2 Забезпечення комп'ютерної безпеки в інформаційних системах

Людмила Ковальчук, Наталія Кучинська, Леонід Скрипник
ІСЗЗІ НТУУ "КПІ"

УДК 621.391:519.2:519.7

ПОБУДОВА ВЕРХНІХ ОЦІНОК СЕРЕДНІХ ІМОВІРНОСТЕЙ ЦІЛОЧИСЕЛЬНИХ ДИФЕРЕНЦІАЛІВ КОМПОЗИЦІЙ КЛЮЧОВОГО СУМАТОРА, БЛОКУ ПІДСТАНОВКИ ТА ЛІНІЙНОГО (НАД ДЕЯКИМ КІЛЬЦЕМ) ОПЕРАТОРА

Анотація: **Отримані верхні оцінки середніх імовірностей цілочисельних диференціалів для раундових функцій у випадку нетривіального блока підстановки та лінійного (над деяким кільцем) оператора.**
Summary: **The upper bounds are obtained of the integer differentials average probabilities for round functions in the case of a nontrivial block permutations and a linear (over some ring) operator.**
Ключові слова: **Різницевий криптоаналіз, диференціальний криптоаналіз, блокові шифри, раундові функції, s-блоки.**

I Вступ

Більшість сучасних блокових шифрів (AES [1], ГОСТ 28147 [2], "Калина" [3], "Мухомор" [4]) містять у своїй структурі композицію ключового суматора, блока підстановки та лінійного (над деяким кільцем, здебільшого над полем F_2 або його розширенням) оператора. Тому задача оцінювання стійкості таких шифрів до лінійного, білінійного та різних модифікацій різницевого криптоаналізу [5 – 10] або зводиться до задачі побудови верхніх оцінок середніх імовірностей таких композицій, або містить її як підзадачу. Остання повністю розв'язана у наступних випадках:

- якщо у ключовому суматорі реалізована операція побітового додавання, і вхідні та вихідні різниці у раундовому диференціалі розглядаються відносно цієї ж операції (див. бібліографію, наведену у роботах [5, 7]);

- якщо у ключовому суматорі реалізована операція додавання за модулем 2^n, а вхідні та вихідні різниці у раундовому диференціалі розглядаються відносно операції побітового додавання [5 – 10];

- якщо у ключовому суматорі реалізована операція додавання за модулем 2^n, вхідні та вихідні різниці у раундовому диференціалі розглядаються відносно цієї ж операції (такий диференціал називають цілочисельним [11, 12]), і при цьому або відсутній лінійний оператор [6], або відсутній блок підстановки і лінійний оператор є оператором циклічного зсуву [13];

- якщо у ключовому суматорі реалізована операція побітового додавання або додавання за модулем 2^n, вхідні та вихідні різниці у раундовому диференціалі розглядаються відносно цієї ж операції, блок підстановки є довільним, а лінійний оператор є довільним оператором циклічного зсуву [14 – 17];

- якщо у ключовому суматорі реалізована операція побітового додавання або додавання за модулем 2^n, вхідні та вихідні різниці у раундовому диференціалі розглядаються відносно цієї ж операції, блок підстановки є довільним, а лінійний оператор описується матрицею, обернена до якої містить не більше двох ненульових елементів у кожному рядку [18].

Однак питання про побудову верхніх оцінок середніх імовірностей цілочисельних раундових диференціалів залишається відкритим у випадку нетривіального блока підстановки та довільного лінійного оператора. Зауважимо, що аналітичні складності, які виникають у цьому випадку внаслідок наявності біта переносу у вхідній та вихідній різниці, підсилюються тим, що оператор перестановки не є лінійним відносно цілочисельного додавання. У даній роботі буде розглянуто випадок, коли у ключовому суматорі реалізована або операція побітового додавання, або операція додавання за модулем 2^n, блок підстановки є довільним, а лінійний оператор описується матрицею, обернена до якої містить лише нулі та одиниці.

Вперше використання цілочисельних диференціалів було запропоновано у роботі [13], для побудови високоімовірних різницевих характеристик геш-функції MD5. Дана ідея отримала подальший розвиток у

багатьох наступних роботах (див. [11, 12] та бібліографію в них). Такий вибір операції автори робіт обумовлюють тим, що геш-функція MD5 містить багато перетворень, що є лінійними або близькими до лінійних відносно модульного додавання. У роботі [13] автору вдалось знайти велику кількість високоімовірних цілочисельних диференціалів (імовірність яких не менша, а в деяких випадках і суттєво більша за $\frac{1}{4}$) для відображень, що є композиціями суматора за модулем 2^n та оператора циклічного зсуву. Суттєвим є той факт, що імовірність таких цілочисельних диференціалів виявилась значно вищою, ніж імовірність класичних побітових.

Цілочисельні диференціали використовувались також як для криптоаналіза блокових шифрів, так і для побудови колізій геш-функцій у багатьох інших роботах, у тому числі і в тих випадках, коли імовірність побітових диференціалів була занадто малою для їх використання. Звідси випливає висновок, що при оцінюванні стійкості блокового алгоритму шифрування (або геш-фіункції) недостатньо розглядати лише класичні (побітові) диференціали. Достатньо повний перелік посилань та обґрунтування вибору саме цілочисельних диференціалів можна знайти у [12].

Дана робота розглядає більш складну композицію перетворень та має альтернативний характер. Її метою є побудова верхніх (а не нижніх) оцінок для середніх імовірностей цілочисельних диференціалів відображень, що є композиціями ключового суматора, блока підстановки та лінійного (над деяким примарним кільцем) оператора, а також визначення параметрів s-блоків, від яких залежать дані оцінки, та умов, що забезпечують якомога менші значення цих оцінок.

II Допоміжні позначення, твердження та їх доведення

Для довільного $n \in N$ позначимо через $V_n = \{0,1\}^n$ множину *n*-вимірних бітових векторів. Тут і надалі векторам з V_n будуть природнім чином поставлені у відповідність цілі числа від 0 до $2^n - 1$, тобто ми будемо ототожнювати вектори з V_n та елементи кільця Z_{2^n}.

Нехай $n = pu, \quad p \geq 2$ (природно також вважати, що $p << 2^u$). Тоді будь-який $x \in V_n$ може бути поданий у вигляді $x = (x^{(p)},...,x^{(1)}), \quad x^{(i)} \in V_u, \quad i = \overline{1,p}$.

На множині V_n введемо наступні операції та відображення. Для довільних $a,b \in V_n$ позначимо через $a+b$ ($a-b$) результат додавання (віднімання) відповідних цілих чисел за модулем 2^n. Аналогічне позначення будемо використовувати і для операцій на множині векторів V_n (з контексту буде зрозуміло, яка саме операція мається на увазі).

Лінійний (над кільцем Z_{2^u}) оператор $A : (V_u)^p \to (V_u)^p$ задамо за допомогою матриці

$$A = (a_{ij})_{i,j=1}^{p}, \; a_{ij} \in V_u,$$

де для будь-якого $x = (x^{(p)},...,x^{(1)}) \in V_n$:

$$A\,x^T = y^T = \left(y^{(p)},...,y^{(1)}\right)^T, \; y^{(i)} = \sum_{j=1}^{p} a_{ij} x^{(j)}, \tag{1}$$

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

$$A\,x^T = \left(A_p x^T,...,A_1 x^T\right)^T, \tag{2}$$

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

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

Для довільного вектора $a \in \left(Z_{2^u}\right)^p$ позначимо вагу Хеммінга цього вектора як $wt(a) = \#\left\{i : a_i \neq 0, i = \overline{1,p}\right\}$.

Для довільних $\beta, \gamma \in V_n$ визначимо наступні підмножини, що залежать від оператора *A*:

$$\Gamma_A(\gamma) = \{\beta \in V_n \mid \exists k \in V_n : A(k+\gamma)^T - A(k)^T = \beta\};$$

$$\Gamma_{A^{-1}}(\beta) = \{\gamma \in V_n \mid \exists k \in V_n : A(k+\gamma)^T - A(k)^T = \beta\}. \quad (3)$$

В наших позначеннях виконується наступна лема.

Лема 1: нехай $a_{ij} \in \{0,1\}, \quad i, j = \overline{1,p}$. Тоді:

1) якщо оператор *A* такий, що $wt\left(A_j\right) \le l, \quad j = \overline{1,p}$, то

$$\Gamma_A(\gamma) \subset \left\{(\beta_p, \beta_{p-1}, ..., \beta_1) \mid \beta_i \in \{A_i\gamma^T - 1, A_i\gamma^T, A_i\gamma^T + 1, ..., A_i\gamma^T + l\}, i = \overline{1,p}\right\};$$

2) якщо оператор *A* такий, що $wt\left(A'_j\right) \le l, \quad j = \overline{1,p}$, то

$$\Gamma_{A^{-1}}(\beta) \subset \left\{(\gamma_p, \gamma_{p-1}, ..., \gamma_1), \mid \gamma_i \in \{A'_i\beta^T - 1, A'_i\beta^T, A'_i\beta^T + 1, ..., A'_i\beta^T + l\}, i = \overline{1,p}\right\}.$$

Доведення: нехай $\gamma, k \in V_n = \left(V_u\right)^p$.

Розглянемо різницю

$$A\left(k+\gamma\right)^T - A\left(k\right)^T = A\left(k_p + \gamma_p + \nu_p, ..., k_2 + \gamma_2 + \nu_2, k_1 + \gamma_1 + \nu_1\right)^T - A\left(k_p, ..., k_1\right)^T,$$

де

$$\nu_i = \begin{cases} 1, & \text{якщо} \quad k_{i-1} + \gamma_{i-1} + \nu_{i-1} \ge 2^u, i \ge 2; \\ 0, & \text{інакше} \end{cases}$$

(вважаємо, що $\nu_1 = 0$). Зауважимо, що операції у цьому виразі виконуються за модулями 2^n (віднімання) та 2^u (додавання), залежно від того, якому векторному простору належать аргументи.

Враховуючи (2), дана різниця буде дорівнювати $\left(\beta_p, ..., \beta_1\right)$, де

$$\beta_i = A_i \cdot \left(k_p + \gamma_p + \nu_p, ..., k_1 + \gamma_1 + \nu_1\right)^T - A_i \cdot \left(k_p, ..., k_1\right)^T - \mu_i,$$

та

$$\mu_i = \begin{cases} 1, & \text{якщо} \quad A_{i-1} \cdot \left(k_p + \gamma_p + \nu_p, ..., k_1 + \gamma_1 + \nu_1\right)^T - \mu_{i-1} < A_{i-1} \cdot \left(k_p, ..., k_1\right)^T, \\ 0, & \text{інакше} \end{cases}$$

(вважаємо, що $\mu_1 = 0$).

Внаслідок лінійності скалярного множення над кільцем

$$\beta_i = A_i \cdot \left(\gamma_p, ..., \gamma_1\right)^T + A_i \cdot \left(\nu_p, ..., \nu_1\right)^T - \mu_i, \quad (4)$$

звідки, з урахуванням умови $wt\left(A_j\right) \le l, \quad j = \overline{1,p}$, а також того, що $l \le p < 2^u$, випливає

$$A_i \cdot \left(\nu_p, ..., \nu_1\right) \in \{0,1,...,l\},$$

звідки

$$A_i \cdot \left(\nu_p, ..., \nu_1\right) - \mu_i \in \{-1,0,1,...,l\},$$

а, отже,

$$\beta_l \in \{A_i\gamma^T - 1, A_i\gamma^T, A_i\gamma^T + 1, ..., A_i\gamma^T + l\}, i = \overline{1,p},$$

і перший пункт леми доведено.

Для доведення другого пункту леми зазначимо, що

$$A\left(k+\gamma\right)^T - A\left(k\right)^T = \beta^T \Leftrightarrow A^{-1}\left(\beta^T + A\left(k\right)^T\right)^T - A^{-1}\left(A\left(k^T\right)^T\right) = \gamma^T,$$

і далі застосуємо твердження пункту першого леми до оператора A^{-1}.

Лему доведено.

III Верхні оцінки середніх імовірностей цілочисельних диференціалів для випадку модульного суматора

У даному параграфі буде сформульована перша частина основних результатів цього розділу. Нам будуть необхідні наступні позначення. Для довільної функції $F: V_n \times V_n \to V_n$ позначимо $F_k(x) := F(k,x),\ k,x \in V_n$. У цьому параграфі ми будемо розглядати лише такі раундові функції, що є композиціями ключового суматора (модульного), блока підстановки та оператора перестановки:

$$F_k(x) = A\big(S(x+k)\big) \tag{5}$$

Бієктивне відображення $S: V_n \to V_n$ задамо наступним чином:

$$\forall x \in V_n:\ S(x) = (S^{(p)}(x_p),...,S^{(1)}(x_1)),\quad x_i \in V_u,\ i = \overline{1,p},$$

де $S^{(i)}: V_u \to V_u,\quad i = \overline{1,p}$ – бієктивні відображення. Введене нами відображення часто називають блоком підстановки, а відображення $S^{(i)}$ – *s*-блоками.

Згідно з [7, 14, 15], під середньою (за ключами) імовірністю цілочисельного диференціалу (α,β) (де $\alpha,\beta \in V_n$) функції $F: V_n \times V_n \to V_n$ будемо розуміти вираз

$$d_+^F(\alpha,\beta) = 2^{-2n} \sum_{x,k \in V_n} \delta\big(F_k(x+\alpha) - F_k(x), \beta\big). \tag{6}$$

Аналогічно роботам [14 – 16], легко показати, що для функції $F: V_n \times V_n \to V_n$, визначеної згідно з (5), виконується рівність

$$d_+^F(\alpha,\beta) = d_+^F(0;\alpha,\beta),$$

де

$$d_+^F(0;\alpha,\beta) = 2^{-n} \sum_{k \in V_n} \delta\big(F_k(\alpha) - F_k(0), \beta\big) \tag{7}$$

– середня (за ключами) імовірність цілочисельного диференціалу (α,β) функції F у точці *x*=0.

Також для довільних $a,b \in V_u$ та довільного відображення $S: V_u \to V_u$ позначимо

$$\nu(a,b) = \begin{cases} 1, & \text{якщо} \quad a+b \ge 2^u; \\ 0, & \text{інакше;} \end{cases} \tag{8}$$

$$\mu^{(S)}(a,b) = \begin{cases} 1, & \text{якщо} \quad S(a+b) < S(a); \\ 0, & \text{інакше;} \end{cases} \tag{9}$$

$$\text{та}\ \ \mu^{(i)}(a,b) := \mu^{\left(S^{(i-1)}\right)}(a,b). \tag{10}$$

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

$$\Delta_+^{(i)} = \max_{\alpha,\gamma \in V_n \setminus \{0\}} 2^{-u} \sum_{k \in V_u} \left(\sum_{z=0}^{l+1} \delta\big(S^{(i)}(k+\alpha) - S^{(i)}(k), \gamma + z\big) \right), \tag{11}$$

$$\text{та}\ \ \Delta_+ = \max\left\{\Delta_+^{(i)}, i = \overline{1,p}\right\}. \tag{12}$$

У наших позначеннях справедлива наступна теорема.

Теорема 2: нехай функція F визначена за формулою (5). Тоді справедлива наступна нерівність:

$$\forall \alpha,\beta \in V_n \setminus \{0\} \quad d_+^F(\alpha,\beta) \le \Delta_+, \tag{13}$$

або, іншими словами,

$$\max_{\alpha,\beta \in V_n \setminus \{0\}} d_+^F(\alpha,\beta) \le \Delta_+. \tag{14}$$

Доведення: згідно з означенням імовірності цілочисельного диференціала та за формулою (5),

$$d_+^F(\alpha,\beta)=2^{-2n}\sum_{x,k\in V_n}\delta(F_k(x+\alpha)-F_k(x),\beta)=2^{-2n}\sum_{x,k\in V_n}\delta(A(S(x+k+\alpha))-A(S(x+k)),\beta)$$

Після заміни змінної $x+k$ на k отримаємо:

$$d_+^F(\alpha,\beta)=2^{-n}\sum_{k\in V_n}\delta(A(S(k+\alpha))-A(S(k)),\beta)=$$

$$=2^{-n}\sum_{k\in V_n}\Big\{\sum_{\gamma\in V_n}\delta(A(S(k)+\gamma)-A(S(k)),\beta)\times\delta(S(k+\alpha)-S(k),\gamma)\Big\}=$$

$$=2^{-n}\sum_{k\in V_n}\Big\{\sum_{\gamma\in\Gamma_A^{-1}(\beta)}\delta(A(S(k)+\gamma)-A(S(k)),\beta)\times\delta(S(k+\alpha)-S(k),\gamma)\Big\}\le$$

$$\le 2^{-n}\sum_{k\in V_n}\left\{\sum_{\gamma\in\Gamma_A^{-1}(\beta)}\delta(S(k+\alpha)-S(k),\gamma)\right\}=2^{-n}\sum_{k\in V_n}\sum_{\gamma\in\Gamma_A^{-1}(\beta)}\prod_{i=1}^{p}\delta(S^{(i)}(k_i+\alpha_i+\nu_i)-S^{(i)}(k_i)-\mu_i,\gamma_i),\quad(15)$$

де $\nu_i=\nu(k_{i-1},\alpha_{i-1})$, $\mu_i=\mu^{(i)}(k_{i-1},\alpha_{i-1}+\nu_{i-1})$.

Зауважимо, що остання нерівність отримана внаслідок того, що $\delta(A(S(k)+\gamma)-A(S(k)),\beta)\le 1$.

Для довільного $x\in V_n$, $x=(x_p,x_{p-1},...,x_1)$, $x_i\in V_u$, $i=\overline{1,p}$ та для введеного раніше відображення $S:V_n\to V_n$ введемо оператори проектування $P:V_{pu}\to V_{(p-1)u}$ та $\hat{P}:V_{pu}\to V_u$ та позначимо

$$\hat{x}=\hat{P}(x)=x_1\in V_u,$$

$$\widetilde{x}=P(x)=(x_p,x_{p-1},...,x_2)\in V_{n-u};\ \widetilde{S}:V_{n-u}\to V_{n-u},$$

де

$$\forall\widetilde{x}\in V_{n-u}:\ \widetilde{S}(\widetilde{x})=P(S(x))=(S^{(p)}(x_p),...,S^{(2)}(x_2)),\quad x_i\in V_u,\ i=\overline{2,p}.$$

Також для довільного $\beta\in V_n$ позначимо

$$T(\beta)=\{\hat{P}(A_i'\beta^T+z),\ z\in\{-1,0,1,...,l\}\}$$

(тобто $T(\beta)$ – множина перших координат векторів з множини $\Gamma_{A^{-1}}(\beta)$).

Для довільного $\alpha\in V_n$ позначимо $i(\alpha)=\min\{j=\overline{1,p}:\alpha_j\ne 0\}$.

Розглянемо наступні випадки.

Випадок 1. Нехай $i(\alpha)=1$. Тоді $\gamma=(\widetilde{\gamma},\gamma_1)\in\Gamma_{A^{-1}}(\beta)$ та $\gamma_1\in T(\beta)$. Тоді

$$d_+^F(\alpha,\beta)\le 2^{-(n-u)}\sum_{\widetilde{k}\in V_{n-u}}2^{-u}\sum_{k_1\in V_u}\left[\left(\sum_{\widetilde{\gamma}\in P\left(\Gamma_{A^{-1}}(\beta)\right)}\delta(\widetilde{S}(\widetilde{k}+\widetilde{\alpha}+\nu_2)-\widetilde{S}(\widetilde{k})-\mu_2,\widetilde{\gamma})\right)\times\right.$$

$$\left.\times\left(\sum_{\gamma_1\in T(\beta)}\delta(S^{(1)}(k_1+\alpha_1)-S^{(1)}(k_1),\gamma_1)\right)\right].$$

Зазначимо, що для будь-яких $\alpha,\beta\in V_n$ при кожній фіксованій парі $\widetilde{k}\in V_{n-u}$ та $k_1\in V_u$ в сумі

$$\sum_{\widetilde{\gamma}\in P\left(\Gamma_{A^{-1}}(\beta)\right)}\delta(\widetilde{S}(\widetilde{k}+\widetilde{\alpha}+\nu_2)-\widetilde{S}(\widetilde{k})-\mu_2,\widetilde{\gamma})$$

буде не більше одного ненульового доданку, тому ця сума не перевищує одиниці. Звідси

$$d_+^F(\alpha,\beta)\le 2^{-(n-u)}\sum_{\widetilde{k}\in V_{n-u}}2^{-u}\sum_{k_1\in V_u}\left(\sum_{\gamma_1\in T(\beta)}\delta(S^{(1)}(k_1+\alpha_1)-S^{(1)}(k_1),\gamma_1)\right)=$$

$$= 2^{-u} \sum_{k_1 \in V_u} \left(\sum_{\gamma_1 \in T(\beta)} \delta(S^{(1)}(k_1 + \alpha_1) - S^{(1)}(k_1), \gamma_1) \right).$$

Враховуючи позначення (11) та (12), отримаємо: $d_+^F(\alpha,\beta) \le \Delta_+^{(1)} \le \Delta_+$.

Випадок 2. Нехай тепер $1 < i(\alpha) \le p$, тобто

$$\alpha = (\alpha_p, \alpha_{p-1}, ..., \alpha_i, 0, ..., 0), \quad \alpha_j \in V_u, \quad j = \overline{1, p}.$$

Тоді, внаслідок бієктивності відображення $S : V_n \to V_n$, з умови

$$\delta(S(k+\alpha) - S(k), \gamma) \neq 0$$

випливає умова $\gamma_1 = ... = \gamma_{i-1} = 0$, тобто $\gamma = (\gamma_p, ..., \gamma_i, 0, ..., 0)$.

Для введеного раніше відображення $S : V_n \to V_n$ введемо оператор проектування $\widetilde{P} : V_{pu} \to V_{(p-i)u}$ та позначимо $\widetilde{\widetilde{x}} = \widetilde{P}(x) = (x_p, x_{p-1}, ..., x_{i+1}) \in V_{n-iu}$ і, аналогічно до відображення $\widetilde{S}$ у випадку 1 даного доведення, визначимо $\widetilde{\widetilde{S}} : V_{n-u} \to V_{n-u}$. Також для довільного $\beta \in V_n$ позначимо

$$T'(\beta) = \{A_i' \beta^T + z,\ z \in \{-1, 0, 1, ..., l\}\}$$

(тобто $T'(\beta)$ – множина i-тих координат векторів з множини $\Gamma_{A^{-1}}(\beta)$).

Тоді для деякого $\gamma = (\widetilde{\widetilde{\gamma}}, \gamma_i, 0...0) \in \Gamma_{A^{-1}}(\beta)$, згідно з (15),

$$d_+^F(\alpha,\beta) \le 2^{-(n-(i+1)u)} \sum_{\widetilde{\widetilde{k}} \in V_{n-(i+1)u}} 2^{-u} \sum_{k_i \in V_u} \left[\left(\sum_{\widetilde{\widetilde{\gamma}} \in P(\Gamma_{A^{-1}}(\beta))} \delta(\widetilde{\widetilde{S}}(\widetilde{\widetilde{k}} + \widetilde{\alpha} + \nu_{i+1}) - \widetilde{\widetilde{S}}(\widetilde{\widetilde{k}}) - \mu_{i+1}, \widetilde{\widetilde{\gamma}}) \right) \times \right.$$

$$\left. \times \left(\sum_{\gamma_i \in T'(\beta)} \delta(S^{(i)}(k_i + \alpha_i) - S^{(i)}(k_i), \gamma_i) \right) \right].$$

Звідси, з аналогічних до випадку 1 міркувань

$$d_+^F(\alpha,\beta) \le 2^{-u} \sum_{k_i \in V_u} \left(\sum_{\gamma_i \in T'(\beta)} \delta(S^{(i)}(k_i + \alpha_i) - S^{(1)}(k_i), \gamma_i) \right) \le \Delta_+^{(i)}.$$

Отже, в загальному випадку буде справедлива нерівність

$$d_+^F(\alpha,\beta) \le \Delta_+.$$

Теорему доведено.

IV Верхні оцінки середніх імовірностей цілочисельних диференціалів для випадку побітового суматора

У даному роздлі буде сформульована друга частина основних результатів цього розділу. На відміну від розділу 2, тут розглядатимемо лише такі раундові функції, що є композиціями ключового суматора (побітового), блока підстановки та оператора перестановки:

$$G_k(x) = A(S(x \oplus k)). \tag{16}$$

У цьому випадку

$$d_+^G(\alpha,\beta) = 2^{-2n} \sum_{x,k \in V_n} \delta(G_k(x+\alpha) - G_k(x), \beta) = 2^{-2n} \sum_{x,k \in V_n} \delta(G((x+\alpha) \oplus k) - G(x \oplus k), \beta). \tag{17}$$

За лемою 2 роботи [16] для довільного $\beta \in V_n \setminus \{0\}$ виконується нерівність:

$$\max_{\alpha \in V_n \setminus \{0\}} d_+^G(\alpha,\beta) \le \max_{\alpha \in V_n \setminus \{0\}} \sum_{\gamma \in \Gamma_m^{-1}(\beta)} d_{\oplus,+}^S(0;\alpha,\gamma), \tag{18}$$

де

$$d^{S}_{\oplus,+}(0;\alpha,\gamma) = 2^{-n}\sum_{k\in V_n}\delta(S(k\oplus\alpha)-S(k),\gamma).$$

Звідси

$$\max_{\alpha\in V_n\setminus\{0\}} d^{G}_{+}(\alpha,\beta) \le \max_{\alpha\in V_n\setminus\{0\}}\sum_{\gamma\in\Gamma^{-1}_{m}(\beta)} 2^{-n}\sum_{k\in V_n}\delta(S(k\oplus\alpha)-S(k),\gamma),$$

де вираз у правій частині відрізняється від виразу у формулі (15) лише знаком додавання вхідної різниці, а тому його верхню оцінку можна будувати аналогічно до того, як це зроблено у теоремі 2.

Аналогічно формулам (11) та (12), для кожного $l=\overline{1,p}$ покладемо

$$\Delta^{(i)}_{\oplus+} = \max_{\alpha,\gamma\in V_n\setminus\{0\}} 2^{-u}\sum_{k\in V_u}\left(\sum_{z-0}^{l+1}\delta\left(S^{(i)}(k\oplus\alpha)-S^{(i)}(k),\gamma+z\right)\right) \tag{19}$$

та

$$\Delta_{\oplus+} = \max\left\{\Delta^{(i)}_{\oplus+}, i=\overline{1,p}\right\}. \tag{20}$$

У наших позначеннях справедлива наступна теорема.

Теорема 3: нехай функція G визначена за формулою (16). Тоді справедлива наступна нерівність:

$$\forall\alpha,\beta\in V_n\setminus\{0\}\quad d^{G}_{+}(\alpha,\beta)\le\Delta_{\oplus+}, \tag{21}$$

або, іншими словами,

$$\max_{\alpha,\beta\in V_n\setminus\{0\}} d^{G}_{+}(\alpha,\beta)\le\Delta_{\oplus+}. \tag{22}$$

Доведення теореми практично повністю повторює доведення теореми 2, з тією лише відмінністю, що біт переносу між окремими S -блоками у вхідній різниці відсутній.

V Експериментальні результати. Приклади лінійних операторів та статистичний розподіл параметрів s-блоків

У даному розділі наводяться приклади лінійних (над кільцем Z_{2^u}) операторів, що задаються матрицею розмірності $p\times p$, у яких обернена матриця має не більше за l ненульових елементів (одиниць) у рядку. Також наведено розподіл параметрів Δ_{+}, від яких залежать отримані у цьому розділі верхні оцінки імовірностей, для різних значень l.

5.1 Приклади лінійних операторів

Таблиця 1 – Приклади лінійних операторів та їх обернених матриць

l	2^u	A^{-1}	Визначник	A
2	16	1 0 0 0 0 0 1 0 1 1 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 1	Det = 1	01 00 00 00 00 00 15 01 15 01 00 00 00 00 01 15 00 00 01 15 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 15 01 00 00 00 00 00 00 00 00 01 15 00 00 00 00 00 00 00 01
2	16	1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0	Det = –1	01 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 01 00 00 00 00 00 00 01 00 00 15 00 00 00 00 00 00 00 01 00 00 01 00 00 00 15 00 00
2	16	0 1 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0	Det = –1	15 01 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00

		0 0 0 1 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 1 0		00 00 01 01 00 00 15 00 00 00 00 00 00 01 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 15 00 00 00 01 00
2	16	1 1 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0	Det = 1	01 00 00 00 00 00 00 15 00 00 00 00 00 00 00 01 00 01 00 00 00 00 15 00 00 00 00 00 00 00 01 00 00 00 01 00 00 15 00 00 00 00 00 00 00 01 00 00 00 00 00 01 00 00 00 00 00 00 00 00 01 00 00 00
2	16	0 1 1 0 0 0 0 0 1 0 0 0 0 1 0 0 1 0 0 0 0 0 1 0 0 0 0 1 1 0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 1 0 0 0 0 1 0	Det = –1	00 01 00 01 15 00 15 00 00 01 15 01 15 00 15 01 01 15 01 15 01 00 01 15 00 00 00 01 15 00 00 00 00 00 00 00 01 00 00 00 00 00 00 15 01 00 01 00 00 15 01 15 01 00 01 00 00 15 01 15 01 01 01 15
3	16	1 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 1 1 0 0 1 0 0 1 0 0 1	Det = 1	01 01 15 00 01 00 00 15 00 01 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 15 00 01 00 00 00 00 00 00 00 00 01 00 00 00 00 15 00 00 15 01 00 00 15 01 00 15 00 00 01
3	16	0 0 1 0 0 0 0 0 0 1 1 0 0 0 0 0 1 1 1 0 0 0 0 0 0 0 0 1 1 1 0 0 0 0 0 0 0 0 1 1 0 0 0 1 0 0 1 1 0 1 0 0 0 0 1 0 0 0 0 0 0 1 0 0	Det = 1	00 15 01 00 00 00 00 00 15 01 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 15 01 00 00 00 00 00 01 01 15 00 15 00 00 00 00 00 00 00 01 01 15 00 00 00 00 01 00 15 01 00 00 01 00 15 00
3	16	1 1 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 1 0 0 0 0 1 1 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1 1 0 0 0 0 0 0 1 0	Det = 1	01 15 00 00 00 00 00 15 00 01 00 00 00 00 00 00 00 00 00 00 01 15 00 00 00 00 00 00 00 01 00 00 00 00 15 01 00 15 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 01 00 15 00 00 00 00 01 15
3	16	1 0 0 0 0 1 0 0 1 1 0 0 1 0 0 0 0 1 1 0 0 0 1 0 0 0 0 1 0 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 1 0 0 1 0 1 0 1 0	Det = –3	06 11 05 00 00 10 00 11 05 11 06 00 00 11 00 10 00 00 00 15 01 15 00 01 05 11 05 00 01 10 00 11 05 11 05 00 00 11 00 11 11 05 11 00 00 06 00 05 11 05 11 01 15 06 00 05 05 10 06 00 15 12 01 10
4	16	1 0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 0 1 1 0 0 1 1 0 0 0 0 1 0 0 0 0	Det = 1	01 00 00 00 00 00 00 00 00 01 00 15 00 00 00 00 01 15 01 02 00 15 15 00 00 00 00 01 00 00 00 00

		0 0 0 0 1 0 0 0 1 0 0 1 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 1		00 00 00 00 01 00 00 00 15 00 00 15 00 01 00 00 00 00 00 00 00 00 01 00 00 00 00 00 15 00 00 01
4	16	1 0 0 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 0 0 1 0 0 1 0 1 1 0 0 0 1 0 1 1 0 0 0 1 0 0 0 1 0 1 0 1 0 0 1 0 0 1 1 0 1 0 0 0 1 0 0 1 0 0	Det = –3	05 15 11 11 11 11 06 05 05 00 11 11 11 11 05 05 10 15 06 06 05 06 11 11 05 15 11 11 10 12 06 05 05 01 11 10 11 10 05 06 06 01 10 10 11 10 05 06 01 01 15 00 00 15 00 00 06 00 11 11 10 11 05 05
4	16	1 0 0 0 1 1 0 0 1 0 1 1 0 0 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 1 0 0 1 0 1 1 0 0 0 1 0 0 0 0 0 0 1 0 1 1 0 0 1 0 0 1 0 0 1 0 1 1 0	Det = –1	03 01 12 06 01 15 15 14 01 00 14 03 01 00 00 15 01 01 15 02 00 15 00 15 15 00 01 14 00 00 00 01 00 00 01 15 00 00 00 00 14 15 03 11 15 01 01 02 00 00 00 01 00 00 00 00 13 15 04 10 15 02 01 02
4	16	1 0 0 0 0 0 0 0 0 1 1 0 0 1 0 1 0 0 1 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 0 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 0 1 0	Det = 1	01 00 00 00 00 00 00 00 01 01 00 00 15 00 15 00 00 00 01 15 00 00 00 00 00 00 00 01 00 00 00 00 15 15 00 00 01 15 01 01 15 00 15 01 00 00 01 00 00 00 00 15 00 01 00 00 00 00 00 00 01 00 00 00
4	16	1 0 1 0 1 0 0 0 0 1 0 0 0 0 0 1 1 1 0 1 0 0 1 0 0 0 1 0 0 0 0 0 0 0 1 0 1 1 0 0 0 0 1 0 1 0 0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 1 0 1	Det = 3	06 00 00 00 05 05 00 11 11 01 00 00 11 10 00 05 00 00 00 01 00 00 00 00 10 00 01 00 11 11 15 05 11 00 00 15 11 11 00 05 05 00 00 00 06 05 00 11 05 15 00 00 05 06 01 11 05 00 00 00 05 06 00 11
2	256	1 0 0 0 0 0 1 0 1 1 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 1	Det = 1	001 000 000 000 000 000 255 001 255 001 000 000 000 000 001 255 000 000 001 255 000 000 000 000 000 000 000 001 000 000 000 000 000 000 000 000 001 000 000 000 000 000 000 000 255 001 000 000 000 000 000 000 000 000 001 255 000 000 000 000 000 000 000 001
2	256	1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0	Det = –1	001 000 000 000 000 000 000 000 000 000 000 000 000 001 000 000 000 000 001 000 000 000 000 000 000 000 000 000 000 000 000 001 000 000 000 000 001 000 000 000 000 000 000 001 000 000 255 000 000 000 000 000 000 000 001 000 000 001 000 000 000 255 000 000
2	256	0 1 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 1 0 0 0 0 0 1 0 0	Det = –1	255 001 000 000 000 000 000 000 001 000 000 000 000 000 000 000 000 000 001 000 000 000 000 000 000 000 001 001 000 000 255 000 000 000 000 000 000 001 000 000

		0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 1 0		000 000 000 000 001 000 000 000 000 000 000 000 000 000 000 001 000 000 255 000 000 000 001 000
2	256	1 1 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0	Det = 1	001 000 000 000 000 000 000 255 000 000 000 000 000 000 000 001 000 001 000 000 000 000 255 000 000 000 000 000 000 000 001 000 000 000 001 000 000 255 000 000 000 000 000 000 000 001 000 000 000 000 000 001 000 000 000 000 000 000 000 000 001 000 000 000
2	256	0 1 1 0 0 0 0 0 1 0 0 0 0 1 0 0 1 0 0 0 0 0 1 0 0 0 0 1 1 0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 1 0 0 0 0 1 0	Det = –1	000 001 000 001 255 000 255 000 000 001 255 001 255 000 255 001 001 255 001 255 001 000 001 255 000 000 000 001 255 000 000 000 000 000 000 000 001 000 000 000 000 000 000 255 001 000 001 000 000 255 001 255 001 000 001 000 000 255 001 255 001 001 001 255
3	256	1 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 1 1 0 0 1 0 0 1 0 0 1	Det = 1	001 001 255 000 001 000 000 255 000 001 000 000 000 000 000 000 000 000 001 000 000 000 000 000 000 000 000 001 000 000 000 000 000 000 255 000 001 000 000 000 000 000 000 000 000 001 000 000 000 000 255 000 000 255 001 000 000 255 001 000 255 000 000 001
3	256	0 0 1 0 0 0 0 0 0 1 1 0 0 0 0 0 1 1 1 0 0 0 0 0 0 0 0 1 1 1 0 0 0 0 0 0 0 0 1 1 0 0 0 1 0 0 1 1 0 1 0 0 0 0 1 0 0 0 0 0 0 1 0 0	Det = 1	000 255 001 000 000 000 000 000 255 001 000 000 000 000 000 000 001 000 000 000 000 000 000 000 000 000 000 000 255 001 000 000 000 000 000 001 001 255 000 255 000 000 000 000 000 000 000 001 001 255 000 000 000 000 001 000 255 001 000 000 001 000 255 000
3	256	0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 1 1 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 1 0 1 1 0 0 0 0 0 0 0 1 0 0 0 1 0 0 0 1 1 0 0 0 0 0 0 0 1 1	Det = 1	000 000 000 001 000 000 000 000 000 255 001 255 000 000 000 000 000 001 000 000 000 000 000 000 001 000 000 000 000 000 000 000 000 255 000 000 001 255 000 000 000 000 000 000 000 001 000 000 000 001 255 001 000 255 001 000 000 255 001 255 000 001 255 001
3	256	1 1 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 1 0 0 0 0 1 1 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1 1 0 0 0 0 0 0 1 0	Det = 1	001 255 000 000 000 000 000 255 000 001 000 000 000 000 000 000 000 000 000 000 001 255 000 000 000 000 000 000 000 001 000 000 000 000 255 001 000 255 000 000 000 000 001 000 000 000 000 000 000 000 000 000 000 000 000 001 000 255 000 000 000 000 001 255
3	256	1 0 0 0 0 1 0 0 1 1 0 0 1 0 0 0 0 1 1 0 0 0 1 0 0 0 0 1 0 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 1 1 0 0	Det = –3	086 171 085 000 000 170 000 171 085 171 086 000 000 171 000 170 000 000 000 255 001 255 000 001 085 171 085 000 001 170 000 171 085 171 085 000 000 171 000 171 171 085 171 000 000 086 000 085

		1 0 0 1 0 0 0 1 0 0 1 0 1 0 1 0		171 085 171 001 255 086 000 085 085 170 086 000 255 172 001 170
4	256	1 0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 0 1 1 0 0 1 1 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 1 0 0 1 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 1	Det = 1	001 000 000 000 000 000 000 000 000 001 000 255 000 000 000 000 001 255 001 002 000 255 255 000 000 000 000 001 000 000 000 000 000 000 000 000 001 000 000 000 255 000 000 255 000 001 000 000 000 000 000 000 000 000 001 000 000 000 000 000 255 000 000 001
4	256	1 0 0 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 0 0 1 0 0 1 0 1 1 0 0 0 1 0 1 1 0 0 0 1 0 0 0 1 0 1 0 1 0 0 1 0 0 1 1 0 1 0 0 0 1 0 0 1 0 0	Det = –3	085 255 171 171 171 171 086 085 085 000 171 171 171 171 085 085 170 255 086 086 085 086 171 171 085 255 171 171 170 172 086 085 085 001 171 170 171 170 085 086 086 001 170 170 171 170 085 086 001 001 255 000 000 255 000 000 086 000 171 171 170 171 085 085
4	256	1 0 0 0 1 1 0 0 1 0 1 1 0 0 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 1 0 0 1 0 1 1 0 0 0 1 0 0 0 0 0 0 1 0 1 1 0 0 1 0 0 1 0 0 1 0 1 1 0	Det = –1	003 001 252 006 001 255 255 254 001 000 254 003 001 000 000 255 001 001 255 002 000 255 000 255 255 000 001 254 000 000 000 001 000 000 001 255 000 000 000 000 254 255 003 251 255 001 001 002 000 000 000 001 000 000 000 000 253 255 004 250 255 002 001 002
4	256	1 0 0 0 0 0 0 0 0 1 1 0 0 1 0 1 0 0 1 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 0 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 0 1 0	Det = 1	001 000 000 000 000 000 000 000 001 001 000 000 255 000 255 000 000 000 001 255 000 000 000 000 000 000 000 001 000 000 000 000 255 255 000 000 001 255 001 001 255 000 255 001 000 000 001 000 000 000 000 255 000 001 000 000 000 000 000 000 001 000 000 000
4	256	1 0 1 0 1 0 0 0 0 1 0 0 0 0 0 1 1 1 0 1 0 0 1 0 0 0 1 0 0 0 0 0 0 0 1 0 1 1 0 0 0 0 1 0 1 0 0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 1 0 1	Det = 3	086 000 000 000 085 085 000 171 171 001 000 000 171 170 000 085 000 000 000 001 000 000 000 000 170 000 001 000 171 171 255 085 171 000 000 255 171 171 000 085 085 000 000 000 086 085 000 171 085 255 000 000 085 086 001 171 085 000 000 000 085 086 000 171

5.2 Статистичний розподіл параметрів

Для отримання статистичного розподілу параметру Δ_+ було вибрано випадкові восьмибітові s-блоки (перестановки). Перестановки генерувались методом безповторного набору. У наступних таблицях наведено цей розподіл.

Таблиця 2 – Статистичний розподіл параметру Δ_+ при $l = 2$ (вибірка з 10000 випадкових 8-бітових s-блоків)

Значення Δ_+	Значення $2^8 \cdot \Delta_+$	Кількість	Імовірність
0,046875	12	239	0,00239
0,050781	13	16459	0,16459
0,054688	14	45436	0,45436
0,058594	15	26832	0,26832

0,0625	16	8346	0,08346
0,066406	17	2078	0,02078
0,070313	18	483	0,00483
0,074219	19	102	0,00102
0,078125	20	21	0,00021
0,082031	21	4	0,00004

Таблиця 3 – Статистичний розподіл параметру Δ_+ при $l = 3$ (вибірка з 300000 випадкових 8-бітових s-блоків)

Значення Δ_+	Значення $2^8 \cdot \Delta_+$	Кількість	Імовірність
0,0546875	14	3123	0,01041
0,05859375	15	68005	0,2266833
0,0625	16	125596	0,4186533
0,06640625	17	70239	0,23413
0,0703125	18	24357	0,08119
0,07421875	19	6546	0,02182
0,078125	20	1638	0,00546
0,08203125	21	363	0,00121
0,0859375	22	108	0,00036
0,08984375	23	18	0,00006
0,09375	24	6	0,00002
0,09765625	25	2	0,00000667

VI Висновки

В статті отримано верхні оцінки середніх імовірностей цілочисельних диференціалів відображень, які є композиціями суматора, блока підстановки та довільного лінійного (над деяким кільцем) оператора, який має блокову структуру. Ці оцінки є новими та узагальнюють результати, отримані раніше та представлені в роботах [15 – 18]. Також отримано, строго обгрунтовані, параметри, що залежать від s-блоків та характеризують дані оцінки, та побудовано статистичний розподіл даних параметрів.

Отримані результати дозволяють аналізувати різницеві властивості раундових функцій блокових алгоритмів шифрування, що мають відповідну структуру. Зауважимо, що стійкість всього блокового алгоритму до різницевого аналізу залежить від різницевих властивостей його раундових функцій.

Для подальшого дослідження є цікавими та актуальними наступні задачі.

1. Побудова верхніх оцінок середніх імовірностей цілочисельних диференціалів відображень, які є композиціями суматора, блока підстановки та оператора перестановки у випадку, коли лінійний оператор є довільним (зокрема, має довільну обернену матрицю або або коли цей оператор є лінійним над деяким полем характеристики два).

2. Побудова аналогічних оцінок (у випадку довільного ключового суматора) для "змішаних" диференціалів з різними операціями на вході та виході.

3. Отримання відповідних параметрів, що залежать від s-блоків та характеризують дані оцінки. Побудова статистичного розподілу вказаних параметрів та аналіз даного розподілу.

4. Порівняльний аналіз статистичного розподілу класичних різницевих параметрів та цілочисельних різницевих. Зокрема, пошук таких s-блоків, для яких значення класичних різницевих параметрів суттєво відрізняється від значень параметрів, що характеризують стійкість до цілочисельного криптоаналізу.

5. Аналіз можливості та обгрунтованості такої модифікації блокового шифру, що замінює модульне додавання у ключовому суматорі на покомпонентне. Така модифікація часто спрощує аналіз стійкості шифру до різних видів атак, зокрема, до різницевого аналізу та його різновидів. Але питання про збереження властивостей (наприклад, різницевих) при заміні блокового шифру на таку модифікацію досі не досліджувалось. Для відповіді на це питання необхідно провести порівняльний аналіз операцій покомпонентного та модульного додавання на множині векторів над простим скінченим полем.

Список використаної літератури: ***1.*** *National Institute of Standards and Technology: The Advanced Encryption Standard (AES) – Режим доступа: http://csrc.nist.gov/aes/* ***2.*** *ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Госстандарт СССР, 1989. – 28с.* ***3.*** *Горбенко И. Д., Тоцький О. С., Казьміна С. В. Перспективний блоковий шифр "Калина" – основні положення та специфікація // Прикладна радіоелектроніка. – 2007. - т.6, №2. – С.195-208.* ***4.*** *Горбенко И. Д., Бондаренко М. Ф. та ін. Перспективний блоковий шифр "Мухомор" – основні положення та специфікація // Прикладна радіоелектроніка. – 2007. – т.6. №2. – С.147-157.* ***5.*** *Kovalchuk L., Alekseyshuk A., Upper Bounds of Maximum Value of Average Differential and Linear Characteristic Probabilities of Feistel Cipher with Adder Modulo 2^n, // Theory of Stochastic Processes. – 2006. – Vol. 12(28). – № 1, 2. – P. 20 – 32.* ***6.*** *Ковальчук Л. Верхние оценки средних вероятностей дифференциальных аппроксимаций булевых отображений // Труды Четвёртой Общероссийской научной Конференции "Математика и безопасность информационных технологий" (МаБИТ-05), 2-3 ноября 2005. – С.163-167.* ***7.*** *Ковальчук Л. Обобщённые марковские шифры: оценка практической стойкости к методу дифференциального криптоанализа // Труды Пятой Общероссийской научной Конференции "Математика и безопасность информационных технологий" – (МаБИТ-06), 25-27 октября 2006. – С. 595-599.* ***8.*** *Олексійчук А. Н., Ковальчук Л. В., Пальченко С. В. Криптографічні параметри вузлів заміни, що характеризують стійкість ГОСТ-подібних блокових шифрів відносно методів лінійного та різницевого криптоаналізу // Захист інформації. – 2007. – № 2. – С. 12 – 23* ***9.*** *Алексейчук А., Ковальчук Л., Шевцов А., Скрыпник Л. Оценки практической стойкости блочного шифра «Калина» относительно разностного, линейного билинейного методов криптоанализа. // Труды Седьмой Общероссийской научной Конференции "Математика и безопасность информационных технологий" – (МаБИТ-08), 30 октября – 2 ноября 2008. – С. 15-20.* ***10.*** *А. Алексейчук, Л. Ковальчук., Е. Скрынник, А. Шевцов. Оценки практической стойкости блочного шифра «Калина» относительно методов разностного, линейного криптоанализа и алгебраических атак, основанных на гомоморфизмах. // Прикладная радиоэлектроника. – №1. – 2008. – С. 203–210.* ***11.*** *X. Wang, H. Yu. How to Break MD5 and Other Hash Functions. // Advances in Cryptology EUROCRYPT'05, Lectures Notes in Computer Science 3494, Springer-Verlag, 2005, P. 19-35.* ***12.*** *S. Cotini, R. L. Riverst, M. J. B. Robshaw, Y. Lisa Yin. Security of the RC6^{TM} Block Cipher, http//www.rsasecurity.com/rsalabs/rc6/.* ***13.*** *Tomas A. Berson Differential cryptanalysis mod 2^{32} with applications to MD5 // Advanced in Cryptology. – CRYPTO'98 (LNCS 372). – 1999. – P. 95-103.* ***14.*** *Ковальчук Л. Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и оператора сдвига. //«Кибернетика и системный анализ» – 2010, – №6, С. 89 – 96.* ***15.*** *Ковальчук Л., Кучинская Н. Построение верхних оценок средних вероятностей целочисленных дифференциалов раундовых функций блочных шифров определенной структуры. //«Кибернетика и системный анализ» – 2012, – №5, С. 71 – 81.* ***16.*** *Кучинская Н. В. Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и произвольного оператора циклического сдвига. // Збірник наукових праць «Спеціальні телекомунікаційні системи та захист інформації» – 2013, – №1 (23), С. 18 – 24.* ***17.*** *Кучинская Н. В., Скрыпник Л. В. Построение верхних оценок средних вероятностей целочисленных раундовых функций определённой структуры. // Збірник наукових праць «Спеціальні телекомунікаційні системи та захист інформації» – 2013, – №2 (24), С. 27 – 33.* ***18.*** *Ковальчук Л., Кучинська Н., Бездітний В. Побудова верхніх оцінок середніх імовірностей цілочисельних диференціалів композиції модульного ключового суматора, блоку підстановки та лінійного оператора, що має блокову структуру. // Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту* інформації в Україні» *– 2014, – №28, С.47 – 52.*

Василь Карпінець, Юрій Яремчук
Вінницький національний технічний університет

УДК: 004.056.5

ПІДВИЩЕННЯ СТІЙКОСТІ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У ВЕКТОРНИХ ЗОБРАЖЕННЯХ ДО АТАКИ ВИЯВЛЕННЯ МІСЦЯ ЇХ РОЗТАШУВАННЯ

Анотація: **Запропоновано новий підхід до вбудовування цифрових водяних знаків (ЦВЗ) у частотну область векторних зображень на основі дискретного косинусного перетворення, що дозволяє зменшити максимальні відхилення координат точок до 20% порівняно з існуючим методом. Таке вдосконалення дозволяє зменшити вплив вбудовування ЦВЗ на візуальну якість векторних**