УДК 004.056.55:519.2

ДОКАЗОВА СТІЙКІСТЬ АЛГОРИТМУ ШИФРУВАННЯ “КУЗНЄЧІК” ДО ДИФЕРЕНЦІАЛЬНОГО ТА ЛІНІЙНОГО КРИПТОАНАЛІЗУ

С. В. Яковлєв[1, a]

[1] *Національний технічний університет України «Київський політехнічний інститут»*

Анотація

В роботі наводяться аналітичні оцінки верхніх меж імовірностей двораундових диференціалів та лінійних потенціалів алгоритму шифрування “Кузнєчік”, який висувається на заміну алгоритму ГОСТ 28147-89 в якості національного стандарту шифрування Російської Федерації.

Ключові слова: симетрична криптографія, SP-мережі, диференціальний криптоаналіз, лінійний криптоаналіз, шифр “Кузнєчік”, “Kuznyechik”

Вступ

Алгоритм ГОСТ 28147-89 протягом останніх 25 років виступав міждержавним стандартом шифрування Росії, України та ряду інших країн. Хоча на цей шифр й досі не побудовано жодної практичної атаки, багато дослідників вказували на його конструктивні слабкості, до яких відносили малий розмір блоку, використання циклічного зсуву, що має слабкі властивості розсіювання, дуже просту схему виробки раундових ключів тощо.

У 2012 році для заміни національного стандарту Центром захисту інформації та спеціального зв’язку ФСБ Росії був розроблений новий алгоритм шифрування, який одержав назву “Кузнєчік” [1, 2]. Цей алгоритм побудовано із урахуванням критики на адресу ГОСТ 28147-89 та новітніх тенденцій в галузі синтезу блочних шифрів. Однак у відкритій літературі майже відсутні публікації щодо аналізу стійкості даного алгоритму.

В даній роботі ми наведемо аналітичні оцінки верхніх меж імовіностей двораундових диференціалів та лінійних потенціалів шифру "Кузнєчік". Ці величини визначають теоретичну (доказову) стійкість шифрів до диференціального та лінійного криптоаналізу – двох потужних сучасних методів аналізу блочних шифрів.

1. Опис шифру “Кузнєчік”

Алгоритм шифрування “Кузнєчік” [2] перетворює 128-бітні вхідні повідомлення у 128-бітні шифртексти за допомогою ключа довжиною 256 біт, який розгортується у десять раундових підключів. Схема шифру має вигляд класичної SP-мережі; перші дев’ять раундів мають вигляд $F(x,k) = L(S(x \oplus k))$, де S – шар нелінійної заміни, L – лінійне (відносно операції $\oplus$) перетворення. На останньому, десятому раунді відбувається лише побітове додавання із раундовим ключем.

Шар нелінійної заміни складається з шістнадцяти однакових 8-бітних S-блоків π, які зафіксовані у специфікації шифру. Лінійне перетворення L побудовано на основі регістру зсуву із лінійним зворотним зв’язком над полем $GF(2^8)$; це дозволило одержати перетворення, яке не тільки має гарні властивості з точки зору криптографії (зокрема, максимально можливий індекс розгалуження $B = B(L) = 17$), але й ефективно реалізується на сучасних обчислювальних архітектурах.

Надалі ми робимо стандартне припущення, що раундові підключі шифру “Кузнєчік” є незалежними та рівномірно розподіленими.

2. Оцінки стійкості шифру “Кузнєчік”

Нагадаймо, що *імовірністю диференціала* (α, β) безключового перетворення $s(x)$ називається величина

$$DP^s(\alpha,\beta) = 2^{-n} \sum_x [s(x \oplus \alpha) \oplus s(x) = \beta],$$

а *імовірністю диференціала* (α, β) *в точці* x ключезалежного перетворення $f_k(x)$ із множиною ключів K – величина

$$DP^{f_k}(x;\alpha,\beta) = 2^{-|K|} \sum_{k \in K} [f_k(x \oplus \alpha) \oplus f_k(x) = \beta],$$

де через квадратні дужки позначено *дужки Айверсона*, які дорівнюють 1, якщо записане в них твердження істинне, та 0, якщо хибне. Аналогічно визначаються *лінійні потенціали* (α, β) перетворень $s(x)$ та $f_k(x)$:

$$LP^s(\alpha,\beta) = \left(2^{-n} \sum_x (-1)^{x\cdot\alpha \oplus s(x)\cdot\beta}\right)^2,$$

$$LP^{f_k}(\alpha,\beta) = 2^{-|K|} \sum_{k \in K} \left(2^{-n} \cdot \sum_x (-1)^{x\cdot\alpha \oplus f_k(x)\cdot\beta}\right)^2.$$

[a] yasv@rl.kiev.ua

Максимуми

$$MDP(f_k) = \max_{x,\alpha\neq 0,\beta} DP^{f_k}(x;\alpha,\beta),$$

$$MLP(f_k) = \max_{\alpha,\beta\neq 0} LP^{f_k}(\alpha,\beta)$$

визначають стійкість перетворення f_k до диференціального та лінійного криптоаналізу.

Оскільки шифр "Кузнєчік" відноситься до класу марковських шифрів, до нього застосовна існуюча теорія диференціального та лінійного криптоаналізу. Зокрема, відомо [3], що імовірності диференціалів двораундової SP-мережі E задовольняють такій нерівності:

$$MDP(E) \leqslant p^{B-1},$$

де $p = MDP(\pi)$ – максимум імовірності одного S-блоку, B – індекс розгалуження лінійного перетворення L. В роботі [4] дану оцінку було підсилено; зокрема, було показано, що $MDP(E) \leqslant QD(\pi, B)$, де

$$QD(\pi,B) = \max\Big\{\max_{\alpha\neq 0}\sum_{\gamma}\left(DP^{\pi}(\alpha,\gamma)\right)^{B},\ \max_{\beta\neq 0}\sum_{\gamma}\left(DP^{\pi}(\gamma,\beta)\right)^{B}\Big\}.$$

Ще більш точна оцінка наводиться в роботі [5], де показано, що якщо перетворення L має матричне представлення над полем $GF(2^t)$, де t – розмір S-блоку (для шифра "Кузнєчік" $t = 8$), то $MDP(E) \leqslant QD^*(\pi, B)$, де

$$QD^*(\pi,B) = \max_{1\leqslant u\leqslant B-1}\ \max_{\mu\in GF(2^t)} QD_u(\pi,B,\mu),$$

$$QD_u(\pi,B,\mu) = \max_{\alpha,\beta,\lambda\in GF^*(2^t)}\sum_{\gamma}\left(DP^{\pi}(\alpha,\gamma)\right)^{u}\times \left(DP^{\pi}(\lambda\cdot\gamma\oplus\mu,\beta)\right)^{B-u}.$$

Аналогічно (із заміною імовірностей диференціалів на лінійні потенціали) визначаються параметри $q = MLP(\pi)$, $QL(\pi, B)$ та $QL^*(\pi, B)$, через які оцінюється стійкість SP-мереж до лінійного криптоаналізу. Також потрібно зауважити, що із збільшенням кількості раундів наведені оцінки не погіршуються.

Нами було обчислено параметри p, q, QD, QL та QD^* для S-блоку π шифра "Кузнєчік". Обчислення параметру QL^* зіткнулось із суто технічними труднощами: якщо обчислення QD^* зайняло приблизно 8 годин на персональному комп'ютері із процесором AMD Athlon^{tm} II X4 640 3GHz під орудою ОС Windows 7, то обчислення QL^* на тому ж комп'ютері займе приблизно 480 годин. На жаль, у автора наразі немає таких обчислювальних потужностей. Очікується, що QL^* буде менша за QL приблизно на порядок. Результати обчислень подано нижче.

1) $p = 2^{-5}$, звідки $p^{B-1} = 2^{(-5)\cdot 16} = 2^{-80}$.
   $q = \frac{3136}{2^{16}} \approx 2^{-4.385}$, звідки $q^{B-1} \approx 2^{-70.16}$.
2) $QD(\pi, 17) \approx 2^{-83.978}$, $QL(\pi, 17) \approx 2^{-73.546}$.
3) $QD^*(\pi, 17) \approx 2^{-84.18}$.

З наведених результатів випливає, що складність проведення диференціального криптоаналізу шифру "Кузнєчік" вимагатиме щонайменше 2^{84} операцій, а складність проведення лінійного криптоаналізу – щонайменше 2^{73} операцій, що робить цей шифр доказово стійким до даних видів криптоаналізу.

Висновки

В даній роботі було досліджено стійкість до диференціального та лінійного криптонаалізу нового алгоритму шифрування "Кузнєчік", який пропонується на заміну існуючого національного стандарту шифрування Російської Федерації. Показано, що складність проведення диференціального криптоаналізу складатиме щонайменше 2^{84} операцій, а складність проведення лінійного криптоаналізу – щонайменше 2^{73} операцій. Таким чином, можна вважати алгоритм шифрування "Кузнєчік" стійким до зазначених методів криптоаналізу.

Перелік використаних джерел

1. Shishkin, V. Low-Weight and Hi-End: Draft Russian Encryption Standard. / V. Shishkin, D. Dygin, I. Lavrikov, G. Marshalko, V. Rudskoy, and D. Trifonov // Current Trends in Cryptology (Moscow, 2014). — 2014. — pp. 183—188.
2. Информационная технология. Криптографическая защита информации. Блочные шифры (проект) [електронний ресурс] — Режим доступу: http://www.tc26.ru/standard/draft/GOST-R-bch.pdf
3. Kang J.-S. Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks. / J.-S. Kang, S. Hong, S. Lee, O. Yi, C. Park, J. Lim // ETRI Journal. — #23. — 2001. — pp. 158–167.
4. Park S. Improving the upper bound on the maximum differential and the maximum linear hull probability for the SPN structures and AES. / S. Park, J. Sung, S. Lee, J. Lim // Fast Software Encryption. — FSE'03, Proceedings. — Springer Verlag, 2003. — pp. 247—260.
5. Canteaut A. On the behaviors of affine equivalent S-boxes regarding differential and linear attacks [електронний ресурс] / A. Canteaut, J. Roue // Режим доступу: http://eprint.iacr.org/2015/085.pdf