

ОЦІНКА СТІЙКОСТІ МОДИФІКОВАНОГО ШИФРУ ГОСТ Р 34.12-2015 ДО ЦІЛОЧИСЕЛЬНОГО РІЗНИЦЕВОГО КРИПТОАНАЛІЗУ

Д. М. Поречна¹

¹ Національний технічний університет України «Київський політехнічний інститут»

Анотація

В роботі наводяться аналітичні результати, які дозволили оцінити практичну стійкість відносно цілочисельного різницевого криптоаналізу модифікованого алгоритму «Кузнечік», затвердженого у якості національного стандарту шифрування ГОСТ Р 34.12-2015 Російської Федерації.

Ключові слова: симетрична криптографія, блочні шифри, диференціальний криптоаналіз, шифр «Кузнечік», «Kuznyechik»

Вступ

У 2012 році Центром захисту інформації та спеціального зв'язку ФСБ Росії був розроблений новий алгоритм шифрування, який одержав назву «Кузнечік» [1]. Він затверджений у якості стандарту ГОСТ Р 34.12-2015 [2] і вступив у чинність з 1 січня 2016 року.

В даній роботі наведено аналітичні оцінки практичної стійкості Кузнечік-подібних алгоритмів до потужного сучасного методу аналізу блочних шифрів – цілочисельного різницевого криптоаналізу.

У роботах, в яких розглядалися немарковські та узагальнено марковські блокові шифри будувались оцінки практичної стійкості лише відносно класичного, тобто побітового різницевого криптоаналізу. Питання побудови оцінок стійкості до цілочисельного різницевого криптоаналізу там не розглядалось. Основні означення, що стосуються марковських та узагальнено марковських блокових алгоритмів можна знайти в [3] та [4].

1. Побудова оцінок практичної стійкості Кузнечік-подібних алгоритмів

Введемо необхідні позначення. Лінійний (над кільцем Z_{2^u}) оператор $A : (V_u)^p \rightarrow (V_u)^p$ задамо за допомогою матриці $A = (a_{ij})_{i,j=1}^p$, $a_{ij} \in V_u$, де для будь-якого $x = (x^{(p)}, \dots, x^{(1)}) \in V_n : Ax^T = y^T = (y^{(p)}, \dots, y^{(1)})^T$, $y^{(i)} = \sum_{j=1}^p a_{ij}x^{(j)}$, а операції множення та додавання виконуються у кільці Z_{2^u} .

Позначимо $A_i = (a_{ip}, \dots, a_{i1})$. Тоді, в наших позначеннях $y^{(i)} = A_i x^T$, тобто

$$Ax^T = (A_p x^T, \dots, A_1 x^T)^T,$$

де під скалярним множенням розуміємо множення векторів з $(Z_{2^u})^p$.

Аналогічно позначимо для оберненого оператора $A^{-1} = (A'_p, \dots, A'_1)$, де A'_i , $i = \overline{1, p}$ – рядки матриці A^{-1} (також пронумеровані у зворотному порядку, відповідно до нумерації координат вектора x). Тоді $A^{-1}x^T = (A'_p x^T, \dots, A'_1 x^T)^T$.

Надалі розглядається лише такий оператор A , що $wt(A'_j) \leq l$, $j = \overline{1, p}$.

1.1. Опис модифікованих Кузнечік-подібних алгоритмів

Означення 1. В наших позначеннях будемо називати блоковий алгоритм шифрування *модифікованим Кузнечік-подібним алгоритмом*, якщо його раундова функція має вигляд:

$$f_k(x) = A \cdot S(x * k), \quad (1)$$

де $x \in V_n$ – відкритий текст, $n = pu$, $p \geq 2$, $x = (x_p, \dots, x_1)$, $x_i : V_u \rightarrow V_u$, $i = \overline{1, p}$, $k \in V_n$ – раундовий ключ, $*$ – операція побітового або модульного додавання, $S : V_n \rightarrow V_n$ – блок підстановки такий, що $S = (s^{(p)}, \dots, s^{(1)})$, $s^{(i)} : V_u \rightarrow V_u$.

Модифікований зазначеним чином Кузнечік-подібний алгоритм може містити:

- 1) побітовий ключовий суматор;
- 2) модульний ключовий суматор;
- 3) операції модульного та побітового додавання по чергово, в залежності від раунду.

Операція в ключовому суматорі і буде визначати властивості такого алгоритму.

Наступне твердження визначає для зазначених модифікованих Кузнечік-подібних алгоритмів чи є вони марковськими.

Твердження 1. В залежності від ключового суматора модифікований Кузнечік-подібний алгоритм з раундовою функцією (1) та ключовим суматором згідно 1)-3) буде:

- 1) марковським відносно операції побітового додавання та узагальнено марковським відносно операції модульного додавання;
- 2) марковським відносно операції модульного додавання + та узагальнено марковським відносно операції побітового додавання;
- 3) узагальнено марковським відносно і модульного і побітового додавання.

Наслідок 1. Для модифікованого Кузнечік-подібного алгоритму з модульним ключовим суматором, справедлива оцінка практичної стійкості:

$$EDP(\Omega) = \prod_{i=0}^{r-1} d_+^f(\omega_i, \omega_{i+1})$$

1.2. Допоміжні результати

Отримані в [5] наукові результати дозволяють запропонувати метод оцінювання стійкості раундових функцій SPN-шифрів, а також побудувати оцінки практичної стійкості модифікованих Кузнечік-подібних алгоритмів відносно цілочисельного різницевого криптоаналізу. Наведемо основні результати.

Для кожного $i = \overline{1, p}$ покладемо

$$\Delta_{\oplus+}^{(i)} = \max_{\alpha, \gamma \in V_u \setminus \{0\}} \frac{1}{2^u} \sum_{k \in V_u} \sum_{z=0}^{l+1} \delta(S^i(k \oplus \alpha) - S^i(k), \gamma + z)$$

по всіх $\alpha, \gamma \in V_u \setminus \{0\}$ та

$$\Delta_{\oplus+} = \max \left\{ \Delta_{\oplus+}^{(i)}, i = \overline{1, p} \right\}$$

Для раундової функції вигляду $f_k(x) = A \cdot S(x \oplus k)$ справедлива наступна нерівність:

$$\forall \alpha, \gamma \in V_u \setminus \{0\} \quad d_+^G \leq \Delta_{\oplus+}$$

1.3. Формальний опис методу оцінювання

Вхідними даними для застосування методу є алгоритм блокового шифрування з відомим раундовим перетворенням, яке є композицією ключового суматора, блоку підстановок з $n = pu$, $p \leq 2$, $s^{(i)} : V_u \rightarrow V_u$, $i = \overline{1, p}$ та лінійного (над деяким кільцем) оператора, обернений до якого містить не більше l одиниць. Вихідними даними є значення верхніх оцінок імовірностей цілочисельних диференціалів $\gamma' \in (0; 1)$ відповідного перетворення.

Алгоритм 1 (для ключового суматора за модулем 2):

- 1) Для кожного $s^{(i)}$, $i = \overline{1, p}$ окремо, обчислити для всіх можливих значень $\alpha, \gamma \in V_u$:

$$2^{-u} \sum_{k \in V_u} \sum_{z=0}^{l+1} \delta(S^i(k \oplus \alpha) - S^i(k), \gamma + z).$$

- 2) Серед знайдених значень обрати найбільше значення $\Delta_{\oplus+}^{(i)}$ для кожного $s^{(i)}$, $i = \overline{1, p}$.
- 3) Обчислити $\gamma' = \Delta_{\oplus+} = \max \left\{ \Delta_{\oplus+}^{(i)}, i = \overline{1, p} \right\}$.

Вихід алгоритму: значення верхніх оцінок імовірностей цілочисельних диференціалів відповідної раундової функції. Зауважимо, що час роботи алгоритму для довжини входу k (розмір одного s-блоку) становить $O(lp k^3 \log k)$ бітових операцій.

1.4. Результати

Використовуючи для вищенаведеного алгоритму $l = 8$ та 8-бітових s-блоків (у [2] рекомендовано один s-блок, який позначений π) отримано верхні оцінки імовірностей цілочисельного раундового диференціалу для раундової функції (1):

$$\max_{\alpha, \gamma \in V_n \setminus \{0\}} d_+^f(\omega_i, \omega_{i+1}) \leq 0,08203125,$$

звідки для 10 раундів зашифрування

$$EDP(\Omega) \leq 1,380 \times 10^{-11} \approx 2^{-34}.$$

Висновки

Наведені результати, дозволили оцінити практичну стійкість модифікованих «Кузнечік»-подібних алгоритмів блокового шифрування відносно цілочисельного різницевого криптоаналізу. При цьому середня імовірність різницевої характеристики буде залежати як від кількості раундів, так і від властивостей блока підстановки і наявності додаткових перетворень в раунді. Надалі буде проведено пошук таких вузлів заміни, які б відповідали найменшим значенням параметрів та забезпечували більшу стійкість Кузнечік – подібних алгоритмів відносно цілочисельного різницевого криптоаналізу.

Перелік використаних джерел

1. Low-Weight and Hi-End: Draft Russian Encryption Standard. / V. Shishkin, D. Dygin, I. Lavrikov et al. // Current Trends in Cryptology. — 2014. — P. 183–188.
2. Информационная технология. Криптографическая защита информации. Блочные шифры (проект). — 2015. — URL: http://www.tc26.ru/standard/gost/GOST_R_3412-2015.pdf.
3. Ковальчук Л. В., Пальченко С. В., Скрипник Л.В. Застосування теорії узагальнених марковських шифрів для оцінювання стійкості сучасних блокових алгоритмів до методів різницевого криптоаналізу // Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». — 2015. — Т. 2, № 16.
4. Lai X., Massey J.L., Murphy S. Markov ciphers and differential cryptanalysis // Advances in Cryptology – EUROCRYPT'91, Proceedings. – Springer Verlag. — 1991. — P. 17–38.
5. Ковальчук Л.В., Кучинська Н.В., Скрипник Л.В. Побудова верхніх оцінок середніх імовірностей цілочисельних диференціалів композицій ключового суматора, блока підстановки та лінійного (над деяким кільцем) оператора // Збірник наукових праць Спеціальні телекомунікаційні системи та захист інформації. — 2015. — Т. 1, № 29. — С. 33–45.