УДК 621.3.06

М.Ю. РОДІНКО, Р.В. ОЛІЙНИКОВ, д-р техн. наук

МЕТОДИ ПОШУКУ ДИФЕРЕНЦІЙНИХ ХАРАКТЕРИСТИК ЦИКЛОВОЇ ФУНКЦІЇ СИМЕТРИЧНОГО БЛОКОВОГО ШИФРУ «КИПАРИС»

Вступ

Малоресурсна криптографія [1] є одним з найпопулярніших напрямків у сучасній криптології, орієнтованим на розробку симетричних примітивів, що мають високу швидкодію перетворень та компактну реалізацію на різних платформах. З метою забезпечення цих вимог розробники відходять від традиційних методів побудови симетричних шифрів (зокрема заснованих на застосуванні таблиць підстановок – S-блоків) та все більше звертаються до простих операцій таких, як модульне додавання, циклічний зсув та XOR. Подібна архітектура отримала назву ARX (Addittion-Rotation-XOR) та знайшла застосування у таких відомих симетричних шифрах як SIMON [2], SPECK [3], Salsa20 [4], ChaCha20 [5] та ін.

Із урахуванням останніх тенденцій малоресурсної криптографії на основі ARX-перетворень був розроблений симетричний блоковий шифр «Кипарис» [6]. Розроблений шифр має високу швидкодію перетворень, компактну реалізацію, підтримує довжину ключа, достатню для забезпечення стійкості у постквантовий період (256 та 512 біт). Первинний аналіз алгоритму, що включав статистичне тестування та оцінку лавинних показників, показав, що блоковий шифр «Кипарис» задовольняє цим властивостям. Тепер нагальним питанням є обґрунтування стійкості шифру до найбільш відомої та ефективної атаки на блокові шифри – диференційного криптоаналізу [7].

Однак, якщо для шифрів, заснованих на S-блоках, існує загальний підхід до обґрунтування стійкості до диференційного (а також і лінійного) криптоаналізу, то для ARX-подібних примітивів такого підходу немає. Через велику кількість повторів простих операцій дуже складно представити математичне обґрунтування навіть окремого алгоритму. Зазвичай, ARX-подібна конструкція є скоріш інтуїтивною, ніж математично обґрунтованою.

Традиційно стійкість блокового шифру до диференційного криптоаналізу визначається верхньою границею ймовірності диференційної характеристики (ДХ). У статті пропонується три підходи до знаходження найбільш ймовірної диференційної характеристики блокового шифру «Кипарис».

1. Алгоритм блокового шифрування «Кипарис»

Алгоритм шифрування «Кипарис» [6] виконує перетворення блоків даних розміром l біт, із використанням ключа шифрування довжиною k біт, $l,k \in \{256,512\}$, $l = k$. Операції виконуються над s-бітними словами, $s \in \{32,64\}$.

На вхід процедури зашифрування подається блок відкритого тексту $P = (P_0, P_1, ..., P_7)$ та циклові ключі $RK^{(0)}, RK^{(1)}, \ldots, RK^{(t-1)}$. Блок відкритого тексту P ділиться на два підблока: $L_0 = (P_0, P_1, P_2, P_3)$, $R_0 = (P_4, P_5, P_6, P_7)$. Вихід i-ї ітерації перетворення обчислюється як:

$$L_i = R_{i-1} \oplus F\left(L_{i-1}, RK^{(i-1)}\right),$$

$$R_i = L_{i-1}.$$

Циклова функція F представляє собою додавання підблока L_{i-1} з ключем $RK^{(i-1)}$ за модулем 2 та двократне повторення функції $h(P_0', P_1', P_2', P_3')$, на вхід якої подається чотири s-бітних слова. Вихідне значення функції h обчислюється як:

$$P_0' = ADD(P_0', P_1'),\ P_3' = XOR(P_3', P_0'),\ P_3' = ROTL(P_3', r1),$$
$$P_2' = ADD(P_2', P_3'),\ P_1' = XOR(P_1', P_2'),\ P_1' = ROTL(P_1', r2),$$
$$P_0' = ADD(P_0', P_1'),\ P_3' = XOR(P_3', P_0'),\ P_3' = ROTL(P_3', r3),$$
$$P_2' = ADD(P_2', P_3'),\ P_1' = XOR(P_1', P_2'),\ P_1' = ROTL(P_1', r4),$$

де $ADD(x, y)$ – додавання за модулем s двох s-бітних слів; $XOR(x, y)$ – XOR двох s-бітних слів; $ROTL(x, r)$ – циклічний зсув s-бітного слова вліво на r біт.

2. Диференційні властивості операції модульного додавання

Як відомо, для знаходження диференційних характеристик шифру використовують таблицю розподілу різниць (ТРР) нелінійного перетворення. Таким перетворенням у ARX-подібному шифрі є операція додавання за модулем 2^n.

Диференційна ймовірність додавання за модулем 2^n (xdp^+) – це ймовірність, з якою вхідні різниці α та β переходять у вихідну різницю γ через застосування операції модульного додавання, обчислена для всіх можливих пар n-бітних входів [8]:

$$xdp^+(\alpha, \beta \to \gamma) = 2^{-2n} \times \#\{(x, y) : ((x \oplus \alpha) + (y \oplus \beta)) \oplus (x + y) = \gamma\}.$$

У [9] запропонований швидкий алгоритм для обчислення xdp^+, заснований на S-функціях.

У разі, якщо в якості нелінійної функції шифру виступає S-блок, побудувати ТРР дуже легко, оскільки для S-блока байт-в-байт така таблиця містить всього 256×256 елементів. Для додавання за модулем 2^{32} або більше побудувати повну ТРР не представляється можливим (розмір ТРР для додавання за модулем 2^{32} складає 2^{64}). Підхід до вирішення цієї проблеми представлений у [8], де пропонується будувати так звану часткову таблицю розподілу різниць (англ. partial difference distribution table, pDDT), що містить диференціали $(\alpha, \beta \to \gamma)$ з імовірністю p_{thres} рівною або вищою заданої:

$$(\alpha, \beta, \gamma) \in D \Leftrightarrow DP(\alpha, \beta \to \gamma) \geq p_{thres}.$$

У [8] наведено приклади побудування часткових таблиць для 32-бітових циклових функцій SPECK, XTEA.

Об'єднуючи часткові таблиці для різних компонентів циклової функції, автори будують часткову таблицю для всієї циклової функції, які використовують в модифікованому алгоритмі Мацуї для побудови багатоциклових ДХ [8].

3. Методи пошуку диференційних характеристик циклової функції блокового шифру «Кипарис»

3.1. Прямий метод пошуку ДХ

Особливістю шифру «Кипарис» є те, що циклова функція оперує $l/2$-бітними блоками даних, де $l \in \{256, 512\}$, тому побудування часткової таблиці для всієї циклової функції є складною задачею. У даному випадку, найбільш очевидним видається метод пошуку характеристик, що полягає в наступному.

1) Обрати множину $l/2$-бітних вхідних різниць Ξ.

2) Для кожної вхідної різниці $\xi_i \in \Xi$ побудувати ДХ (ξ_i, ψ_i), де ψ_i – різниця на виході циклової функції. При цьому на j-му з восьми суматорів обирати найбільш ймовірний перехід $\max(\alpha_j, \beta_j \to \gamma_j)$.

3) Імовірність знайденої ДХ $p(\xi_i \to \psi_i)$ обчислити як добуток ймовірностей перетворення на восьми суматорах:

$$p(\xi_i \to \psi_i) = \prod_{j=1}^{8} p(\alpha_j, \beta_j \to \gamma_j) \quad (1)$$

Головним питанням є вибір множини Ξ. Аналіз часткової таблиці для додавання за модулем 2^{32} показав, що ймовірність перетворення на суматорі зростає зі зменшенням кількості активних біт на вході. Так, наприклад для суматора за модулем 2^{32} та $p(\alpha, \beta \to \gamma) \geq 1/2$, максимальна кількість активних біт у вхідній різниці (α, β) складає 2 біти. У зв'язку із цим, з метою мінімізації кількості активних біт на входах суматорів циклової функції, до множини Ξ доцільно включати вхідні різниці:

- з мінімальною вагою Хемінга, наприклад такі, що мають по одному активному біту в одному, двох або трьох s-бітних словах;
- базуючись на найбільш ймовірних переходах часткової ТРР для суматора.

У результаті, за допомогою запропонованого методу для 256-бітової циклової функції шифру «Кипарис» була знайдена ДХ з імовірністю $p(\xi \to \psi) = 2^{-12}$ (табл. 1).

Таблиця 1

Параметри ДХ циклової функції шифру «Кипарис»

Вхідна різниця (hex)	80000000 80000000 80000000 0
Вихідна різниця (hex)	40844 26260262 C4484400 44084400
Ймовірність ($\log_2 p$)	-12

3.2. Метод пошуку ДХ «у двох напрямках»

Вибір вхідних різниць з мінімальною кількістю активних бітів хоч і дозволяє дещо збільшити загальну ймовірність характеристики, проте, завдяки дифузії, навіть один активний біт на вході циклової функції вже на середині перетворення активує достатньо велику кількість бітів. Як було вказано вище, циклова функція F представляє собою дві ітерації функції h. З метою активізації якомога меншого числа бітів на входах суматорів пропонується оптимізація представленого вище методу, що полягає в наступному.

1) Обрати множину $l/2$-бітних різниць Ξ тим самим способом, що й у попередньому методі.

2) Кожну різницю $\xi_i \in \Xi$ розглядати як вихід першої та вхід другої ітерації функції h. Для кожної вхідної різниці $\xi_i \in \Xi$ побудувати ДХ для функції h та її інверсії h^{-1}. ДХ для циклової функції F буде представляти об'єднання характеристик для h^{-1} та h.

3) Імовірність ДХ $p(\xi_i \to \psi_i)$ для циклової функції F обчислити як добуток на восьми суматорах за формулою (1).

Цей метод дозволив значно покращити попередній результат: для 256-бітової циклової функції шифру була знайдена ДХ з імовірністю $p(\xi \to \psi) = 2^{-3}$ (табл. 2).

Таблиця 2

Параметри ДХ циклової функції, отриманої за допомогою методу пошуку «у двох напрямках»

Вхідна різниця (hex)	80000 80080000 80000000 80000000
Вихідна різниця (hex)	800 4040040 80080000 80000
Ймовірність ($\log_2 p$)	-3

Представлений метод все одно не гарантує, що знайдена ДХ є найкращою, і не існує інших ДХ з більшою ймовірністю.

3.3. Оптимізований метод пошуку найкращої ДХ циклової функції

Відмітимо, що для знайденої вище ДХ, ймовірність перетворення на суматорі $p(\alpha_j, \beta_j \to \gamma_j) \geq 1/2$. Цей факт дозволяє стверджувати, що якщо існує якась ДХ, краща за

знайдену, то вона також буде містити переходи на суматорах з імовірністю, не менше ½. Таким чином, множину вхідних різниць Ξ можна суттєво обмежити, вибравши вхідні різниці таким чином, щоб ймовірність перетворення на перших двох суматорах була не менше ½. Це дозволить знайти ДХ з високою ймовірністю, яка існує для циклової функції. Новий метод складається з наступних кроків.

1) Побудувати ТРР для операції додавання за модулем 2^n, що містить переходи з імовірністю $p(\alpha_j, \beta_j \to \gamma_j) \geq 1/2$.

2) Враховуючи, що кожна вхідна різниця $\xi_i \in \Xi$ складається з чотирьох s-бітних слів $\xi_i = \left\{\xi_i^{(0)}, \xi_i^{(1)}, \xi_i^{(2)}, \xi_i^{(3)}\right\}$, множину вхідних різниць Ξ сформувати за допомогою алгоритму, наведеного на рис. 1.

$$
\begin{aligned}
&\textit{for each } (\alpha_j, \beta_j \to \gamma_j) \textit{ from pDDT}\\
&\xi_i^{(0)} = \alpha_j; \xi_i^{(1)} = \beta_j;\\
&\textit{for each } (\alpha_k, \beta_k \to \gamma_k) \textit{ from pDDT}\\
&\xi_i^{(2)} = \alpha_k; \xi_i^{(3)} = XOR(\gamma_j, ROTR(\beta_k, 16));
\end{aligned}
$$

Рис. 1. Алгоритм вибору вхідних різниць

3) Для кожної вхідної різниці $\xi_i \in \Xi$ побудувати ДХ (ξ_i, ψ_i). Імовірність ДХ $p(\xi_i \to \psi_i)$ для циклової функції F обчислюється як добуток на восьми суматорах за формулою (1).

Цей метод дозволив ще покращити попередній результат: для 256-бітової циклової функції шифру була знайдена ДХ з імовірністю $p(\xi \to \psi) = 2^{-2}$ (табл. 3).

Таблиця 3

Параметри ДХ циклової функції, отриманої за допомогою оптимізованого методу

Вхідна різниця (hex)	0 80000000 800000 80008080
Вихідна різниця (hex)	80000000 4000 80 80
Ймовірність ($\log_2 p$)	-2

У табл. 4 представлені переходи на суматорах, що складають отриману характеристику.

Таблиця 4

Ймовірності переходів на восьми суматорах

Номер суматора	$(\alpha, \beta) \to \gamma$		p
1	(0, 80000000)	→ 80000000	1
2	(800000, 80800000)	→ 80000000	1/2
3	(80000000, 0)	→ 80000000	1
4	(80000000, 80000000)	→ 0	1
5	(80000000, 0)	→ 80000000	1
6	(0, 0)	→ 0	1
7	(80000000, 0)	→ 80000000	1
8	(80, 0)	→ 80	1/2

З табл. 4 можна помітити, що старший активний біт різниці не впливає на ймовірність переходу, а у випадку $p = 1/2$ вхідна різниця містить один активний біт, не враховуючи старший.

Висновки

Таким чином, запропоновано три методи пошуку диференційних характеристик циклової функції блокового шифру «Кипарис»: прямий метод пошуку, метод пошуку «у двох напрямках» та оптимізований метод пошуку диференційної характеристики з високою ймовірністю. Метою всіх трьох підходів є активізація найменшої кількості біт на входах суматорів циклової функції, що, в свою чергу, збільшує ймовірність заданого перетворення. Останній із запропонованих методів дозволив знайти диференційну характеристику на циклову функцію блокового шифру «Кипарис» з ймовірністю, що дорівнює ¼.

Список літератури: 1. *Mouha, Nicky*. The Design Space of Lightweight Cryptography [Text] / Nicky Mouha // NIST Lightweight Cryptography Workshop 2015. – 2015. – 19 p. 2. *Beaulieu R. et al*. The SIMON and SPECK lightweight block ciphers // Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE // IEEE, 2015. – С. 1-6. 3. *Bernstein D. J*. The Salsa20 family of stream ciphers Salsa. – 2007. 4. *Bernstein D. J*. ChaCha, a Variant of Salsa // Workshop Record of SASC: The State of the Art of Stream Ciphers. 6. *Родінко М.Ю., Олійников Р.В*. Постквантовий малоресурсний симетричний блоковий шифр «Кипарис» // Радіотехніка. – 2017. – Вип. 189. – С. 100-107. 7. *Biham, E*. Differential Cryptanalysis of DES-like Cryptosystem / E. Biham, A. Shamir // Journal of Cryptology. – 1991. – Vol. 4. – P. 3-72. 8. *Biryukov A., Velichkov V*. Automatic Search for Differential Trails in ARX Ciphers //CT-RSA. – 2014. – Т. 8366. – С. 227-250. 9. *Mouha N. et al*. The Differential Analysis of S-Functions // Selected Areas in Cryptography. – 2010. – V. 6544. – P. 36-56.

Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 12.11.2017