2. Шор Н. З. Методы минимизации недифференцируемых функций и их применение. К.: Наук. думка, 1979. 208 с.
3. Журбенко Н. Г.Об одной модификации *r*-алгоритма. Материалы III Международной конференции *Математическое моделирование, оптимизация и информационные технологии*. Кишинеу: Эврика, 2012. С. 355–361.
4. Журбенко Н. Г., Чумаков Б. М. Программное управление коэффициентами растяжения *r*-алгоритма. *Теорія оптимальних рішень*. Київ: Ін-т кібернетики ім. В. М. Глушкова НАН України, 2012. С. 113–118.

Is considered the family of minimization algorithms using space dilation operation along the direction of the difference of two successive subgradients. In contrast to r-algorithm, in the proposed modifications the values of dilation coefficients are calculated in the process of algorithm. The algorithms can be used with a constant step size. Is the result of the study of the numerical efficiency of the algorithm considered family.

Key words: *nonsmooth optimization, subgradient, the transformation of the space, numerical efficiency.*

Получено 15.03.2017

УДК 681.3.06:006.354

Л. В. Ковальчук*, д-р техн. наук,
Н. В. Кучинська,** канд. техн. наук

*Інститут СЗР України, м. Київ,
**Національний технічний університет України «КПІ», м. Київ

ОЦІНКИ ПРАКТИЧНОЇ СТІЙКОСТІ МОДИФІКАЦІЙ НОВИХ СТАНДАРТІВ БЛОКОВОГО ШИФРУВАННЯ ВІДНОСНО ЦІЛОЧИСЕЛЬНОГО РІЗНИЦЕВОГО КРИПТОАНАЛІЗУ

Отримані науково обґрунтовані оцінки практичної стійкості до цілочисельного різницевого криптоаналізу ГОСТ-подібних та «Калина»-подібних блокових шифрів, проведено статистичний порівняльний аналіз отриманих значень з відповідними параметрами для випадкових вузлів заміни.

Ключові слова: *різницевий, диференціальний криптоаналіз, блокові шифри, стійкість, s-блоки, вузли заміни.*

Вступ. Сьогодні симетричні блокові алгоритми шифрування є основним криптографічним засобом забезпечення конфіденційності при обробці інформації у сучасних інформаційно-телекомунікаційних системах. За останні кілька років у країнах СНД прийнято низку власних стандартів блокових шифрів, а саме СТБ 34.101.31-2011 (Білорусь), ГОСТ Р 34.12 2015 (РФ) та ДСТУ 7624:2014 «Калина» (Україна). Варто зауважити, що в стандарті ГОСТ Р 34.12 2015 визначено

два алгоритми блокового шифрування для довжини блока 128 біт («Кузнєчик») та 64 біт («Магма»). Другий алгоритм є за своєю суттю аналогічним алгоритму, визначеному в ГОСТ 28147-89. Крім того український («Калина») та російський («Кузнєчик») стандарти схожі за своєю будовою. Тому ГОСТ Р 34.12 2015 «Кузнєчик» можна вважати «Калина»-подібним алгоритмом.

Починаючи з 90-х років минулого століття, цілочисельні диференціали використовувались, в перше чергу, для побудови колізій геш-функцій. Пізніше, за останні 5–7 років, з'явились перші роботи, присвячені аналізу стійкості раундових функцій до цілочисельного різницевого криптоаналізу (наприклад, [1–3]). Запропонований у цих роботах підхід може бути застосований для дослідження блокових алгоритмів, які містять додаткове нелінійне перетворення — суматор за модулем 2^{32} або 2^{64}.

1. Побудова оцінок практичної стійкості ГОСТ-подібного алгоритму. Розглянемо $\Im$ — r-раундовий блоковий шифр, який перетворює відкритий текст $x \in V_n$ в шифрований текст $y \in V_n$ при ключі шифрування $k = (k_1, k_2, \ldots, k_r) \in (V_m)^r$ за наступним правилом:

$$y = \Im_k(x) = f_{k_r} \circ f_{k_{r-1}} \circ \cdots \circ f_{k_1}(x), \qquad (1)$$

де $k_i \in V_m$, $i = \overline{1, r}$ — раундові ключі, $f_\lambda(\cdot) : V_n \to V_n$, $\lambda \in V_m$ — раундова функція шифрування.

Означення 1. Будемо називати блоковий алгоритм шифрування (1) *модифікованим ГОСТ-подібним алгоритмом*, якщо його раундова функція має наступний вигляд:

$$f_k(u, v) = (v, u + \varphi(v + k)), \qquad (2)$$

де $x = (u, v) \in V_n$, $n = 2m$, $u, v, k \in V_m$, k — раундовий ключ, $\varphi : V_m \times V_m \to V_m$ — раундове перетворення алгоритму (2), а + є додаванням за модулем 2^m.

Довжина блоку алгоритму визначається як $n = pu$, $p \geq 2$, а блок підстановок — набором: $\forall x \in V_n : S(x) = (s^{(p)}(x^{(p)}), \ldots, s^{(1)}(x^{(1)}))$, $x^{(i)} \in V_u$, $i = \overline{1, p}$, де s-блоки $s^{(i)} : V_u \to V_u$, $i = \overline{1, p}$ — бієктивні відображення. Відображення зсуву вліво t біт вектора з V_m позначено $L_t : V_m \to V_m$. Раундове перетворення $\varphi : V_m \times V_m \to V_m$, яке задано в (2), у введених позначеннях можна представити:

$$\varphi(x, k) = L_t\left(S(x + k)\right). \qquad (3)$$

Справедливим є наступний результат.

Теорема 1. Для модифікованого ГОСТ-подібного алгоритму з r раундами справедлива оцінка практичної стійкості:

$$\max_{\Omega} EDP(\Omega) \le \left(\max_{\alpha,\beta \in V_n \setminus \{0\}} d_{+}^{\varphi}(\alpha,\beta) \right)^{\left\lceil 2r/3 \right\rceil}.$$

Для доведення теореми використовуються отримані в [2, с. 72–73; 3, с. 27] наукові результати, які, зокрема, дозволяють оцінити величину $\max\limits_{\alpha,\beta \in V_n \setminus \{0\}} d_{+}^{\varphi}(\alpha,\beta)$ в даному випадку.

В такому випадку, якщо 4-бітові вузли заміни обрані з рекомендованих до використання, але з найменшими значеннями параметрів (dke2 або dke7) оцінкою буде $\max\limits_{\Omega} EDP(\Omega) \le 0{,}0024 \approx 2^{-9}$.

Але таку оцінку можна покращити, якщо обрати вузли заміни з $\max\limits_{\alpha,\beta \in V_n \setminus \{0\}} d^{\varphi}(\omega_i, \omega_{i+1}) \le 2 \cdot 0{,}1875$, тоді

$$\max_{\Omega} EDP(\Omega) \le 1{,}13 \cdot 10^{-9} \approx 2^{-29}.$$

Якщо модифікувати ГОСТ до використання 8-бітових вузлів заміни і обрати їх так, щоб $\max\limits_{\alpha,\beta \in V_n \setminus \{0\}} d^{\varphi}(\omega_i, \omega_{i+1}) \le 2 \cdot 0{,}0195$, то $\max\limits_{\Omega} EDP(\Omega) \le 2{,}58 \cdot 10^{-30} \approx 2^{-98}$.

Побудова оцінок практичної стійкості «Калина»-подібних алгоритмів. Введемо лінійний (над кільцем Z_{2^u}) оператор $A : (V_u)^p \to (V_u)^p$, який задамо за допомогою матриці $A = \left(a_{ij}\right)_{i,j=1}^{p}$, $a_{ij} \in V_u$, де $\forall x = (x^{(p)}, ..., x^{(1)}) \in V_n$: $A\,x^T = y^T = \left(y^{(p)}, ..., y^{(1)}\right)^T$, $y^{(i)} = \sum\limits_{j=1}^{p} a_{ij} x^{(j)}$, а операції множення та додавання виконуються у кільці Z_{2^u}. Позначимо $A_i = \left(a_{ip}, ..., a_{i1}\right)$. Тоді, в наших позначеннях, $y^{(i)} = A_i x^T$, тобто $A\,x^T = \left(A_p x^T, ..., A_1 x^T\right)^T$.

Аналогічно позначимо для оберненого оператора $A^{-1} = \left(A_p^{'}, ..., A_1^{'}\right)$, і $A^{-1} x^T = \left(A_p^{'} x^T, ..., A_1^{'} x^T\right)^T$. Надалі розглядається лише такий оператор A, що $wt\left(A_j^{'}\right) \le l,\ j = \overline{1, p}$.

Означення 2. В наших позначеннях будемо називати блоковий алгоритм шифрування (1) *модифікованим «Калина»-подібним алгоритмом,* якщо його раундова функція має вигляд:

$$f_k(x) = A \circ S(x * k), \tag{4}$$

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

У введених позначеннях для модифікованого раундового перетворення (4) алгоритмів «Калина» та «Кузнєчик» справедливим є наступна теорема, яка встановлює оцінки практичної стійкості алгоритмів відносно цілочисельного різницевого криптоаналізу.

Теорема 2.

1) для модифікованого «Калина»-подібного алгоритму верхні оцінки імовірності узагальненої диференціальної характеристики алгоритму визначаються як:

$$EDP(\Omega) \leq \max_{\alpha,\beta \in V_n \setminus \{0\}} d^f_{+,+}(\alpha, \beta) \cdot (\max_{\alpha,\beta \in V_n \setminus \{0\}} d^f_{\oplus,+}(\alpha, \beta))^{N-1},$$

де N — кількість раундів блокового алгоритму;

2) для модифікованого алгоритму «Кузнєчик» верхні оцінки імовірності узагальненої диференціальної характеристики алгоритму з N раундами за шифрування визначаються як:

$$EDP(\Omega) \leq \max_{\alpha,\beta \in V_n \setminus \{0\}} d^f_{\oplus,+}(\alpha, \beta)^{N-1}.$$

Для доведення теореми використовуються отримані в [1, с. 36–39] наукові результати та дозволяють оцінити величину $\max\limits_{\alpha,\beta \in V_n \setminus \{0\}} d^{\varphi}_{+}(\alpha, \beta)$ в даному випадку.

У такому випадку, якщо вузли заміни обрані з рекомендованих в стандарті ДСТУ7624:2014, тоді $\max\limits_{\alpha,\beta \in V_n \setminus \{0\}} d^f_{\oplus,+}(\alpha, \beta) \leq 0{,}09375$ і $\max\limits_{\alpha,\beta \in V_n \setminus \{0\}} d^f_{+,+}(\alpha, \beta) \leq 0{,}10546875$. Звідки, для 10 раундів зашифрування $EDP(\Omega) \leq 5{,}9 \cdot 10^{-11} \approx 2^{-34}$, для 14 раундів зашифрування, $EDP(\Omega) \leq$ $\leq 4{,}578 \cdot 10^{-15} \approx 2^{-48}$, для 18 раундів зашифрування $EDP(\Omega) \leq$ $\leq 3{,}521 \cdot 10^{-19} \approx 2^{-61}$.

Якщо обрати вузли заміни таким чином, щоб вони відповідали найменшим значенням параметрів $\max\limits_{\alpha,\beta \in V_n \setminus \{0\}} d^f_{\oplus,+}(\alpha, \beta) \leq 0{,}08203125$ і

$\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^f_{+,+}(\alpha,\beta)\le 0{,}08203125$, то для 10 раундів зашифрування отримали б $EDP(\Omega)\le 1{,}38\cdot 10^{-11}\approx 2^{-36}$ для 14 раундів зашифрування $EDP(\Omega)\le 6{,}248\cdot 10^{-16}\approx 2^{-51}$ і для 18 раундів зашифрування $EDP(\Omega)\le 2{,}829\cdot 10^{-20}\approx 2^{-65}$.

Для модифікованого алгоритму (з модульним ключовим сумато-ром), при оптимальному виборі значень параметрів справедлива аналогічна оцінка.

У випадку, якщо використано вузол заміни із стандарту ГОСТ Р 34.12 2015, тоді для модифікованого алгоритму із побітовим додаванням у ключовому суматорі $\max\limits_{\alpha,\beta\in V_n\setminus\{0\}} d^f_{\oplus,+}(\alpha,\beta)\le 0{,}09375$, звід-ки за теоремою 3 для 10 раундів зашифрування (враховуючи, що останній раунд не використовує нелінійну заміну, а лише побітове додавання ключа), отримаємо $EDP(\Omega)\le 3{,}814\cdot 10^{-10}\approx 2^{-31}$.

Висновки. Наведені результати дозволили оцінити практичну стій-кість алгоритмів блокового шифрування визначених ув стандартах Украї-ни та Росії відносно цілочисельного різницевого криптоаналізу. Отри-мано оцінки верхніх меж практичної стійкості модифікованого ГОСТ-подібного алгоритму до цілочисельного різницевого криптоаналізу. Отримано оцінки верхніх меж практичної стійкості модифікованих ал-горитмів «Кузнєчик» та «Калина» до цілочисельного різницевого крип-тоаналізу у двох випадках: коли в ключовому суматорі реалізована опе-рація модульного додавання або побітового додавання. Порівняння отриманих значень зі статистичними розподілами цих параметрів дає привід припускати, що при проектуванні шифру «Кузнєчик», окрім стій-кості до класичного побітового різницевого криптоаналізу, могла бути врахована необхідність практичної стійкості і до цілочисельного різни-цевого криптоаналізу. Неможливо стверджувати напевно, чи був такий тип атаки розглянутий авторами шифру при проектуванні його *S*-блоку. Варто зазначити, щодо інших сучасних алгоритмів, стійкість до цілочи-сельного різницевого криптоаналізу не розглядалася ні при побудові шифру AES, ні шифру «Калина». Якщо припущення правильне, то «Ку-знєчик» стає першим алгоритмом шифрування, який би використовував нелінійні вузли заміни за замовчуванням із близькими до практично до-сяжних найменших значень параметрів, тобто тих, що забезпечують йо-му практичну стійкість раундових перетворень до цілочисельного різни-цевого криптоаналізу.

Список використаних джерел:

1. Ковальчук Л. В., Кучинська Н. В., Скрипник Л. В. Побудова верхніх оці-нок середніх імовірностей цілочисельних диференціалів композицій клю-

чового суматора, блока підстановки та лінійного (над деяким кільцем) оператора. Науково-технічний збірник «*Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*». 2015. № 1 (29). С. 33–45.
2. Ковальчук Л. В., Кучинська Н. В. Построение верхних оценок средних вероятностей целочисленных дифференциалов раундовых функций блочных шифров определенной структуры. *Кибернетика и системный анализ.* 2012. № 5. С. 71–81.
3. Кучинская Н. В., Скрипник Л. В. Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и произвольного оператора циклического сдвига *Спеціальні телекомунікаційні системи та захист інформації*. 2013. Вип. 2(24). С. 26–32.

Practical estimates are obtained for cryptographic security of GOST-like and Kalyna-like block cipher statistical comparative analysis is conducted of the relevant parameters values for random nodes replacement.

Key words: *difference, differential cryptanalysis, block ciphers, s-blocks.*

Одержано 28.02.2017

УДК 519.8

И. В. Козин, д-р физ.-мат. наук, профессор,
С. Е. Батовский, аспирант,
В. И. Сардак, аспирантка

Запорожский национальный университет, г. Запорожье

ФРАГМЕНТАРНАЯ МОДЕЛЬ И ЭВОЛЮЦИОННЫЙ АЛГОРИТМ 2D УПАКОВКИ ОБЪЕКТОВ

Рассмотрена задача двумерной упаковки в прямоугольник объектов сложной формы. Показано, что задача упаковки имеет фрагментарную структуру. Для поиска приближенного решения задачи предложена модификация эволюционного алгоритма на перестановках с геометрическим оператором кроссовера. Приводятся результаты численного эксперимента.

Ключевые слова: *фрагментарная модель, задача размещения, 2d-упаковка, эволюционный алгоритм, геометрический кроссовер*

Введение. Задача плоского размещения или двумерной упаковки возникает в многочисленных инженерных и экономических приложениях. Решение проблемы упаковки требуется для таких отраслей, как транспорт, обработка дерева, стекла, кожи, при поиске оптимальных размещений механических и электромеханических узлов агрегатов, при загрузке автомобилей, железнодорожных платформ,