є потоковим ARX-шифром, два послідовних раунди якого складається з восьми так званих «чвертьраундових» функцій $G(a, b, c, d)$, кожна з яких виконує перетворення над чотирма словами стану за схемою:

$$\begin{array}{ll} a \leftarrow a + b, & d \leftarrow (d \oplus a) \lll r_1, \\ c \leftarrow c + d, & b \leftarrow (b \oplus c) \lll r_2, \\ a \leftarrow a + b, & d \leftarrow (d \oplus a) \lll r_3, \\ c \leftarrow c + d, & b \leftarrow (b \oplus c) \lll r_4, \end{array}$$

де r_i – наперед визначені величини зсувів; для результатів, одержаних в даній роботі, величини r_i можуть бути довільними.

Шифр NORX використовує такі само чвертьраундові перетворення, як і ChaCha, однак модульні додавання у NORX замінені на специфічну операцію

$$H(x, y) = (x \oplus y) \oplus ((x \& y) \ll 1)$$

Функція H виконує бітове перетворення, що імітує додавання з перенесенням і застосовується багаторазово в межах основної G -функції шифру NORX.

Імовірності диференціалів чвертьраундових перетворень

Диференціалом $\omega = (\alpha, \beta \rightarrow \gamma)$ функції $f(x, y)$ називають довільну трійку векторів $\alpha, \beta, \gamma \in V_n$, що задає різниці між двома вхідними (або вихідними) значеннями f відносно операції $\oplus$. Ймовірність диференціалу ω функції f визначається як

$$\begin{aligned} xdp^f(\omega) &= xdp^f(\alpha, \beta \rightarrow \gamma) = \\ &= \Pr_{x,y} \{f(x \oplus \alpha, y \oplus \beta) = f(x, y) \oplus \gamma\} \end{aligned}$$

Ймовірності xdp^f характеризують стійкість до диференціального криптоаналізу.

Чвертьраундова функція ChaCha має два ланцюги послідовних додавань, які у попередніх роботах вважались незалежними. Однак у структурі перетворення ці додавання

не розділяються забілюваннями із ключем або іншими перетвореннями, які вносять випадковість, тому припущення про їх незалежність, взагалі кажучи, є помилковим.

Для функції $\Phi_+(x, y, z) = x + y + z$ введемо умовні диференціальні імовірності

$$xdr^{\Phi}(\alpha_x, \alpha_y, \alpha_z \rightarrow \gamma \mid \beta) = \\ = \Pr_{x,y,z} \left\{ \begin{array}{l} \Phi(x \oplus \alpha_x, y \oplus \alpha_y, z \oplus \alpha_z) = \Phi(x, y, z) \oplus \gamma, \\ (x \oplus \alpha_x) + (y \oplus \alpha_y) = (x + y) \oplus \beta \end{array} \right\}$$

Такі імовірності розглядають проходження диференціалу через складене перетворення із фіксуванням його проміжних значень. Аналогічні імовірності можна ввести й для перетворення $\Phi_H(x, y, z) = H(H(x, y), z)$, яке використовується у NORX.

Основний результат даної роботи сформулюємо у вигляді такої теореми.

Теорема. Для чвертьраундової функції $G(a, b, c, d)$ шифру ChaCha (NORX) імовірності диференціалів дорівнюють

$$xdr^G(\alpha_a, \alpha_b, \alpha_c, \alpha_d \rightarrow \gamma_a, \gamma_b, \gamma_c, \gamma_d) = \\ = \\ xdr^{\Phi}(\alpha_a, \alpha_b, \beta_b \rightarrow \gamma_a \mid \beta_a) \cdot xdr^{\Phi}(\alpha_c, \beta_d, \gamma_d \rightarrow \gamma_c \mid \beta_c),$$

$$\begin{aligned} \text{де } \beta_a &= \alpha_d \oplus (\gamma_a \ggg r_1) \oplus (\gamma_d \ggg (r_1 + r_4)), \\ \beta_b &= \gamma_c \oplus (\gamma_b \ggg r_3), \\ \beta_c &= \alpha_b \oplus (\gamma_c \ggg r_2) \oplus (\gamma_b \ggg (r_2 + r_3)), \\ \beta_d &= \gamma_a \oplus (\gamma_d \ggg r_4), \end{aligned}$$

а функція Φ визначається як Φ_+ для шифру ChaCha та Φ_H для шифру NORX.

Висновки

У даній роботі одержано аналітичні вирази для імовірностей диференціалів чвертьраундових функцій шифрів ChaCha та NORX; одержані вирази використовують новий математичний об'єкт – умовні диференціальні імовірності для композиції однотипних перетворень, у

якості яких виступають модульне додавання у шифрі ChaCha та специфічна операція, яка апроксимує модульне додавання, у шифрі NORX. Одержані вирази не ґрунтуються на припущеннях про незалежність складових елементів чвертьраундового перетворення, а тому дозволяють будувати більш точні оцінки для диференціальних імовірностей. У подальшому планується застосувати одержані результати для побудови більш ефективних розпізнавачів для шифрів ChaCha та NORX.

Список використаних джерел

1. Biham E., Shamir A. Differential Cryptanalysis of DES-like Cryptosystems, J. Cryptology, vol. 4, no. 1, 1991.
2. Bernstein D. J. The ChaCha family of stream ciphers, 2008. URL: <https://cr.yp.to/papers.html#chacha>
3. Aumasson J.-P., Jovanovic P., Neves S. NORX 3.0, CAESAR Competition Submission. URL: <https://competitions.cr.yp.to/round3/norxv30.pdf>
4. E. Bellini, R. Makarim, C. Sanna. Finding differential trails on ChaCha by means of state functions, 2021. DOI: <https://dx.doi.org/10.1504/IJACT.2024.10063705>