УДК 003.26:004.056.55:519.2

ВЕРХНІ ОЦІНКИ СТІЙКОСТІ БЛОКОВИХ ШИФРІВ ІЗ РАНДОМІЗОВАНИМИ ВУЗЛАМИ ЗАМІНИ ДО МЕТОДІВ ЛІНІЙНОГО ТА ДИФЕРЕНЦІАЛЬНОГО КРИПТОАНАЛІЗУ

Василь Кінзерявий

На сьогодні теорія аналізу та обґрунтування стійкості блокових шифрів із фіксованими вузлами заміни відносно методів лінійного та диференціального криптоаналізу досить сильно розвинена. Існують також блокові шифри, в яких вузли заміни визначаються раундовими ключами. Зрозуміло, що використання рандомізованих вузлів заміни у шифрах ускладнює їх криптоаналіз, проте кількісно це важко оцінити. З огляду на це, актуальною задачею є виведення аналітичних виразів, що дають можливість довести практичну стійкість блокових шифрів із рандомізованими вузлами заміни відносно методів лінійного і диференціального криптоаналізу та дозволять зробити кількісну оцінку їх ефективності. У роботі отримані аналітичні верхні оцінки параметрів, що характеризують практичну стійкість блокових шифрів із рандомізованими вузлами заміни відносно методів лінійного та диференціального криптоаналізу. Зазначені оцінки узагальнюють раніше відомі на блокові шифри із рандомізованими вузлами заміни і дозволяють обґрунтовувати підвищення стійкості відносно зазначених методів криптоаналізу.

Ключові слова: *криптографія, блоковий шифр, лінійний криптоаналіз, диференціальний криптоаналіз, рандомізовані вузли заміни.*

ВСТУП

Одними з найефективніших методів криптоаналізу блокових шифрів (БШ) є диференціальний та лінійний криптоаналіз [1-3]. На сьогодні теорія аналізу та обґрунтування стійкості БШ до зазначених атак досить сильно розвинена [4-9]. У багатьох БШ при шифруванні використовуються декілька різних таблиць замін, послідовність використання яких наперед фіксована (наприклад, алгоритм шифрування ГОСТ 28147-89 [10], Калина [11] та інші). Так у роботах [7-9] отримані аналітичні верхні оцінки параметрів, що характеризують практичну стійкість зазначених алгоритмів відносно методів лінійного та диференціального криптоаналізу. Існують також БШ, в яких операції підстановок визначаються раундовими ключами (наприклад, ADE [12]). Логічно припустити, що використання рандомізованих вузлів заміни ускладнює криптоаналіз БШ, проте кількісно це важко оцінити.

З огляду на це, актуальною задачею є виведення аналітичних виразів, що дозволяють довести практичну стійкість БШ із рандомізованими вузлами заміни відносно методів лінійного і диференціального криптоаналізу та дозволить зробити кількісну оцінку ефективності таких БШ.

ПОСТАНОВКА ЗАДАЧІ

У роботі [7] були отримані аналітичні верхні оцінки середніх ймовірностей диференціальних і лінійних характеристик БШ, побудованих за схемою шифру "Калина-128". Покажемо ефективність застосування рандомізованих вузлів замін до БШ побудованих за схемою шифру "Калина-128", у кожен раунд яких введено додатковий раундовий ключ, що впливає на вибір таблиць замін.

Розглянемо r-раундовий БШ $\mathfrak{I}$ із рандомізованими вузлами заміни, множиною відкритих (шифрованих) повідомлень $V_n = \{0,1\}^n$, множиною раундових ключів $K = V_{n+q}$ та сімейством шифруючих перетворень

$$F_k = f_{r,k_r} \circ ... \circ f_{1,k_1},\ k = (k_1, ..., k_r) \in K^r, \qquad (1)$$

де $r = 2r' + 1$, $n = pt$, $q = pq'$, $p = 4p'$, t, p', r', q' – натуральні числа. Параметр $b = 2^{q'}$ визначає кількість різних таблиць підстановок, що використовуються у БШ.

Раундове перетворення $f_{i,k}(x)$ для будь-яких $x \in V_n$, $k \in K$, $i \in \overline{1, r}$ описується як

$$f_{i,k}(x) = \begin{cases} \varphi\left(x \oplus k^{(1)}, k^{(2)}\right), & \text{якщо } i \equiv 1 \pmod 2,\ i < r \\ \varphi\left(\overset{\circ}{x + k^{(1)}}, k^{(2)}\right), & \text{якщо } i \equiv 0 \pmod 2,\ i < r \\ s\left(x \oplus k^{(1)}, k^{(2)}\right), & \text{якщо } i = r \end{cases}, \qquad (2)$$

де $k^{(1)}$ та $k^{(2)}$ частини раундового ключа k ($k = \left(k^{(1)}, k^{(2)}\right)$, $k^{(1)} \in V_n$, $k^{(2)} \in V_q$).

Підстановки φ і s визначаються за формулами:

$$\varphi(x, y) = s(x, y)M,\ x \in V_n,\ y \in V_q, \qquad (3)$$

$$s(x, y) = \left(s_{y_{p-1}}(x_{p-1}), \ldots, s_{y_0}(x_0)\right),$$
$$x = (x_{p-1}, \ldots, x_0), y = (y_{p-1}, \ldots, y_0), \quad (4)$$

де $x_j \in V_t$, $y_j \in V_{q'}$, s_{y_j} – підстановка на множині V_t (по індексу y_j обирається для використання одна таблиця підстановок із b можливих), $j \in \overline{0, p-1}$, M – оборотна $p \times p$ - матриця над полем $\mathrm{GF}(2^t)$, а множення $s(x, y)$ на M у виразі (3) виконується над цим полем при ототожненні двійкових векторів $s_{y_j}(x_j)$ із його елементами.

У формулі (2) символи $\oplus$ і $\overset{\circ}{+}$ відповідають відповідно операціям по координатного булевого додавання двійкових векторів довжини n та алгебраїчну операцію виду

$$x \overset{\circ}{+} k = \left(x^{(1)} + k^{(1)}, \ldots, x^{(4)} + k^{(4)}\right), \quad (5)$$

де $x = \left(x^{(1)}, \ldots, x^{(4)}\right)$, $k = \left(k^{(1)}, \ldots, k^{(4)}\right)$, $x^{(v)}, k^{(v)} \in V_{tp'}$, $v \in \overline{1,4}$, а $+$ це символ операції додавання за модулем $2^{tp'}$ на множині $V_{tp'}$.

Нагадаємо, що імовірність диференціальної характеристики $\Omega = (\omega_0, \omega_1, \ldots, \omega_r) \in \left(V_n \setminus \{0\}\right)^{r+1}$ БШ $\mathfrak{I}$ при ключі шифрування $(k_1, \ldots, k_r)$ визначається по формулі [13]:

$$DP^{(k_1, \ldots, k_r)}(\Omega) = \mathrm{P}\left(\bigcap_{i=1}^{r}\left\{X_i \oplus X_i' = \omega_i\right\} \mid X \oplus X' = \omega_0\right), \quad (6)$$

де X, X' – незалежні випадкові рівноімовірні двійкові вектори довжини n:

$X_i = \left(f_{i,k_i} \circ \ldots \circ f_{1,k_1}\right)(X)$, $X_i' = \left(f_{i,k_i} \circ \ldots \circ f_{1,k_1}\right)(X')$, $i \in \overline{1, r}$.

Середнє значення (6) по всім $(k_1, \ldots, k_r) \in K^r$ називають середньою імовірністю диференціальної характеристики Ω та визначають за формулою [13]:

$$EDP(\Omega) = |K|^{-r} \sum_{(k_1, \ldots, k_r) \in K^r} DP^{(k_1, \ldots, k_r)}(\Omega). \quad (7)$$

Також нагадаємо [13], що середня ймовірність лінійної характеристики $\Omega = (\omega_0, \omega_1, \ldots, \omega_r)$ БШ $\mathfrak{I}$ визначається за формулою:

$$ELP(\Omega) = \prod_{i=1}^{r} l^{(i)}(\omega_{i-1}, \omega_i), \quad (8)$$

де для будь-яких $\alpha, \beta \in V_n$, $i \in \overline{1, r}$

$$l^{(i)}(\alpha, \beta) = 2^{-(n+q)} \sum_{k \in V_{n+q}} \left(2^{-n} \sum_{x \in V_n} (-1)^{\alpha x \oplus \beta f_{i,k}(x)}\right)^2. \quad (9)$$

Метою даної роботи є оцінка практичної стійкості БШ із рандомізованими вузлами заміни, що описуються формулами (1)–(5), відносно методів диференціального та лінійного криптоаналізу за рахунок отримання аналітичних верхніх меж параметрів (7), (8). На основі даних оцінок покажемо ефективність використання рандомізованих вузлів заміни.

ВЕРХНЯ ОЦІНКА СЕРЕДНІХ ЙМОВІРНОСТЕЙ ДИФЕРЕНЦІАЛЬНИХ ХАРАКТЕРИСТИК

Нагадаємо [7], що для довільної диференціальної характеристики Ω БШ $\mathfrak{I}$ із сімейством шифруючих перетворень (1) виконується нерівність:

$$EDP(\Omega) \le \prod_{i=1}^{r} \max_{x \in V_n} d_x^{(i)}(\omega_{i-1}, \omega_i), \quad (10)$$

де для будь-яких $x, \alpha, \beta \in V_n$, $i \in \overline{1, r}$

$$d_x^{(i)}(\alpha, \beta) = |K|^{-1} \sum_{k \in K} \delta\left(f_{i,k}(x \oplus \alpha) \oplus f_{i,k}(x), \beta\right). \quad (11)$$

Нехай $\mathfrak{I}$ – БШ, що описуються формулами (1)–(5). З огляду на те, що для даного БШ раундовий ключ описується співвідношенням $k = \left(k^{(1)}, k^{(2)}\right)$, $k^{(1)} \in V_n$, $k^{(2)} \in V_q$, перепишемо формулу (11) в наступному вигляді

$$d_x^{(i)}(\alpha, \beta) = 2^{-(n+q)} \sum_{k \in V_{n+q}} \delta\left(f_{i,k}(x \oplus \alpha) \oplus f_{i,k}(x), \beta\right) =$$
$$= 2^{-q} \sum_{k^{(2)} \in V_q} \left(2^{-n} \sum_{k^{(1)} \in V_n} \delta\left(f_{i,\left(k^{(1)}, k^{(2)}\right)}(x \oplus \alpha) \oplus f_{i,\left(k^{(1)}, k^{(2)}\right)}(x), \beta\right)\right). \quad (12)$$

Для знаходження верхньої межі параметра $EDP(\Omega)$ оцінимо кожен із співмножників правої частини нерівності (10).

Спочатку введемо деякі позначення. Для будь-якого натурального l позначимо $u + v$ суму за модулем 2^l двійкових цілих чисел, представлених у вигляді векторів u та v $(u, v \in V_l)$; символом $\nu(u, v)$ позначимо біт переносу в l-й розряд при додаванні чисел u і v в кільці Z.

Для будь-якого $j \in \overline{0, b-1}$, аналогічно роботі [7], позначимо:

$$d_{\oplus}^{(s_j)}(\alpha, \beta) = 2^{-t} \sum_{k \in V_t} \delta\left(s_j(k \oplus \alpha) \oplus s_j(k), \beta\right), \quad (13)$$

$$d_{+}^{(s_j)}(\alpha, \beta) = 2^{-t} \sum_{k \in V_t} \delta\left(s_j(k + \alpha) \oplus s_j(k), \beta\right), \quad (14)$$

$$\Delta_{\oplus} = \max\left\{d_{\oplus}^{(s_j)}(\alpha,\beta): \alpha,\beta \in V_t \setminus \{0\}, j \in \overline{0,b-1}\right\}, \quad (15)$$

$$\Delta_{+} = \max\left\{d_{+}^{(s_j)}(\alpha,\beta): \alpha,\beta \in V_t \setminus \{0\}, j \in \overline{0,b-1}\right\}, \quad (16)$$

$$\Delta = \max\left\{\Delta_{\oplus}, \Delta_{+}\right\}. \quad (17)$$

Додатково введемо наступні співвідношення:

$$\tilde{\Delta}_{\oplus} = b^{-1}\sum_{j=0}^{b-1}\max\left\{d_{\oplus}^{(s_j)}(\alpha,\beta): \alpha,\beta \in V_t \setminus \{0\}\right\}, \quad (18)$$

$$\tilde{\Delta}_{+} = b^{-1}\sum_{j=0}^{b-1}\max\left\{d_{+}^{(s_j)}(\alpha,\beta): \alpha,\beta \in V_t \setminus \{0\}\right\}, \quad (19)$$

$$\tilde{\Delta} = \max\left\{\tilde{\Delta}_{\oplus}, \tilde{\Delta}_{+}\right\}, \quad (20)$$

$$\tilde{\tilde{d}}_{\oplus}(\alpha,\beta) = b^{-1}\sum_{j=0}^{b-1} d_{\oplus}^{(s_j)}(\alpha,\beta), \quad (21)$$

$$\tilde{\tilde{d}}_{+}(\alpha,\beta) = b^{-1}\sum_{j=0}^{b-1} d_{+}^{(s_j)}(\alpha,\beta), \quad (22)$$

$$\tilde{\tilde{\Delta}}_{\oplus} = \max\left\{\tilde{\tilde{d}}_{\oplus}(\alpha,\beta): \alpha,\beta \in V_t \setminus \{0\}\right\}, \quad (23)$$

$$\tilde{\tilde{\Delta}}_{+} = \max\left\{\tilde{\tilde{d}}_{+}(\alpha,\beta): \alpha,\beta \in V_t \setminus \{0\}\right\}, \quad (24)$$

$$\tilde{\tilde{\Delta}} = \max\left\{\tilde{\tilde{\Delta}}_{\oplus}, \tilde{\tilde{\Delta}}_{+}\right\}. \quad (25)$$

Нагадаємо [7], що вага вектора $x = (x_{p-1}, \ldots, x_0)$ визначається за формулою:

$$wt(x) = \#\left\{j \in \overline{0,\ p-1}: x_j \neq 0\right\}, \quad (26)$$

де $x_j \in \mathrm{GF}(2^t)$, $j \in \overline{0,\ p-1}$. Індекс галуження матриці M визначається за формулою [14]:

$$B_M = \min\left\{wt(x) + wt\left(xM^{-1}\right): x \in GF\left(2^t\right)^p \setminus \{0\}\right\}. \quad (27)$$

Тепер доведемо наступне твердження.

Лема 1. Нехай $\mathfrak{I}$ – БШ, що описується співвідношеннями (1)–(5). Тоді для будь-якого $x \in V_n$ виконуються наступні твердження:

1) якщо $i \equiv 1 \pmod 2$, $i < r$, то

$$d_x^{(i)}(\omega_{i-1}, \omega_i) \le \left(\tilde{\tilde{\Delta}}_{\oplus}\right)^{wt(\omega_i M^{-1})}; \quad (28)$$

2) якщо $i = r$, то

$$d_x^{(i)}(\omega_{i-1}, \omega_i) \le \left(\tilde{\tilde{\Delta}}_{\oplus}\right)^{wt(\omega_i)}; \quad (29)$$

3) якщо $i \equiv 0 \pmod 2$, $i < r$, то

$$d_x^{(i)}(\omega_{i-1}, \omega_i) \le \left(\tilde{\tilde{\Delta}}_{+}\right)^{wt(\omega_i M^{-1})}; \quad (30)$$

4) якщо $i < r$, то

$$wt\left(\omega_i M^{-1}\right) = wt\left(\omega_{i-1}\right); \quad (31)$$

5) якщо $i = r$, то

$$wt(\omega_r) = wt\left(\omega_{r-1}\right). \quad (32)$$

Доведення. Нехай $i \equiv 1 \pmod 2$, $i < r$. Враховуючи співвідношення (2) перепишемо формулу (12):

$$d_x^{(i)}(\omega_{i-1}, \omega_i) = 2^{-q}\sum_{k^{(2)} \in V_q}\left(2^{-n}\sum_{k^{(1)} \in V_n}\delta\left(\varphi\left(k^{(1)} \oplus \omega_{i-1}, k^{(2)}\right) \oplus \varphi\left(k^{(1)}, k^{(2)}\right), \omega_i\right)\right) =$$

$$= 2^{-q}\sum_{k^{(2)} \in V_q}\left(2^{-n}\sum_{k^{(1)} \in V_n}\delta\left(s\left(k^{(1)} \oplus \omega_{i-1}, k^{(2)}\right) \oplus s\left(k^{(1)}, k^{(2)}\right), \omega_i M^{-1}\right)\right).$$

Звідки на основі формул (4), (13), (21) випливає, що

$$d_x^{(i)}(\omega_{i-1}, \omega_i) = \prod_{j=0}^{p-1}\left(2^{-q'}\sum_{k_j^{(2)} \in V_{q'}}\left(2^{-t}\sum_{k_j^{(1)} \in V_t}\delta\left(s_{k_j^{(2)}}\left(k_j^{(1)} \oplus (\omega_{i-1})_j\right) \oplus s_{k_j^{(2)}}\left(k_j^{(1)}\right), \left(\omega_i M^{-1}\right)_j\right)\right)\right) =$$

$$= \prod_{j=0}^{p-1}\left(2^{-q'}\sum_{k_j^{(2)} \in V_{q'}}\left(d_{\oplus}^{\left(s_{k_j^{(2)}}\right)}\left((\omega_{i-1})_j, \left(\omega_i M^{-1}\right)_j\right)\right)\right) = \prod_{j=0}^{p-1}\left(\tilde{\tilde{d}}_{\oplus}\left((\omega_{i-1})_j, \left(\omega_i M^{-1}\right)_j\right)\right). \quad (33)$$

Оскільки $\tilde{\tilde{d}}_{\oplus}\left((\omega_{i-1})_j, \left(\omega_i M^{-1}\right)_j\right) \le 1$, то максимальне значення співвідношення (33) досягає коли $(\omega_{i-1})_j = \left(\omega_i M^{-1}\right)_j = 0$, в такому випадку $\tilde{\tilde{d}}_{\oplus}\left((\omega_{i-1})_j, \left(\omega_i M^{-1}\right)_j\right) = 1$ (зауважимо, що хоча б для одного j $(\omega_{i-1})_j, \left(\omega_i M^{-1}\right)_j \neq 0$ ($j \in \overline{0,\ p-1}$)). На основі чого, з використанням формули (23) слідує вірність нерівності (28) та формули (31):

$$d_x^{(i)}(\omega_{i-1},\omega_i)=\prod_{j=0}^{p-1}\left(\tilde{\tilde{d}}_{\oplus}\left((\omega_{i-1})_j,\left(\omega_i M^{-1}\right)_j\right)\right)\le\tilde{\tilde{\Delta}}_{\oplus}^{\,wt\left(\omega_i M^{-1}\right)},$$

$$wt\left(\omega_i M^{-1}\right)=wt\left(\omega_{i-1}\right).$$

Аналогічним чином доводяться співвідношення (29), (32).

Доведемо співвідношення (30). Нехай $i\equiv 0\pmod 2$, $i<r$. Враховуючи співвідношення (2) перепишемо формулу (12):

$$d_x^{(i)}(\omega_{i-1},\omega_i)=2^{-q}\sum_{k^{(2)}\in V_q}\left(2^{-n}\sum_{k^{(1)}\in V_n}\delta\left(\varphi\left(\left(x\oplus\omega_{i-1}\right)\overset{\circ}{+}k^{(1)},k^{(2)}\right)\oplus\varphi\left(x\overset{\circ}{+}k^{(1)},k^{(2)}\right),\omega_i\right)\right)=$$

$$=2^{-q}\sum_{k^{(2)}\in V_q}\left(2^{-n}\sum_{k^{(1)}\in V_n}\delta\left(s\left(k^{(1)}\overset{\circ}{+}\left(\left(x\oplus\omega_{i-1}\right)\overset{\circ}{-}x\right),k^{(2)}\right)\oplus s\left(k^{(1)},k^{(2)}\right),\omega_i M^{-1}\right)\right). \qquad (34)$$

У роботі [7] доведено, що для довільних фіксованих підстановок на множині V_t, $s(x)=\left(s_{m-1}(x_{m-1}),\dots,s_0(x_0)\right)$, $x=(x_{m-1},\dots,x_0)$ при будь-яких $\alpha,\beta\in V_{mt}$ справедлива нерівність:

$$d_+^{(s)}(\alpha,\beta)\overset{\text{def}}{=}2^{-mt}\sum_{k\in V_{mt}}\delta\left(s(\alpha+k)\oplus s(k),\beta\right)\le\left(\Delta_+\right)^{wt(\beta)}. \qquad (35)$$

Аналогічно перепишемо формулу (35) для випадку, коли таблиця підстановок s буде залежати від параметра y (див. формулу (4)).

Нехай $s(x,y)=\left(s_{y_{m-1}}(x_{m-1}),\dots,s_{y_0}(x_0)\right)$ – довільна підстановка на множині V_{mt}, $x=(x_{m-1},\dots,x_0)$, $y=(y_{m-1},\dots,y_0)$, $x_j\in V_t$, $y_j\in V_{q'}$, $j\in\overline{0,m-1}$ (параметром y_j зазначається яка конкретна таблиця замін на множині V_t буде використовуватись – обирається одна таблиця із $2^{q'}$ можливих). Тоді для будь-яких $\alpha,\beta\in V_{mt}$ справедлива нерівність:

$$d_+^{(s)}(\alpha,\beta)\overset{\text{def}}{=}2^{-mq'}\sum_{y\in V_{mq'}}\left(2^{-mt}\sum_{k\in V_{mt}}\delta\left(s(\alpha+k,y)\oplus s(k,y),\beta\right)\right)\le\left(\tilde{\tilde{\Delta}}_+\right)^{wt(\beta)}. \qquad (36)$$

Доведемо нерівність (36) методом математичної індукції по параметру m (аналогічно [7]). Перевіримо при $m=1$ справедливість твердження (36). На основі співвідношення (14), (22) та (24) випливає, що:

$$d_+^{(s)}(\alpha,\beta)=2^{-q'}\sum_{y\in V_{q'}}\left(2^{-t}\sum_{k\in V_t}\delta\left(s_y(\alpha+k)\oplus s_y(k),\beta\right)\right)=$$

$$=2^{-q'}\sum_{y\in V_{q'}}\left(d_+^{(s_y)}(\alpha,\beta)\right)=\tilde{\tilde{d}}_+(\alpha,\beta)\le\left(\tilde{\tilde{\Delta}}_+\right)^{wt(\beta)}.$$

Тепер припустимо, що твердження (36) виконується для усіх підстановок виду $\left(s_{y_{m-1}}(x_{m-1}),\dots,s_{y_1}(x_1)\right)$, де s_{y_j} – підстановка на множині V_t, $y_j\in V_{q'}$, $j\in\overline{1,m-1}$.

Для будь-якого $x=(x_{m-1},\dots,x_0)\in V_{mt}$, $y=(y_{m-1},\dots,y_0)\in V_{mq'}$ позначимо

$$\tilde{x}=(x_{m-1},\dots,x_1),\qquad \tilde{y}=(y_{m-1},\dots,y_1),$$

$$\tilde{s}\left(\tilde{x},\tilde{y}\right)=\left(s_{y_{m-1}}(x_{m-1}),\dots,s_{y_1}(x_1)\right).$$

В силу рівності

$$\alpha+k=\left(\tilde{\alpha}+\tilde{k}+\nu(\alpha_0,k_0),\alpha_0+k_0\right),\qquad \alpha,k\in V_{mt},$$

справедливе наступне:

$$d_+^{(s)}(\alpha,\beta)=2^{-q'}\sum_{y_0\in V_{q'}}\left(2^{-t}\sum_{k_0\in V_t}\delta\left(s_{y_0}(\alpha_0+k_0)\oplus s_{y_0}(k_0),\beta_0\right)\right)\times$$

$$\times 2^{-(mq'-q')} \sum_{\tilde{y}\in V_{mq'-q'}} \left(2^{-(mt-t)} \sum_{\tilde{k}\in V_{mt-t}} \delta\left(\tilde{s}\left(\tilde{\alpha}+\tilde{k}+\nu(\alpha_0,k_0), \tilde{y} \right) \oplus \tilde{s}\left(\tilde{k}, \tilde{y} \right), \tilde{\beta} \right) \right) =$$

$$= \underset{\nu(\alpha_0,k_0)=1}{\overset{\approx}{d}}{}_{+}(\alpha_0,\beta_0) \times 2^{-(mq'-q')} \sum_{\tilde{y}\in V_{mq'-q'}} \left(2^{-(mt-t)} \sum_{\tilde{k}\in V_{mt-t}} \delta\left(\tilde{s}\left(\tilde{\alpha}+\tilde{k}+1, \tilde{y} \right) \oplus \tilde{s}\left(\tilde{k}, \tilde{y} \right), \tilde{\beta} \right) \right) +$$

$$+ \underset{\nu(\alpha_0,k_0)=0}{\overset{\approx}{d}}{}_{+}(\alpha_0,\beta_0) \times 2^{-(mq'-q')} \sum_{\tilde{y}\in V_{mq'-q'}} \left(2^{-(mt-t)} \sum_{\tilde{k}\in V_{mt-t}} \delta\left(\tilde{s}\left(\tilde{\alpha}+\tilde{k}, \tilde{y} \right) \oplus \tilde{s}\left(\tilde{k}, \tilde{y} \right), \tilde{\beta} \right) \right) =$$

$$= \underset{\nu(\alpha_0,k_0)=1}{\overset{\approx}{d}}{}_{+}(\alpha_0,\beta_0) \times d_{+}^{\left(\tilde{s}\right)}\left(\tilde{\alpha}+1, \tilde{\beta} \right) + \underset{\nu(\alpha_0,k_0)=0}{\overset{\approx}{d}}{}_{+}(\alpha_0,\beta_0) \times d_{+}^{\left(\tilde{s}\right)}\left(\tilde{\alpha}, \tilde{\beta} \right). \quad (37)$$

Оскільки $d_{+}^{\left(\tilde{s}\right)}\left(\tilde{\alpha}+1, \tilde{\beta} \right) \le \left(\overset{\approx}{\Delta}_{+} \right)^{wt\left(\tilde{\beta}\right)}$ та $d_{+}^{\left(\tilde{s}\right)}\left(\tilde{\alpha}, \tilde{\beta} \right) \le \left(\overset{\approx}{\Delta}_{+} \right)^{wt\left(\tilde{\beta}\right)}$ за припущенням індукції, то на основі формули (37) слідує справедливість твердження (36):

$$d_{+}^{(s)}(\alpha,\beta) \le \underset{}{\overset{\approx}{d}}{}_{+}(\alpha_0,\beta_0) \times \left(\overset{\approx}{\Delta}_{+} \right)^{wt\left(\tilde{\beta}\right)} \le \left(\overset{\approx}{\Delta}_{+} \right)^{wt\left(\tilde{\beta}\right)+wt(\beta_0)} = \left(\overset{\approx}{\Delta}_{+} \right)^{wt(\beta)},$$

що і потрібно було довести.

Перепишемо співвідношення (34) враховуючи нерівність (36):

$$d_{x}^{(i)}\left(\omega_{i-1},\omega_i\right) = d_{+}^{(s)}\left(\left(x\oplus\omega_{i-1} \right)^{\circ} - x, \omega_i M^{-1} \right) \le \left(\overset{\approx}{\Delta}_{+} \right)^{wt\left(\omega_i M^{-1}\right)}.$$

Отже, справедлива нерівність (30). Лема доведена.

Тепер встановимо аналітичну верхню оцінку стійкості параметру (7) для БШ, що описуються співвідношеннями (1)-(5).

Теорема 1. Нехай $\Im - r$-раундовий БШ, що описується співвідношеннями (1)-(5). Тоді виконуються наступна нерівність:

$$EDP(\Omega) \le \overset{\approx}{\Delta}^{r'B_M+1} \le \tilde{\Delta}^{r'B_M+1} \le \Delta^{r'B_M+1}. \quad (38)$$

Доведення.

На основі співвідношень формул (10), (23)-(25), (28)-(30) справедлива оцінка:

$$EDP(\Omega) \le \overset{\approx}{\Delta}^{\sum_{i=1}^{r-1} wt\left(\omega_i M^{-1}\right)+wt(\omega_r)}. \quad (39)$$

Оскільки за формулами (13)-(25) $\overset{\approx}{\Delta} \le \tilde{\Delta} \le \Delta < 1$, то права частина нерівності буде максимальною тільки коли $\sum_{i=1}^{r-1} wt\left(\omega_i M^{-1}\right) + wt(\omega_r)$ буде мінімальним. В роботі [7] показано, що $\sum_{i=1}^{r-1} wt\left(\omega_i M^{-1}\right) + wt(\omega_r) \ge r'B_M + 1$, на основі чого слідує нерівність (38). Теорема доведена.

ВЕРХНЯ ОЦІНКА СЕРЕДНІХ ЙМОВІРНОСТЕЙ ЛІНІЙНИХ ХАРАКТЕРИСТИК

Для будь-якого $\alpha,\beta \in V_t$, $j \in \overline{0,b-1}$, аналогічно роботі [7], позначимо:

$$l^{(s_j)}(\alpha,\beta) = 2^{-t} \sum_{k\in V_t} \left(2^{-t} \sum_{x\in V_t} (-1)^{\alpha x \oplus \beta s_j(x\oplus k)} \right)^2, \quad (40)$$

$$\Lambda^{(s_j)}(\alpha,\beta) = 2^{-t} \sum_{k\in V_t} \left(2^{-t} \sum_{a\in\{0,1\}} \left| \sum_{x\in V_t : \nu(x,k)=a} (-1)^{\alpha x \oplus \beta s_j(x+k)} \right| \right)^2, \quad (41)$$

$$\Lambda_{\oplus} = \max\left\{ l^{(s_j)}(\alpha,\beta) : \alpha,\beta \in V_t \setminus \{0\}, j \in \overline{0,b-1} \right\}, \quad (42)$$

$$\Lambda_{+} = \max\left\{ \Lambda^{(s_j)}(\alpha,\beta) : \alpha \in V_t, \beta \in V_t \setminus \{0\}, j \in \overline{0,b-1} \right\}, \quad (43)$$

$$\Lambda = \max\left\{ \Lambda_{\oplus}, \Lambda_{+} \right\}. \quad (44)$$

Додатково введемо наступні співвідношення:

$$\tilde{\Lambda}_{\oplus} = b^{-1} \sum_{j=0}^{b-1} \max\left\{ l^{(s_j)}(\alpha,\beta) : \alpha,\beta \in V_t \setminus \{0\} \right\}, \quad (45)$$

$$\tilde{\Lambda}_{+} = b^{-1} \sum_{j=0}^{b-1} \max\left\{ \Lambda^{(s_j)}(\alpha,\beta) : \alpha \in V_t, \beta \in V_t \setminus \{0\} \right\}, \quad (46)$$

$$\tilde{\Lambda} = \max\left\{ \tilde{\Lambda}_{\oplus}, \tilde{\Lambda}_{+} \right\}, \quad (47)$$

$$\tilde{\tilde{l}}(\alpha,\beta)=b^{-1}\sum_{j=0}^{b-1}l^{(s_j)}(\alpha,\beta), \quad (48)$$

$$\tilde{\tilde{\Lambda}}(\alpha,\beta)=b^{-1}\sum_{j=0}^{b-1}\Lambda^{(s_j)}(\alpha,\beta), \quad (49)$$

$$\tilde{\tilde{\Lambda}}_{\oplus}=\max\left\{\tilde{\tilde{l}}(\alpha,\beta):\alpha,\beta\in V_t\setminus\{0\}\right\}, \quad (50)$$

$$\tilde{\tilde{\Lambda}}_{+}=\max\left\{\tilde{\tilde{\Lambda}}(\alpha,\beta):\alpha\in V_t,\beta\in V_t\setminus\{0\}\right\}, \quad (51)$$

$$\tilde{\tilde{\Lambda}}=\max\left\{\tilde{\tilde{\Lambda}}_{\oplus},\tilde{\tilde{\Lambda}}_{+}\right\}. \quad (52)$$

Для знаходження верхньої межі параметра $ELP(\Omega)$ оцінимо кожен із співмножників правої частини співвідношення (8).

Лема 2. Нехай $\mathfrak{I}$ – БШ, що описується співвідношеннями (1)–(5). Тоді для будь-якого $x\in V_n$ виконуються наступні твердження:

1) якщо $i\equiv 1\pmod 2$, $i<r$, то

$$l^{(i)}(\omega_{i-1},\omega_i)\le\left(\tilde{\tilde{\Lambda}}_{\oplus}\right)^{wt(\omega_iM)}; \quad (53)$$

2) якщо $i=r$, то

$$l^{(i)}(\omega_{i-1},\omega_i)\le\left(\tilde{\tilde{\Lambda}}_{\oplus}\right)^{wt(\omega_i)}; \quad (54)$$

3) якщо $i\equiv 0\pmod 2$, $i<r$, то

$$l^{(i)}(\omega_{i-1},\omega_i)\le\left(\tilde{\tilde{\Lambda}}_{+}\right)^{wt(\omega_iM)}; \quad (55)$$

4) якщо $i<r$, то

$$wt(\omega_iM)=wt(\omega_{i-1}); \quad (56)$$

5) якщо $i=r$, то

$$wt(\omega_r)=wt(\omega_{r-1}). \quad (57)$$

Доведення. Нехай $i\equiv 1\pmod 2$, $i<r$. Враховуючи співвідношення (2) перепишемо формулу (9):

$$l^{(i)}(\omega_{i-1},\omega_i)=2^{-q}\sum_{k^{(2)}\in V_q}\left(2^{-n}\sum_{k^{(1)}\in V_n}\left(2^{-n}\sum_{x\in V_n}(-1)^{\omega_{i-1}x\oplus\omega_i\varphi\left(x\oplus k^{(1)},\,k^{(2)}\right)}\right)^2\right)=$$

$$=2^{-q}\sum_{k^{(2)}\in V_q}\left(2^{-n}\sum_{k^{(1)}\in V_n}\left(2^{-n}\sum_{x\in V_n}(-1)^{\omega_{i-1}x\oplus(\omega_iM)\cdot s\left(x\oplus k^{(1)},\,k^{(2)}\right)}\right)^2\right).$$

Звідки на основі формул (4), (40), (48) випливає, що

$$l^{(i)}(\omega_{i-1},\omega_i)=\prod_{j=0}^{p-1}\left(2^{-q'}\sum_{k_j^{(2)}\in V_{q'}}\left(2^{-t}\sum_{k_j^{(1)}\in V_t}\left(2^{-t}\sum_{x_j\in V_t}(-1)^{(\omega_{i-1})_jx_j\oplus(\omega_iM)_j\cdot s_{k_j^{(2)}}\left(x_j\oplus k_j^{(1)}\right)}\right)^2\right)\right)=$$

$$=\prod_{j=0}^{p-1}\left(2^{-q'}\sum_{k_j^{(2)}\in V_{q'}}\left(l^{\left(s_{k_j^{(2)}}\right)}\left((\omega_{i-1})_j,(\omega_iM)_j\right)\right)\right)=\prod_{j=0}^{p-1}\left(\tilde{\tilde{l}}\left((\omega_{i-1})_j,(\omega_iM)_j\right)\right). \quad (58)$$

Оскільки $\tilde{\tilde{l}}\left((\omega_{i-1})_j,(\omega_iM)_j\right)\le 1$, то максимальне значення співвідношення (58) досягає при $(\omega_{i-1})_j=(\omega_iM)_j=0$, в такому випадку $\tilde{\tilde{l}}\left((\omega_{i-1})_j,(\omega_iM)_j\right)=1$ (зауважимо, що хоча б для одного j $(\omega_{i-1})_j,(\omega_iM)_j\ne 0$ ($j\in\overline{0,\,p-1}$)). На основі чого, з використанням формули (50) слідує вірність нерівності (53) та формули (56):

$$l^{(i)}(\omega_{i-1},\omega_i)=\prod_{j=0}^{p-1}\left(\tilde{\tilde{l}}\left((\omega_{i-1})_j,(\omega_iM)_j\right)\right)\le\tilde{\tilde{\Lambda}}_{\oplus}^{\,wt(\omega_iM)},$$

$$wt(\omega_iM)=wt(\omega_{i-1}).$$

Аналогічним чином доводяться співвідношення (54), (57).

Доведемо співвідношення (55). Нехай $i\equiv 0\pmod 2$, $i<r$. Враховуючи співвідношення (2) перепишемо формулу (9):

$$l^{(i)}(\omega_{i-1},\omega_i)=2^{-q}\sum_{k^{(2)}\in V_q}\left(2^{-n}\sum_{k^{(1)}\in V_n}\left(2^{-n}\sum_{x\in V_n}(-1)^{\omega_{i-1}x\oplus\omega_i\varphi\left(\overset{\circ}{x+k^{(1)}},\,k^{(2)}\right)}\right)^2\right)=$$

$$=2^{-q}\sum_{k^{(2)}\in V_q}\left(2^{-n}\sum_{k^{(1)}\in V_n}\left(2^{-n}\sum_{x\in V_n}(-1)^{\omega_{i-1}x\oplus(\omega_iM)s\left(\overset{\circ}{x+k^{(1)}},\,k^{(2)}\right)}\right)^2\right). \quad (59).$$

Нехай $s(x, y)=\left(s_{y_{m-1}}(x_{m-1}), \ldots, s_{y_0}(x_0)\right)$ – довільна підстановка на множині V_{mt}, $x=(x_{m-1}, \ldots, x_0)$, $y=(y_{m-1}, \ldots, y_0)$, $x_j \in V_t$, $y_j \in V_{q'}$, $j \in \overline{0, m-1}$ (параметром y_j зазначається яка конкретна таблиця замін на множині V_t буде використовуватись – обирається одна таблиця із $2^{q'}$ можливих). Тоді для будь-яких $\alpha, \beta \in V_{mt}$ справедлива нерівність:

$$l_+^{(s)}(\alpha, \beta) \stackrel{\text{def}}{=} 2^{-mq'} \sum_{y \in V_{mq'}} \left(2^{-mt} \sum_{k \in V_{mt}} \left(2^{-mt} \sum_{x \in V_{mt}} (-1)^{\alpha x \oplus \beta s(x+k, y)} \right)^2 \right) \le \left(\tilde{\tilde{\Lambda}}_+ \right)^{wt(\beta)}. \quad (60)$$

Доведемо нерівність (60) методом математичної індукції по параметру m. Перевіримо при $m=1$ справедливість твердження (60). На основі співвідношення (41), (49) та (51) випливає, що:

$$l_+^{(s)}(\alpha, \beta) = 2^{-q'} \sum_{y \in V_{q'}} \left(2^{-t} \sum_{k \in V_t} \left(2^{-t} \sum_{x \in V_t} (-1)^{\alpha x \oplus \beta s(x+k, y)} \right)^2 \right) =$$

$$= 2^{-q'} \sum_{y \in V_{q'}} \left(2^{-t} \sum_{k \in V_t} \left(2^{-t} \sum_{a \in \{0,1\}} \left| \sum_{x \in V_t : \nu(x, k)=a} (-1)^{\alpha x \oplus \beta s_y(x+k)} \right| \right)^2 \right) = \tilde{\tilde{\Lambda}}(\alpha, \beta) \le \left(\tilde{\tilde{\Lambda}}_+ \right)^{wt(\beta)}.$$

Тепер припустимо, що твердження (60) виконується для усіх підстановок виду $\left(s_{y_{m-1}}(x_{m-1}), \ldots, s_{y_1}(x_1)\right)$, де s_{y_j} – підстановка на множині V_t, $y_j \in V_{q'}$, $j \in \overline{1, m-1}$.

Для будь-якого $x=(x_{m-1}, \ldots, x_0) \in V_{mt}$, $y=(y_{m-1}, \ldots, y_0) \in V_{mq'}$ позначимо

$$\tilde{x}=(x_{m-1}, \ldots, x_1), \ \tilde{y}=(y_{m-1}, \ldots, y_1), \ \tilde{s}\left(\tilde{x}, \tilde{y}\right)=\left(s_{y_{m-1}}(x_{m-1}), \ldots, s_{y_1}(x_1)\right).$$

В силу рівності $x+k=\left(\tilde{x}+\tilde{k}+\nu(x_0, k_0), x_0+k_0\right)$, $\alpha, k \in V_{mt}$, справедливе наступне:

$$l_+^{(s)}(\alpha, \beta) = 2^{-q'} \sum_{y_0 \in V_{q'}} \left(2^{-t} \sum_{k_0 \in V_t} \left(2^{-t} \sum_{x_0 \in V_t} (-1)^{\alpha_0 x_0 \oplus \beta_0 s_{y_0}(x_0+k_0)} \right)^2 \right) \times$$

$$\times 2^{-(mq'-q')} \sum_{\tilde{y} \in V_{(mq'-q')}} \left(2^{-(mt-t)} \sum_{\tilde{k} \in V_{(mt-t)}} \left(2^{-(mt-t)} \sum_{\tilde{x} \in V_{(mt-t)}} (-1)^{\tilde{\alpha} \tilde{x} \oplus \tilde{\beta} \tilde{s}\left(\tilde{x}+\tilde{k}+\nu(x_0, k_0), \tilde{y}\right)} \right)^2 \right) =$$

$$= \tilde{\tilde{\Lambda}}(\alpha_0, \beta_0) \times l_+^{\left(\tilde{s}\right)}\left(\tilde{\alpha}, \tilde{\beta}\right) \le \tilde{\tilde{\Lambda}}(\alpha_0, \beta_0) \times \left(\tilde{\tilde{\Lambda}}_+ \right)^{wt(\tilde{\beta})} \le \left(\tilde{\tilde{\Lambda}}_+ \right)^{wt(\tilde{\beta})+wt(\beta_0)} = \left(\tilde{\tilde{\Lambda}}_+ \right)^{wt(\beta)},$$

що і потрібно було довести.

На основі нерівності (60) слідує вірність співвідношення (55):

$$l^{(i)}(\omega_{i-1}, \omega_i) = l_+^{(s)}(\omega_{i-1}, \omega_i M) \le \tilde{\tilde{\Lambda}}_+^{wt(\omega_i M)}.$$

Лема доведена.

Теорема 2. Нехай $\mathfrak{I}$ – r-раундовий БШ, що описується співвідношеннями (1)-(5). Тоді виконуються наступна нерівність:

$$ELP(\Omega) \le \tilde{\tilde{\Lambda}}^{r' B_M + 1} \le \tilde{\Lambda}^{r' B_M + 1} \le \Lambda^{r' B_M + 1}. \quad (61)$$

Доведення.

На основі співвідношень формул (8), (50)-(55) справедлива оцінка:

$$ELP(\Omega) \le \tilde{\tilde{\Lambda}}^{\sum_{i=1}^{r-1} wt(\omega_i M)+wt(\omega_r)}. \quad (62)$$

Оскільки за формулами (40)-(52) $\tilde{\tilde{\Lambda}} \le \tilde{\Lambda} \le \Lambda < 1$, то права частина нерівності буде максимальною тільки коли $\sum_{i=1}^{r-1} wt(\omega_i M) + wt(\omega_r)$ буде мінімальним. У роботі [7] показано, що

$\sum_{i=1}^{r-1} wt(\omega_i M) + wt(\omega_r) \geq r' B_M + 1$, на основі чого слідує нерівність (61). Теорема доведена.

ОЦІНКА ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ РАНДОМІЗОВАНИХ ВУЗЛІВ ЗАМІНИ

Нагадаємо, що в роботі [7] описаний r-раундовий блоковий шифр $\Im'$ (побудований за схемою шифру "Калина-128") із множиною відкритих (шифрованих) повідомлень $V_n = \{0,1\}^n$, множиною раундових ключів $K = V_n$ та сімейством шифруючих перетворень

$$F_k = f_{r,k_r} \circ \ldots \circ f_{1,k_1},\ k = (k_1, \ldots, k_r) \in K^r, \quad (63)$$

де t, p', r' – натуральні числа, $p = 4p'$, $r = 2r' + 1$, $n = pt$.

Раундова функція $f_{i,k}$, для будь-яких $x \in V_n$, $k \in K$, $i \in \overline{1, r}$ описується наступним чином:

$$f_{i,k} = \begin{cases} \varphi(x \oplus k), & \textit{якщо } \mathrm{i} \equiv 1 \pmod 2,\ i < r \\ \varphi\left(x \mathbin{\mathring{+}} k\right), & \textit{якщо } \mathrm{i} \equiv 0 \pmod 2,\ i < r \\ s(x \oplus k), & \textit{якщо } \mathrm{i} = \mathrm{r} \end{cases}. \quad (64)$$

Підстановки φ і s визначаються за формулами:

$$\varphi(x) = s(x) M,\ x \in V_n, \quad (65)$$

$$s(x) = \left(\mathrm{s}_{p-1}(x_{p-1}), \ldots, s_0(x_0)\right),$$

$$x = \left(x_{p-1}, \ldots, x_0\right), \quad (66)$$

де $x_j \in V_t$, s_j – підстановка на множині V_t, $j \in \overline{0, p-1}$, M – оборотна $p \times p$-матриця над полем $\mathrm{GF}(2^t)$, а множення $s(x)$ на M у виразі (65) виконується над цим полем при ототожненні двійкових векторів $s_j(x_j)$ із його елементами. Символи $\oplus$ і $\mathring{+}$ відповідають операціям по координатного булевого додавання двійкових векторів та алгебраїчну операцію (5).

У [7] доведено, що для БШ $\Im'$ (описується співвідношеннями (63)-(66)) виконуються наступні нерівності:

$$EDP(\Omega) \leq \Delta^{r' B_M + 1}, \quad (67)$$

Припустимо, що у БШ Калина-128 додатково ввели раундові ключі, що визначають, які таблиці замін використовуються у раунді. У такому випадку отримаємо БШ $\Im$ (з параметрами $q' = 3$, $q = 48$, $b = 8$). Для такого БШ можна застосовувати нерівності (38) та (61) для розрахунку верхніх аналітичних оцінок стійкості відносно методів диференціального та лінійного криптоаналізу. На

$$ELP(\Omega) \leq \Lambda^{r' B_M + 1}. \quad (68)$$

Якщо у раундову функцію $f_{i,k}$ БШ $\Im'$ (справедливі співвідношення (63)-(66)) ввести додатковий раундовий ключ, що впливає на формування операції підстановок (див. формулу (4)), то фактично БШ $\Im'$ перетвориться на БШ $\Im$ (справедливі співвідношення (1)-(5)). В силу формул (13)-(25), (40)-(52) та нерівностей (38), (61) верхня аналітична оцінка середніх ймовірностей диференціальних та лінійних характеристик БШ $\Im'$ покращиться відповідно у $\left(\tilde{\Delta}/\Delta\right)^{r' B_M + 1}$ та $\left(\tilde{\Lambda}/\Lambda\right)^{r' B_M + 1}$ разів. Зауважимо, що чим більшою буде кількість різних таблиць замін БШ $\Im'$, тим кращими будуть верхні оцінки стійкості до лінійного та диференціального криптоаналізу.

Покажемо ефективність використання рандомізованих вузлів заміни на прикладі БШ Калина-128 [11] (являється конкретним прикладом БШ $\Im'$ з параметрами $t = 8$, $p' = 4$, $r' = 5$, $p = 16$, $r = 11$, $n = 128$, у кожному раунді використовуються 8 різних таблиць замін на множині V_8).

Параметри (15), (16), (42), (43) для кожної таблиці замін алгоритму шифрування Калина-128 наведені у табл. 1. Згідно формул (15)-(17), (42)-(44) та нерівностей (67) і (68) отримаємо: $\Delta = 0,031250$, $\Lambda = 0,0625$, $EDP(\Omega) \leq 2^{-230}$, $ELP(\Omega) \leq 2^{-184}$ ($r' = 5$, $B_M = 9$).

Параметри таблиць замін БШ Калина-128. Таблиця 1

Інд. табл. підстан.	$\Delta_{\oplus}^{(s_j)}$	$\Delta_{+}^{(s_j)}$	$\Lambda_{\oplus}^{(s_j)}$	$\Lambda_{+}^{(s_j)}$
1	0,03125	0,0273438	0,0625	0,0425324
2	0,03125	0,03125	0,0549316	0,0297253
3	0,03125	0,03125	0,0625	0,0297267
4	0,03125	0,0273438	0,0625	0,0551662
5	0,03125	0,03125	0,0625	0,0356412
6	0,03125	0,03125	0,0625	0,0353937
7	0,03125	0,03125	0,0625	0,0296712
8	0,03125	0,03125	0,0625	0,0625

основі формул (21)-(25), для описаних в шифрі Калина таблиць замін [11], були розраховані параметри (23)-(25): $\tilde{\Delta}_{\oplus} = 0{,}015625$, $\tilde{\Delta}_{+} = 0{,}0107422$, $\tilde{\Delta} = 0{,}015625$. Для цих же таблиць замін [11], на основі формул (48)-(52), були розраховані параметри (50)-(52): $\tilde{\Lambda}_{\oplus} = 0{,}0159302$, $\tilde{\Lambda}_{+} = 0{,}0143183$, $\tilde{\Lambda} = 0{,}0159302$.

Оскільки $r' = 5$, $B_M = 9$, то на основі нерівностей (38), (61) були розраховані верхні межі стійкості удосконаленого БШ Калина-128 із рандомізованими вузлами заміни до методів диференціального та лінійного криптоаналізу відповідно: $EDP(\Omega) \le 2^{-276}$, $ELP(\Omega) \le 2^{-274}$. Як видно з розрахунків верхні аналітичні оцінки середніх ймовірностей диференціальних та лінійних характеристик удосконаленого БШ Калина-128 відповідно покращилися у 2^{46} і 2^{90} разів у порівнянні із оригіналом.

ВИСНОВКИ

У роботі отримані аналітичні верхні оцінки параметрів, що характеризують практичну стійкість БШ $\Im$ із рандомізованими вузлами заміни (описуються формулами (1)−(5)) відносно методів лінійного та диференціального криптоаналізу. Показано, що використання рандомізованих вузлів заміни у БШ дозволяє покращити аналітичні верхні оцінки середніх ймовірностей диференціальних та лінійних характеристик відповідно у $\left(\tilde{\Delta}/\Delta\right)^{r'B_M+1}$ та $\left(\tilde{\Lambda}/\Lambda\right)^{r'B_M+1}$ разів у порівнянні із аналогічними оцінками схожих БШ з фіксованими вузлами заміни. На прикладі БШ Калина-128 показано, що використання у ньому рандомізованих вузлів заміни дозволяє покращити верхні межі середніх ймовірностей диференціальних та лінійних характеристик у 2^{46} і 2^{90} разів відповідно.

ЛІТЕРАТУРА

[1]. Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems // Journal of Cryptology. , 1991. , V. 4. , № 1. , P. 3 – 72.

[2]. Lai X., Massey J.L., Murphy S. Markov ciphers and differential cryptanalysis // Advances in Cryptology – EUROCRYPT'91, Proceedings. , Springer Verlag, 1991. , P. 17 – 38.

[3]. Matsui M. Linear cryptanalysis methods for DES cipher // Advances in Cryptology – EUROCRYPT'93, Proceedings, Springer Verlag, 1994., P. 386 – 397.

[4]. Vaudenay S. Decorrelation: a theory for block cipher security // J. of Cryptology., 2003., V. 16., № 4., P. 249 – 286.

[5]. Daemen J., Rijmen V. Statistics of correlation and differentials in block ciphers // http://eprint.iacr.org/ 2005/212.

[6]. Kanda M. Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function // Selected Areas in Cryptography. – SAC 2000, Proceedings., Springer Verlag, 2001, P. 324 – 338.

[7]. Алексейчук А.Н. Оценки практической стойкости блочного шифра «Калина» относительно методов разностного, линейного криптоанализа и алгебраических атак, основанных на гомоморфизмах / А.Н. Алексейчук, Л.В. Ковальчук, Е.В. Скрынник, А.С. Шевцов // Прикладная радиоэлектроника. – 2008. – Т.7, № 3. – С. 203-209.

[8]. Алексейчук А.Н. Верхние оценки несбалансированности билинейных аппроксимаций раундовых функций блочных шифров ГОСТ и "Калина" / А.Н. Алексейчук, А.С. Шевцов // Сучасний захист інформації. – 2010. – № 2. – С. 23 – 30.

[9]. Алексейчук А.Н., Ковальчук Л.В. Верхние границы максимальных значений вероятностей дифференциальных и линейных характеристик шифра Фейстеля, содержащего сумматор по модулю 2m // Прикладная радиоэлектроника. – 2006. – Т. 5. – № 1. – С. 74 – 82.

[10]. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Госстандарт СССР, 1989.

[11]. Горбенко І.Д., Долгов В.І., Олійников Р.В., Руженцев В.І., Михайленко М.С., Горбенко Ю.І., Тоцький О.С., Казьміна С.В. Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікації // Прикладная радиоэлектроника. – 2007. – Т. 6. – № 2. – С. 195 – 208.

[12]. Кузнецов А.А. Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption) / А.А. Кузнецов, Р.В. Сергиенко, А.А. Наумко. // Прикладная радиоэлектроника. – 2007. – Т. 6, № 2. – С. 241-249.

[13]. Vaudenay S. On the security of CS-cipher // Fast Software Encryption. – FSE'99, Proceedings. – Springer Verlag, 1999. – P. 260 – 274.

[14]. Daemen J. Cipher and hash function design strategies based on linear and differential cryptanalysis. – Doctoral Dissertation, 1995.

REFERENCES

[1]. Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems // Journal of Cryptology., 1991., V. 4., № 1., P. 3 – 72.

[2]. Lai X., Massey J.L., Murphy S. Markov ciphers and differential cryptanalysis // Advances in Cryptology – EUROCRYPT'91, Proceedings., Springer Verlag, 1991., P. 17 – 38.
[3]. Matsui M. Linear cryptanalysis methods for DES cipher // Advances in Cryptology, EUROCRYPT'93, Proceedings.– Springer Verlag, 1994., P. 386 – 397.
[4]. Vaudenay S. Decorrelation: a theory for block cipher security // J. of Cryptology., 2003., V. 16., № 4., P. 249 – 286.
[5]. Daemen J., Rijmen V. Statistics of correlation and differentials in block ciphers // http://eprint.iacr.org/ 2005/212.
[6]. Kanda M. Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function // Selected Areas in Cryptography., SAC 2000, Proceedings., Springer Verlag, 2001., P. 324 – 338.
[7]. Alekseychuk A.N. Evaluate the feasibility of "Kalina" block cipher strength on the methods of difference, linear cryptanalysis and algebraic attacks based on homomorphisms / A.N. A.N. Alekseychuk, L.V.Kovalchuk, E.V.Skrinnik, A.S. Shevtsov // Applied radio-electronics., 2008., V.7, № 3., P. 203-209.
[8]. Alekseychuk A.N. Upper bounds imbalance of bilinear approximations of round function block cipher GOST and "Kalina" / A.N. Alekseychuk, A.S. Shevtsov // Modern information security, 2010, № 2, P. 23 - 30.
[9]. Alekseychuk A.N., Kovalchuk L.V. The upper boundary of the maximum values of the probabilities of differential and linear characteristics of the Feistel cipher containing the adder modulo 2m / / Applied radio-electronics, 2006, V. 5, № 1, P. 74 - 82.
[10]. GOST 28147-89. Information processing systems. Cryptographic Security. Cryptographic transformation algorithm. - Moscow: State Standard of the USSR, 1989.
[11]. Gorbenko I.D., Dolgov V.I., Oliynikov R.V., Ruzhentsev V.I., Mikhaylenko M.S, Gorbenko Yu.I., Totsky O.S., Kazmina S.V. Promising symmetric block cipher "Kalina" - main provisions and specifications/ Applied radio-electronics, 2007, V. 6, № 2., P. 195 - 208.
[12]. Kuznetsov A.A. Symmetric encryption algorithm ADE (Algorithm of Dynamic Encryption) / A.A. Kuznetsov, R.V. Sergienko, A.A. Naumko // Applied radio-electronics., 2007, V. 6, № 2, P. 241-249.
[13]. Vaudenay S. On the security of CS-cipher // Fast Software Encryption. – FSE'99, Proceedings, Springer Verlag, 1999, P. 260 – 274.
[14]. Daemen J. Cipher and hash function design strategies based on linear and differential cryptanalysis, Doctoral Dissertation, 1995.

ВЕРХНИЕ ОЦЕНКИ СТОЙКОСТИ БЛОКОВЫХ ШИФРОВ С РАНДОМИЗИРОВАННЫМИ УЗЛАМИ ЗАМЕНЫ ОТНОСИТЕЛЬНО МЕТОДОВ ЛИНЕЙНОГО И ДИФЕРЕНЦИАЛЬНОГО КРИПТОАНАЛИЗА

Теория анализа и обоснования стойкости блочных шифров с фиксированными узлами замены относительно методов линейного и дифференциального криптоанализа довольно сильно развита. Существуют также блочные шифры, в которых узлы замены определяются раундовими ключами. Понятно, что использование рандомизированных узлов замены в шифрах затрудняет их криптоанализ, однако количественно это трудно оценить. Учитывая это, актуальной задачей является выведение аналитических выражений, позволяющих доказать практическую стойкость блочных шифров с рандомизированными узлами замены относительно методов линейного и дифференциального криптоанализа и позволят сделать количественную оценку их эффективности. В работе получены аналитические верхние оценки параметров, характеризующих практическую стойкость блочных шифров с рандомизированными узлами замены относительно методов линейного и дифференциального криптоанализа. Указанные оценки обобщают ранее известные на блочные шифры с рандомизированными узлами замены и позволяют обосновывать повышение стойкости относительно указанных методов криптоанализа.

Ключевые слова: криптография, блочный шифр, линейный криптоанализ, дифференциальный криптоанализ, рандомизированные узлы замены.

UPPER BOUNDS OF BLOCK CIPHERS RESISTANCE WITH RANDOMIZED NODES CHANGE TO LINEAR AND DIFFERENTIAL CRYPTANALYSIS METHODS

The theory analysis and basis of block ciphers resistance with fixed replacement nodes regard to the linear and differential cryptanalysis is quite developed.There are also block ciphers in which the nodes are defined by replacing the round key. It is clear that the using of randomized replacement nodes in ciphers makes difficult cryptanalysis for them, but it is difficult to assess quantitatively. Given this, the urgent task is to take the analytical expressions that allow to prove the practical resistance of block ciphers with randomized replacement nodes regard to the linear and differential cryptanalysis and will make a quantitative assessment of their effectiveness. In this paper obtain analytical upper bounds for the parameters characterizing the practical resistance of block ciphers with randomized replacement nodes regard to the linear and differential cryptanalysis. These estimates generalize previously known to block ciphers with randomized replacement

nodes can explain increase resistance regard to these methods of cryptanalysis.
Index words: cryptography, block cipher, linear cryptanalysis, differential cryptanalysis, randomized replacement nodes.

Кінзерявий Василь Миколайович, асистент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: v.kinzeryavyy@gmail.com

Кинзерявый Василий Николаевич, асистент кафедры безопасности информационных технологий Национального авиационного университета.
Kinzeryavyy Vasyl, Assistant of Academic Department of IT-Security, National Aviation University.

УДК 004.056.5(045)

АНАЛИЗ И ОЦЕНИВАНИЕ РИСКОВ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Светлана Казмирчук

Для построения систем менеджмента информационной безопасности, комплексных систем защиты информации и других систем безопасности необходимо проводить анализ и оценивание рисков. Существующие средства оценки в подавляющем большинстве основаны на статистических подходах. Во многих странах, как на уровне предприятий, так и на государственном уровне подобная статистика не ведется. Это ограничивает возможности существующих средств, например, по использованию различных типов входящих данных для оценки. Известный инструментарий не дает возможности применения для анализа и оценки рисков широкого спектра начальных параметров. На основе предложенного автором метода анализа и оценки рисков, который на основе использования модели интегрированного представления параметров риска, позволяет проводить оценивание в детерминированных условиях, с использованием десяти параметров, которые могут быть представлены, как в числовой, так и лингвистической форме, было реализовано программную систему анализа и оценки рисков потери информационных ресурсов. Для верификации разработанного программного продукта было смоделировано несколько различных ситуаций относительно защищенности информационных ресурсов, после чего проведен анализ и оценивание рисков при каждой такой ситуации. Полученные результаты исследования подтверждают адекватность реагирования программного средства на изменение значений оценочных компонент при разных условиях среды оценивания, а значение риска существенно не изменяется при изменении базиса оценочных компонент.
Ключевые слова: *риск, анализ риска, оценка риска, система анализа и оценки риска, параметры риска, безопасность информационных ресурсов.*

Параллельно со стремительным развитием и внедрением IT-технологий во все сферы деятельности человечества, растет и число угроз связанных с нарушением конфиденциальности, целостности и доступности информационных ресурсов (ИР), которые обрабатываются с помощью этих технологий. Поэтому безопасность таких ресурсов становится приоритетной задачей, как для предпринимательской деятельности, так и для государства в целом.

На сегодняшний день решать такую задачу целесообразно с помощью комплексного подхода к обеспечению информационной безопасности (ИБ) ИР. Одним из этапов построения комплексной системы защиты информации (КСЗИ) является разработка модели угроз [7], методология создания которой включает в себя анализ и оценивание рисков (АОР) [6]. На данный момент существует необходимость в эффективных средствах, которые позволили бы в автоматизированном режиме осуществлять АОР. Для решения такой задачи, используя методологию синтеза систем АОР потерь ИР [2], которая основана на логико-лингвистическом подходе, известных методах [3] и модели интегрированного представления параметров риска [1], было предложено новое соответствующее структурное решение системы оценивания [4]. Для практического при-