Аналіз підсумкової таблиці з врахуванням практичних припущень ($p_0 >> p_1,p_2,p_3$; $p_1 \approx p_2 \approx p_3$) показує, що відносна автокоригуюча здатність більш висока у ЕА з повністю визначеною системою переходів (типів *S,R,E,JK*). Найнижчий показник *L* для ЕА типу *SRT* обумовлений невизначеністю половини всіх можливих переходів цього ЕА.

Література: ***1.*** *Тарасенко-Клятченко О. В. Сравнительный анализ корректирующих свойств переключательных функций // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні.- К.: 2002, вип.5, с. 189…194.* ***2.*** *Тарасенко В. П. Метод оценки автокорректирующих свойств поразрядных логических операций/ В.П. Тарасенко, О.В. Тарасенко-Клятченко// Радиоэлектроника и информатика. -2001. - № 1(14). -С.83-86.* ***3.*** *Самофалова К. Г., Цифровые ЕВМ. Теория и проектирование / Самофалова К. Г., Корнійчук В. И., Тарасенко В. П. // К.: «Вища школа», 1989, - 424 с.* ***4.*** *Компьютерная схемотехника (краткий курс)/ Процюк Р. О., Корнійчук В. И., Кузьменко П. В., Тарасенко В. П. - К.: вид-во «Корнійчук», 2006, - 432 с.* ***5.*** *Щербаков Н. С. Достоверность работы цифровых устройств /Н. С. Щербаков; –М.: «Машиностроение», 1989. -224 с.* ***6.*** *Кулик А. Я. Адаптивні алгоритми передавання інформації / Вінниця: «Універсум», 2003, -213с.* ***7.*** *Отказобезопасные информационно-управляющие системы на программируемой логике/Е. С. Бахмач, А. Д. Герасименко, В. А. Головир, А. А. Сиора, В. В. Скляр, В. И. Токарев, В. С. Харченко; -Харьков-Кировоград.: -Изд-во НАУ „ХАИ” и НПП „Радий”, 2008. -380 с* ***8.*** *Бондаренко М. Ф., Кривуля Г. Ф., Рябцев В. Г., Фрадков С. О., Хаханов В. И. Проектирование и диагностика компьютерных сетей и систем / -К.: НМЦВО, 2000, -306 с.*

УДК 621.391:519.2

ЗАСТОСУВАННЯ ТЕОРІЇ УЗАГАЛЬНЕНИХ МАРКІВСЬКИХ ШИФРІВ ДО ОЦІНЮВАННЯ СТІЙКОСТІ СУЧАСНИХ БЛОКОВИХ АЛГОРИТМІВ ШИФРУВАННЯ ДО МЕТОДІВ РІЗНИЦЕВОГО КРИПТОАНАЛІЗУ

Людмила Ковальчук, Сергей Пальченко*, Леонид Скрипник
*ІСЗЗІ НТУУ «КПІ», *ФТІ НТУУ «КПІ»*

Анотація: **Представлено теоретичне підґрунтя для оцінювання стійкості узагальнених марківських шифрів відносно різницевого криптоаналізу. Даний застосовано інструментарій для оцінювання стійкості БШ «Мухомор».**
Summary: **In this article presented theory for evaluation of Generalized Markov Cipher resistance. And use this method for evaluation of "Muhomor" block cipher.**
Ключові слова: **Безпека інформації, криптологія, блочні алгоритми шифрування, диференціальний криптоаналіз, узагальнені марківські шифри, «Калина».**

I Вступ

У зв'язку з інтенсивним розвитком математичних методів у сфері криптоаналізу та захисту інформації багато криптографічних систем та протоколів, що застосовуються, вже не задовольняють сучасним вимогам. Наслідком цього є низка програм та конкурсів, зокрема міжнародних, таких як AES [1], NESSIE [2] та інші. Аналогічні процеси почали відбуватися і в Україні. Про це свідчить конкурс на новий Національний стандарт симетричного блочного шифрування, що розпочався кілька років тому. У конкурсі брали участь 5 алгоритмів. На даний момент переможця не визначено, але, на думку авторів даної роботи, найбільш перспективними є алгоритми «Калина» [3] та «Мухомор» [4], розроблені Харківським національним університетом радіоелектроніки.

У даній роботі основна увага приділяється формалізації опису та дослідженню основних властивостей стійкості до різницевого криптоаналізу шифру «Мухомор». Детальний аналіз стійкості до різницевого та декількох інших видів криптоаналізу шифру «Калина» було представлено у роботах [5, 6]. Специфіка даного алгоритму полягає в тому, що він, як і діючий стандарт блокового шифрування ГОСТ 28147-89 [7], не є марківським шифром (МШ). Тому до нього не може бути застосована класична теорія оцінювання стійкості, яку побудовано і розвинуто в роботах [8 – 12].

До недавнього часу взагалі не існувало робіт, в яких були отримані науково обґрунтовані оцінки стійкості немарківських блокових шифрів (БШ) до різницевого та лінійного криптоаналізу. Найперша з таких робіт [13] з'явилась у 2004 році. Її результати були допрацьовані, систематизовані та узагальнені у

[14, 15]. Далі, в [16] вперше було введено поняття узагальненого марківського шифру (УМШ) та отримано результати, що узагальнюють відомі результати для МШ.

У даній роботі отримали подальший розвиток результати роботи [16]. Введено загальніше, порівняно з [16], означення УМШ у широкому сенсі; досліджено основні різницеві властивості таких шифрів; показано, що шифри ГОСТ 28147-89 та «Мухомор» є УМШ у широкому сенсі. Останнє твердження дає можливість оцінити зверху середню ймовірність різницевої характеристики шифру через середню ймовірність раундових диференціалів, що дозволяє звести дослідження різницевих властивостей шифру до дослідження різницевих властивостей раундової функції.

У роботі також виявлено низку некоректних тверджень, наведених в [17, 18], щодо різницевих властивостей раундової функції шифру. Замість деяких з них надані та доведені правильні формулювання. Але слід зазначити, що оцінки стійкості алгоритму, наведені у даній роботі, хоч і є повністю науково обґрунтованими, але можуть допускати суттєве підсилення.

Робота містить також глобальну методологію побудови оцінок стійкості до різницевого криптоаналізу УМШ (у широкому сенсі) типу «Мухомор», але детальне дослідження різницевих властивостей раундових функцій ще не завершено.

II Означення узагальненого марківського шифру (УМШ). Побудова оцінок практичної стійкості УМШ до різницевого криптоаналізу

II.1 Основні позначення та допоміжні твердження

Нехай $\Im$ – r-раундовий БШ з раундовою функцією $f_{k_i} : G \to G,\ i = \overline{1,r}$, де $k_i \in V_n$ – ключ i-го раунду, $V_n = \{0,1\}^n$, G – довільна скінченна група.

Позначимо $k = (k_1, k_2, \ldots, k_r)$. Тоді відображення $\Im_k : G \to G$ задається наступним чином: $\Im_k(x) = f_{k_r} \circ f_{k_{r-1}} \circ \ldots f_{k_1}(x),\ \forall x \in G$. Також введемо позначення

$$M = (\mu_0, \ldots, \mu_r), \tag{1}$$

де $\mu_i : G \times G \to G$ – групові операції на G, $\mu_i(a,b) = a \circ_i b,\ a,b \in G,\ i = \overline{0,r}$. Нейтральний елемент групи G відносно операції μ_i будемо позначати 0_i.

Означення 2.1: узагальненою диференціальною характеристикою (УДХ) шифру $\Im$ назвемо послідовність

$$(\Omega, M) = ((\omega_0, \mu_0), (\omega_1, \mu_1), \ldots, (\omega_{r+1}, \mu_{r+1})), \tag{2}$$

де $\omega_i \in G \setminus \{0_i\},\ i = \overline{1,r}$.

Означення 2.2: середньою (по ключах) ймовірністю УДХ (2) назвемо величину

$$EDP(\Omega, M) = 2^{-nr} \sum_{k \in (V_n)^r} \frac{1}{|G|} \sum_{x_0 \in G} \prod_{i=1}^{r} \delta(f_{k_i}(x_{i-1} \circ_{i-1} \omega_{i-1}) \circ_i f_{k_i}(x_{i-1})^{-1}, \omega_i), \tag{3}$$

де $x_i = f_{k_i}(x_{i-1})$, а під $f_{k_i}(x_{i-1})^{-1}$ розуміється елемент, обернений до $f_{k_i-1}(x_{i-1})$ відносно операції $\circ_i$.

Ми будемо розглядати лише такі Ω, що $EDP(\Omega, M) \neq 0$.

Зауваження 2.3: вираз (3) також може бути переписано у вигляді

$$EDP(\Omega, M) = \frac{1}{|G|} \sum_{x_0 \in G} \prod_{i=1}^{r} \left\{ 2^{-n} \sum_{k \in V_n} \delta(f_{k_i}(x_{i-1} \circ_{i-1} \omega_{i-1}) \circ_i f_{k_i}(x_i)^{-1}, \omega_i) \right\} \tag{4}$$

Позначимо

$$d^f_{\mu_1,\mu_2}(x;\alpha x;\alpha = 2^{-n} \sum_{k \in V_n} \delta(f_k(x \circ \alpha) \circ f_k(x)^{-1}, \beta) \tag{5}$$

$$d^f_{\mu_1,\mu_2}(\alpha\alpha,\beta = \frac{1}{|G|} \sum_{x \in G} d^f_{\mu_1,\mu_2}(x;\alpha x;\alpha. \tag{6}$$

Якщо $\mu_1 = \mu_2 = \mu$, будемо також використовувати позначення $d^f(x;\alpha x;\alpha$ і $d^f(\alpha,\beta)$.

Означення 2.4: величину (5) будемо називати середньою ймовірністю раундового диференціалу (α,β) в точці x відносно операцій μ_1,μ_2; величину (6) – середньою ймовірністю раундового диференціалу $(\alpha\alpha,\beta$ відносно операцій μ_1,μ_2.

В позначеннях (5), (6)

$$EDP(\Omega,M)=\frac{1}{|G|}\sum_{x_0\in G}\prod_{i=1}^{r}d^{f}_{\mu_{i-1},\mu_i}(x_{i-1};\omega_{i-1},\omega_i). \tag{7}$$

Зауваження 2.5: якщо $\mu_1=\mu_2=\mu$, де $\mu_i(a,b)=a\circ_i b$, $a,b\in G$ і шифр $\Im$ є марківським відносно операції μ, то, відповідно до означення марківського шифру (МШ) ([9]),

$$d^{f}(x;\alpha,\beta)=d^{f}(0;\alpha,\beta),\ \forall x\in G,$$

звідки

$$d^{f}(\alpha,\beta)=d^{f}(0;\alpha,\beta). \tag{8}$$

Зрозуміло також, що в цьому випадку

$$EDP(\Omega)=\prod_{i=1}^{r}d^{f}(\omega_{i-1},\omega_i)=\prod_{i=1}^{r}d^{f}(0;\omega_{i-1},\omega_i), \tag{9}$$

тобто середня ймовірність раундового диференціалу в точці x однакова для $\forall x\in G$, і середня ймовірність УДХ (Ω) дорівнює добутку середніх ймовірностей відповідних раундових диференціалів в точці x.

Прикладом шифру $\Im$, для якого справедливими є співвідношення (7)-(9), може бути будь-який БШ з раундовою функцією

$$f_k(x)=\varphi_{k^{(1)}}(x*k^{(2)}), \tag{10}$$

де $k=(k^{(1)},k^{(2)})$, $k^{(1)}\in V_n$, $x,k^{(2)}\in V_m$, $\varphi_{k^{(1)}}:V_m\to V_m$ - бієкція $\forall k^{(1)}$, $*$-операція на V_m, оскільки такий шифр є марківським відносно операції "$*$".

На поточний момент досить добре розроблена загальна теорія оцінювання практичної стійкості марківських (як правило, для $\mu=\oplus$) шифрів відносно різницевого (а також і лінійного) криптоаналізу; одними з основоположних робіт в цьому напрямку можна вважати [8 – 12]. Як правило, при побудові оцінок використовуються наслідки формули (9):

$$\max_{\Omega}EDP(\Omega)\le\max_{\Omega_1}EDP(\Omega_1)\max_{\Omega_2}EDP(\Omega_2),\ \Omega=(\Omega_1,\Omega_2), \tag{11}$$

$$\max_{\Omega}EDP(\Omega)\le(\max_{\omega_1,\omega_2\ne 0}d^{f}(\omega_1,\omega_2))^{r}, \tag{12}$$

а наслідком формули (11) в свою чергу є оцінка:

$$\max_{\Omega}EDP(\Omega)\le\max_{\Omega}p_s^{(\Omega)}, \tag{13}$$

де $\#\Omega$ - мінімально можлива кількість активних *S*-блоків в Ω, $p_s=\max_{s\in S}\max_{\omega_1,\omega_2}d^{s}(\omega_1,\omega_2)$, де *S* – множина *S*-блоків шифру (якщо його раундова функція є композицією лінійних перетворень і блоку підстановок).

Що стосується немарківських БШ, то властивість (9) для них, загалом, не виконується, що унеможливлює отримання оцінок вигляду (11) – (13) аналогічними методами. При побудові аналогів цих оцінок необхідно враховувати залежність (5) від *x*.

Твердження 2.6: для величини *EDP(Ω, M)*, заданої формулою (3), справедливі наступні нерівності:

$$EDP(\Omega,M)\le\prod_{i=1}^{r}\max_{x\in G}d^{f}_{\mu_{i-1},\mu_i}(x;\omega_{i-1},\omega_i), \tag{14}$$

$$\max_{\Omega,M}EDP(\Omega,M)\le\prod_{i=1}^{r}\max_{x\in G}\max_{\substack{\omega_{i-1},\omega_i\\ \omega_{i-1}\ne 0_{i-1}\\ \omega_i\ne 0_i}}d^{f}_{\mu_{i-1},\mu_i}(x;\omega_{i-1},\omega_i). \tag{15}$$

Доведення: для простоти викладення доведемо (14) для двораундової характеристики

$$(\Omega, M) = ((\omega_0, \mu_0), (\omega_1, \mu_1), (\omega_2, \mu_2)),$$

для якої формула (15) є прямим наслідком (14).

Відповідно до (7):

$$EDP(\Omega, M) = \frac{1}{|G|} \sum_{x_0 \in G} d^f_{\mu_1,\mu_2}(x_0; \omega_1, \omega_2) d^f_{\mu_2,\mu_3}(x_1; \omega_2, \omega_3),$$

де $x_1 = f_{k_1}(x_0)$, $k_1 \in V_n$ - ключ першого раунду. Тоді

$$EDP(\Omega, M) \le \frac{1}{|G|} \sum_{x_0 \in G} \max_{x \in G} d^f_{\mu_1,\mu_2}(x; \omega_1, \omega_2) \cdot \max_{x \in G} d^f_{\mu_2,\mu_3}(x; \omega_2, \omega_3) =$$

$$= \max_{x \in G} d^f_{\mu_1,\mu_2}(x; \omega_1, \omega_2) \cdot \max_{x \in G} d^f_{\mu_2,\mu_3}(x; \omega_2, \omega_3).$$

Доведення закінчене.

Наявність в (14), (15) додаткового параметра $x \in G$ істотно ускладнює побудову чисельних оцінок для $EDP(\Omega, M)$, і, в той же час, робить отримані оцінки більш грубими, а в деяких випадках навіть тривіальними. Тому, як правило, вони не можуть бути використані на практиці. Таким чином, для немарківських БШ, до виникнення робіт [13 – 16], була практично відсутня теорія побудови оцінок стійкості до диференціального (а також і лінійного) криптоаналізу. Варто відмітити, що в роботах [19 – 26] були отримані деякі результати в даній області, проте вони не були повністю теоретично обґрунтовані.

II.2. Означення узагальненого марківського шифру

Властивості УМШ. Приклади. Побудова оцінок практичної стійкості до різницевого криптоаналізу. Нехай задано деяке відображення $f: V_n \times G \to G$, таке, що при кожному $k \in V_n$ відображення $f(k,x) := f_k(x)$ є бієкцією на G. З даним відображенням будемо пов'язувати множину матриць M_x розмірності $|G| \times |G|$, $x \in G$. Елементами матриці M_x є $a^x_{\alpha,\beta} \in [0,1]$, $\alpha,\beta \in G$, де $a^x_{\alpha,\beta} \in [0,1] = d^f_{\mu_1,\mu_2}(x;\alpha x \beta)$. (Припускається, що на групі G зафіксовано деякий лінійний порядок; зокрема, якщо $G = V_m$, то бітові вектори природнім чином відповідають цілим числам від 0 до $2^m - 1$).

Позначимо через П множину підстановочних матриць розмірності $|G| \times |G|$.

Означення 2.7: відображення $f: V_n \times G \to G$, введене вище, будемо називати узагальненим марківським відображенням (УМВ) (відносно операцій μ_1, μ_2), якщо $\forall x, x' \in G \ \exists \pi, \pi' \in \Pi$:

$$\pi_x \cdot M_x = \pi'_{x'} \cdot M_{x'} \qquad (16)$$

(під множенням в (16) розуміється звичайне матричне множення, яке в даному випадку зводиться до перестановки рядків матриць M_x і $M_{x'}$).

Лема 2.8 (властивість УМВ): для УМВ f в наших позначеннях справедлива рівність:

$$\forall \beta \in G \quad \max_{\substack{x, \alpha \in V_n \\ \alpha \ne 0}} d^f_{\mu_1,\mu_2}(x; \alpha, \beta) = \max_{\substack{\alpha \in V_n \\ \alpha \ne 0}} d^f_{\mu_1,\mu_2}(0; \alpha, \beta).$$

Доведення випливає безпосередньо з означення УМВ, а саме з того факту, що стовпчики матриць M_x і M_0 з номером β відрізняються лише деякою перестановкою елементів. Отже, максимальний елемент у стовпчиках з однаковим номером матриць M_x і M_0 є однаковим, що й стверджується у лемі.

Означення 2.9: БШ $\Im$ будемо називати УМШ (відносно операцій μ_1, μ_2) у вузькому сенсі, якщо його раундова функція є узагальненим марківським відображенням (УМВ) відносно цих операцій.

БШ $\Im$ будемо називати УМШ у вузькому сенсі відносно послідовності операцій *M*, якщо шифр $\Im$ є УМШ у вузькому сенсі відносно μ_{i-1}, μ_i, $i = \overline{1, r}$.

Зауваження 2.10. Якщо в (3.16) $G = V_m$, $\mu_1 = \mu_2 = XOR$, а $\pi = \pi' = Id$, $\forall x, x' \in G$, то дане означення співпадає з класичним означенням марківського БШ [8].

Означення 2.7 еквівалентне наступному: $\forall i = \overline{1,r}$, $\forall x \in G$ $\exists \sigma_{x,\mu_{i-1}}$ - перестановка на *G*, така, що $\forall \alpha, \beta \in G$:

$$d^f_{\mu_{i-1},\mu_i}(x;\alpha,\beta) = d^f_{\mu_{i-1},\mu_i}(0_{i-1};\sigma_{x,\mu_i}(\alpha),\beta). \tag{17}$$

Зокрема, якщо $\mu_{i-1} = \mu_i = \mu$, то

$$d^f(x;\alpha,\beta) = d^f(0\ ;\sigma_x(\alpha),\beta). \tag{18}$$

Наступна теорема демонструє виконання для УМШ деяких оцінок, отриманих раніше для МШ.

Теорема 2.11: для будь-якого УМШ у вузькому сенсі $\Im$ (відносно операцій *M*) справедливі наступні твердження.

$$1.\ \forall x, \omega' \in G:\ \max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(x;\omega,\omega') = \max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(0;\omega,\omega'),\ \forall i = \overline{1,r}. \tag{19}$$

$$2.\ \forall x, \omega' \in G:\ \max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(\omega,\omega') \le \max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(x;\omega,\omega') = \max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(0;\omega,\omega'),$$
$$\forall i = \overline{1,r}. \tag{20}$$

$$3.\ EDP(\Omega,M) \le \prod_{i=1}^{r} \max_{\omega \in G} d^f_{\mu_i - 1,\mu_i}(0;\omega\omega_i). \tag{21}$$

$$4.\ \max_{\Omega} EDP(\Omega DP \le \prod_{i=1}^{r} \max_{\substack{\omega,\omega' \in G \\ \omega' \ne 0_i}} d^f_{\mu_{i-1},\mu_i}(0;\omega\omega,\omega). \tag{22}$$

5. Якщо з умови $EDP(\Omega D \ne 0$ випливає умова $\omega_{i-1} \in U,\ \omega_i \in V,\ i \in I$, для деяких $I \subset \{1,...,r\}$, $U, V \subset G$, то

$$\max_{\Omega} EDP(\Omega D \le \prod_{i \in I} \max_{\substack{\omega_{i-1} \in U, \\ \omega_i \in V}} d^{\varphi}(0;\omega_{i-1},\omega_i) \prod_{i \notin I} \max_{\omega_{i-1},\omega_i \in G} d^{\varphi}(0;\omega_{i-1},\omega_i). \tag{23}$$

Доведення: формула (19) випливає безпосередньо з означення УМШ і п. 2. зауваження 2.8, оскільки

$$\max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(x;\omega x\omega') = \max_{\omega_0} d^f_{\mu_{i-1},\mu_i}(0;\omega_0,\omega'),$$

де $\omega_0 = \sigma_{x,\mu_{i-1}}(\omega)$, $x \in G$, $i = \overline{1,r}$.

Формула (20) випливає з (19), оскільки

$$\max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(\omega,\omega') = \max_{\omega \in G} \frac{1}{|G|} \sum_{x \in G} d^f_{\mu_{i-1},\mu_i}(x;\omega,\omega') \le \le \frac{1}{|G|} \sum_{x \in G} \max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(x;\omega;\omega') = \max_{\omega \in G} d^f_{\mu_{i-1},\mu_i}(0;\omega,\omega')$$

Формула (21) випливає з твердження 2.1 і п. 2. зауваження 2.8, а (22), (23) є наслідками формули (21). Доведення завершене.

Зауваження 2.12: останнє твердження теореми може бути узагальнене на випадок декількох підмножин $\{1,...,r\}$ та G.

Наступна теорема описує деякі важливі підкласи класу УМШ.

Теорема 2.13: БШ $\Im$, який має вигляд (10), є УМШ у вузькому сенсі відносно будь-якої послідовності операцій, визначеної в (1), на V_m.

Доведення: для фіксованого $x \in V_m$ розглянемо вираз

$$2^{-(m+n)} \sum_{\substack{k^{(2)} \in V_m \\ k^{(1)} \in V_n}} \delta(f_k(x \circ_1 \omega) \circ_2 f_k(x)^{-1}, \omega') = = 2^{-(m+n)} \sum_{\substack{k^{(2)} \in V_m \\ k^{(1)} \in V_n}} \delta(\varphi_{k^{(1)}}((x \circ_1 \omega) * k^{(2)}) \circ_2 \varphi_{k^{(1)}}(x * k^{(2)})^{-1}, \omega')$$

Запишемо $x \circ_1 \omega$ в наступному вигляді: $x \circ_1 \omega = \nu(x,\omega) * \omega * x$, де $\nu(x,\omega) = (x \circ_1 \omega) * x^{-1} * \omega^{-1}$.

Відмітимо, що відображення $\omega \to \omega_0 = \nu(x,\omega) * \omega$ при фіксованому $x \in V_m$ є перестановкою на V_m. Дійсно, якщо $\nu(x,\omega_1) * \omega_1 = \nu(x,\omega_2) * \omega_2$, то

$$(x \circ_1 \omega_1) * x^{-1} * \omega_1^{-1} * \omega_1 = (x \circ_1 \omega_2) * x^{-1} * \omega_2^{-1} * \omega_2,$$

звідки $x \circ_1 \omega_1 = x \circ_1 \omega_2$, $\omega_1 = \omega_2$.

Позначимо перестановку $\omega \to \nu(x,\omega) * \omega$ через $\sigma_x(\omega)$. З наведених вище міркувань випливає, що $\forall x \in V_m$:

$$2^{-(m+n)} \sum_{\substack{k^{(2)} \in V_m \\ k^{(1)} \in V_n}} \delta(\varphi_{k^{(1)}}((x \circ_1 \omega) * k^{(2)}) \circ_2 \varphi_{k^{(1)}}(x * k^{(2)})^{-1}, \omega') =$$

$$= 2^{-(m+n)} \sum_{\substack{k^{(2)} \in V_m \\ k^{(1)} \in V_n}} \delta(\varphi_{k^{(1)}}(\nu(x,\omega) * x * \omega * k^{(2)}) \circ_2 \varphi_{k^{(1)}}(x * k^{(2)})^{-1}, \omega') =$$

$$= 2^{-(m+n)} \sum_{\substack{k^{(2)} \in V_m \\ k^{(1)} \in V_n}} \delta(\varphi_{k^{(1)}}(\sigma_x(\omega\omega * k^{(2)}) \circ_2 \varphi_{k^{(1)}}(k^{(2)})^{-1}, \omega\omega),$$

що й завершує доведення теореми.

Наступні теореми описують деякі важливі класи УМШ.

Теорема 2.14: ітеративний БШ $\Im$, який має вигляд (10), є УМШ у вузькому сенсі відносно будь-якої послідовності *M* групових операції на V_m.

Доведення: для фіксованого $x \in V_m$ розглянемо вираз

$$2^{-m} \sum_{k \in V_m} \delta(f_k(x \circ_1 \alpha) \circ_2 f_k(x)^{-1}, \beta) = 2^{-m} \sum_{k \in V_m} \delta(\varphi((x \circ_1 \alpha) * k) \circ_2 \varphi(x * k)^{-1}, \beta).$$

Помітимо, що $x \circ_1 \alpha = \alpha' * x$, де $\alpha' = (x \circ_1 \alpha) * x^{-1}$, причому легко бачити, що відображення $\alpha \to \alpha'$ при довільному фіксованому x є перестановкою на V_m. Таким чином,

$$\forall x \in V_m \quad 2^{-m} \sum_{k \in V_m} \delta(f_k(x \circ_1 \alpha) \circ_2 f_k(x)^{-1}, \beta) = 2^{-m} \sum_{k \in V_m} \delta(\varphi(\sigma_x(\alpha) * x * k) \circ_2 \varphi(x * k)^{-1}, \beta),$$

де $\sigma_x(\alpha) = (x \circ_1 \alpha) * x^{-1}$. Виконання умови $\sigma_x(0_1) = 0_2 \quad \forall x \in V_m$ випливає з означення $\sigma_x(\alpha)$. Доведення завершено.

Зауваження: 2.15: теореми 2.13, 2.14 справедливі і у загальнішому випадку, а саме для такого шифру $\Im$, у якого раундові функції мають вигляд (10), але є різними: наприклад, відрізняються операцією **"*"** у ключовому суматорі. У цьому випадку в теорему 2.13 необхідно внести відповідні зміни щодо операції у ключовому суматорі. Прикладом БШ з різними операціями у раундах є кандидат у Національний стандарт БШ шифр "Калина" [3].

Далі наведемо означення, що є більш загальним за означення 1.5.

Означення 2.16: БШ $\Im$ з раундовою функцією $f_k : G \to G, \quad k \in V_n$, будемо називати узагальненим марківським шифром у широкому сенсі (відносно операцій μ_1, μ_2 на G), якщо існують відображення $\psi : G \times G \to \{0,1\}$, $\varphi_k : G' \to G', \quad k \in V_n$, та функції

$$x' : G \to G', \alpha' : G \times G \to G', \beta' : G \times G \to G'.$$

де G' – деяка група, μ_1', μ_2' – операції на ній (також будемо їх позначати $''*'', \quad ''\circ''$), такі, що:

$$\forall x, \alpha, \alpha \in G \quad \exists\, x' = x'(x), \alpha' = \alpha'(\alpha\alpha, \beta)\beta' = \beta'(\alpha\alpha, \beta \in G'):$$

$$d^{f}_{\mu_1,\mu_2}(x; \alpha x; \alpha = \psi(\alpha, \beta) d^{\varphi}_{\mu_1',\mu_2'}(x'(x), \alpha'(\alpha\alpha, \beta)\beta'(\alpha\alpha, \beta), \tag{24}$$

і при цьому відображення φ є узагальненим марківським.

БШ $\Im$ будемо називати УМШ у широкому сенсі відносно послідовності операцій *M*, якщо шифр $\Im$ є УМШ у широкому сенсі відносно μ_{i-1}, μ_i, $i = \overline{1,r}$. При цьому групи G', групові операції μ_1', μ_2',

відображення ψ, φ, а також функції $x'(x), \alpha'(\alpha,\beta), \beta'(\alpha,\beta)$ можуть бути різними для різних раундів, залежно від послідовності операцій M. Надалі будемо розглядати УМШ у широкому сенсі лише в спрощеному випадку, коли всі операції в послідовності M однакові (здебільшого це буде операція побітового додавання). У цьому випадку всі названі вище об'єкти є однаковими для всіх раундів.

Зауваження 2.17. 1. Очевидно, що для УМШ у широкому сенсі умова $\psi(\alpha,\beta)=1$ є необхідною для виконання умови $EDP(\Omega,M)\neq 0$.

2. УМШ у вузькому сенсі завжди є УМШ у широкому. Дійсно, в цьому випадку

$$\psi\equiv 1,\ G'=G,\ \mu_1'=\mu_1,\ \mu_2'=\mu_2,\ \varphi_k=f_k,\quad k\in V_n,\ x'=x,\alpha'=\alpha,\beta'=\beta.$$

Наступна теорема є аналогом теореми 2.9 для УМШ у широкому сенсі.

Теорема 2.18: для будь-якого УМШ у широкому сенсі $\Im$ справедливі наступні твердження:

1. $\forall \alpha,\beta\in G$:

$$\max_{x\in G} d^f(x;\alpha x\beta)\le \max_{x'\in G'} d^{\varphi}\left(0;\alpha'(\alpha,\beta),\beta'(\alpha,\beta)\right); \tag{25}$$

2. $\forall \alpha,\beta\in G$:

$$\max_{x\in G} d^f(\chi;\alpha,\beta)\le \max_{\alpha'\in G'} d^{\varphi}\left(0;\alpha',\beta'(\alpha,\beta)\right)=\max_{\alpha'\in G'} d^{\varphi}\left(\alpha',\beta'(\alpha,\beta)\right); \tag{26}$$

$$3.\ EDP(\Omega)\le \prod_{i=1}^{r}\psi(\omega_{i-1},\omega_i)\max_{\alpha'\in G'} d^{\varphi}\left(0;\alpha',\beta'(\omega_{i-1},\omega_i)\right)=$$

$$=\prod_{i=1}^{r}\psi(\omega_{i-1},\omega_i)\max_{\alpha'\in G'} d^{\varphi}\left(\alpha',\beta'(\omega_{i-1},\omega_i)\right)\le \prod_{i=1}^{r}\max_{\alpha'\in G'} d^{\varphi}\left(\alpha',\beta'(\omega_{i-1},\omega_i)\right); \tag{27}$$

4. Якщо з умови $EDP(\Omega)\neq 0$ випливає умова $\alpha'(\omega_{i-1},\omega_i)\in U,\ \beta'(\omega_{i-1},\omega_i)\in V,\ i\in I$, для деяких $I\subset\{1,...,r\}$, $U,V\subset G'$, то

$$\max_{\Omega} EDP(\Omega)\le \prod_{i\in I}\max_{\substack{\alpha'\in U,\\ \beta'\in V}} d^{\varphi}(0;\alpha',\beta')\prod_{i\notin I}\max_{\alpha',\beta'\in G'} d^{\varphi}(0;\alpha',\beta'). \tag{28}$$

Доведення теореми аналогічне до теореми 1.9, з використанням означення УМШ у широкому сенсі.

Зауваження 2.19: останнє твердження теореми може бути узагальнене на випадок декількох підмножин $\{1,...,r\}$ та G'.

Приклади УМШ у широкому сенсі. 1. Національний стандарт блокового шифрування ГОСТ 28147-89 є УМШ у широкому сенсі відносно операції побітового додавання. Дійсно, в цьому випадку

$$G=V_{64},\ G'=V_{32},\ d^f(x;\alpha,\beta)=\psi(\alpha,\beta)d^{\varphi}(x';\alpha',\beta'),$$

де $\psi(\alpha,\beta)=\delta(\alpha_2,\beta_1)$, $x'(x)=x_2$, $\alpha'(\alpha,\beta)=\alpha_2$, $\beta'(\alpha,\beta)=\alpha_1\oplus\beta_2$, $x=(x_1,x_2)$, $\alpha=(\alpha_1,\alpha_2)$, $\beta=(\beta_1,\beta_2)$, φ_k – раундове перетворення, яке є УМВ.

2. У наступному розділі буде показано, що кандидат на новий національний стандарт БШ «Мухомор» є УМШ у широкому сенсі.

III. Дослідження стійкості шифру «Мухомор» до різницевого криптоаналізу

III.1. Аналіз результатів досліджень, проведених розробниками.

Перші дослідження практичної стійкості БШ „Мухомор" відносно різницевого криптоаналізу було здійснено розробниками [24]. При оцінювані було зроблено декілька припущень відосно БШ „Мухомор":

1) БШ „Мухомор" є марківським шифром;

2) кількість ненульових байтів вхідної різниці в SL-перетворенні дорівнюють кількості вихідних байт;

3) події, що полягають в проходженні різниці через різні s-блоки в одному раундовому перетворенні, є незалежними;

4) мінімальна кількість активних s-блоків у одному раунді при проходженні ненульової різниці, що має ненульову ймовірність, дорівнює 5.

Але дані твердження потребують уточнення.

По-перше, БШ „Мухомор” не є марківським шифром. Крім того, кількість ненульових байтів вхідної різниці в раундовому перетворенні, в загальному випадку, не дорівнюють кількості ненульових байт виходу, внаслідок наявності в ключовому суматорі операції додавання за модулем 2^{32}.

Далі, події, що полягають у проходженні різниці через різні s-блоки в одному раундовому перетворенні, є залежними, оскільки виходи і входи SL-перетворень в межах одного раунду пов’язані між собою. З урахуванням того, що сумування з ключем (і, відповідно, вхідна різниця) береться за модулем 232, за наявності біту переносу, події, що полягають у проходженні різниць через s-блоки в одному SL-перетворенні, вже не є незалежними.

Також відповідна кількість активних s-блоків у одному раунді може бути меншою за 5 (див рис. 1). Дійсно, якщо ліва половина вхідної різниці αL має лише один активний байт, а права половина різниці α_R містить лише три активних байти, тоді, з урахуванням того, що після s-блоків отриманий вектор передається на матрицю МДВ-перетворення (сума ненульових байт різниці на вході та різниці на виході SL-перетворення не менше за 5), після проходження α_L через SL_1-перетворення (γ_1) буде містити 4 ненульових байти. Можливий варіант, що при сумуванні γ_1 та α_R відбудеться скорочення і сума $\gamma_1 \oplus \alpha_R$, яка подається на SL_2-перетворення, буде містити теж тільки один ненульовий байт. Відповідно на виході після SL_2-перетворення можливо отримати різницю, яка буде дорівнювати різниці на виході з першого SL-перетворення і, відповідно, при сумуванні виходи з перших двох SL-перетвореннь можуть скоротитися і різниця γ_2, що подаватиметься на вхід SL_3-перетвореннь, не матиме жодного ненульового байта.

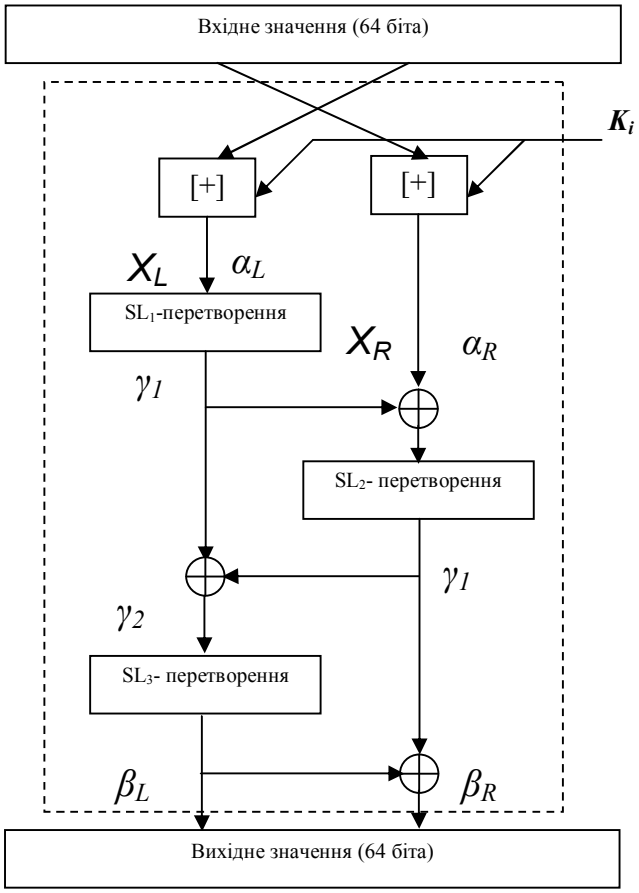

Рисунок 1 – Дослідження кількості активних s-блоків в одному раундовому перетворенні

Виходячи з міркувань, наведених вище, можна помітити, що у даному випадку в одному раунді буде лише 2 активних s-блока.

Доведемо, що існує така пара α,β (α – вхідна різниця, β – вихідна), яка має відповідну властивість та ненульову ймовірність.

Якщо на вхід SL_3-перетворення поступає нульова різниця, то виконується наступна рівність:

$$SL_1(X_L) \oplus SL_2(SL_1(X_L) \oplus X_R) = SL_1(X_L + \alpha_L) \oplus SL_2(SL_1(X_L + \alpha_L) \oplus (X_R + \alpha_R)). \quad (29)$$

Розробимо алгоритм побудови різниці, що буде задовольняти рівності (29).

Нехай

$$SL_1(X_L) \oplus SL_2(SL_1(X_L) \oplus X_R) = \bar{0}. \quad (30)$$

Тоді для будь-якого X_L завжди існує X_R таке, що виконується рівність (30), а саме:

$$SL_1(X_L) \oplus X_L = X_R. \quad (31)$$

Відповідно до (30) і (31), має виконуватись наступна рівність:

$$SL_1(X_L + \alpha_L) \oplus SL_2(SL_1(X_L + \alpha_L) \oplus (X_R + \alpha_R)) = \bar{0}. \quad (32)$$

Тоді для будь яких X_L і α_L можна підібрати α_R так, щоб виконувалась рівність (32):

$$((X_L + \alpha_L) \oplus SL_1(X_L + \alpha_L)) - X_R = \alpha_R. \quad (33)$$

Спираючись на міркування, що описані вище, представимо наступний алгоритм знаходження різниці, при якій буде лише 2 активних s-блоки.

Алгоритм 3.1: довільним чином обираємо X_L;

обираємо будь-яке значення α_L, з одним ненульовим байтом;

обчислюємо X_R та α_R, використовуючи (31) та (33), відповідно;

покладемо $\beta_L = \bar{0}$, а $\beta_R = SL_1(X_L) \oplus S1_2(X_L + \alpha_L)$.

Зауваження 3.2: Різниця, яку отримаємо при виконані Алгоритму 3.1, не обов'язково може вкладатись в схему, описану на початку розділу, тобто можливий випадок, коли α_L містить один активній байт, а α_R містить не три, а чотири активних байти. Але кількість активних s-блоків буде дорівнювати 2.

Очевидно, що мінімальна кількість активних s-блоків в одному раунді, при проходженні ненульової різниці з ненульовою ймовірністю, не може дорівнювати 1. Дійсно, при цьому єдиний ненульовий байт подається або на перше, або на друге SL-перетворення, на виході якого отримуємо 4 ненульових байта, які подаються на вхід 3-го SL-перетворення; відповідно отримуємо 5 активних s-блоків.

Приклад різниці, при якій в раунді буде лише два активні s-блоки:

α_L=(0,0,0,2) α_R=(78,174,47,151), β_L=(0,0,0,0) β_R=(212,47,236,179).

III.2. Формалізований опис шифру "Мухомор"

Для того, щоб зробити позначення та доведення менш громіздкими, будемо розглядати "Мухомор – 128". Всі отримані для цього випадку результати легко узагальнити для "Мухомор – 256" та "Мухомор – 512".

Для зручного представлення раундової функції шифру "Мухомор" необхідно ввести наступні позначення.

Нехай $n = 128$, $l = 16$. Для кожного $x \in V_n$ введемо представлення $x = (x_1, x_2, x_3, x_4)$, де $x_i \in V_{2l}$. Крім того, позначимо $x_i = (x_i^l, x_i^r)$, де $x_i^l, x_i^r \in V_l$, $i = \overline{1,4}$. Аналогічно для ключа i-го раунду $k_i \in V_{4l}$ позначимо $k = (k_{i1}, k_{i2})$, де $k_{i1}, k_{i2} \in V_{2l}$, $i = \overline{1,r}$, r – кількість раундів шифрування. Також введемо позначення: $y_1 = x_1 \oplus x_2$, $y_2 = x_3 + x_4$, $u_{i1} = (x_1 \oplus x_2) + k_{i1}$, $u_{i2} = (x_3 \oplus x_4) + k_{i2}$, $u_{i2} = (u_{i2}, u_{i1})$, де під " $\oplus$ " та "+" розуміються операції додавання за $\bmod 2$ та за $\bmod 2^{32}$, відповідно. Іноді номер раунду i у позначеннях $u_{i1}, u_{i2}, k_{i1}, k_{i2}, k_i$ будемо опускати, якщо розглядається один (фіксований чи довільний) раунд шифрування.

Нехай $f : V_{32} \times V_{32} \to V_{64}$ – функція ускладнення шифру. Будемо представляти $f(v_1, v_2)$ у вигляді

$$f(v_1, v_2) = (f_1(v_1, v_2), f_2(v_1, v_2)) = (f_1^l(v_1, v_2), f_1^r(v_1, v_2), f_2^l(v_1, v_2), f_2^r(v_1, v_2)),$$

де $v_1, v_2 \in V_{32}$, $f_i : V_{32} \times V_{32} \to V_{32}$; $f_i^i, f_i^r : V_{32} \times V_{32} \to V_{16}$, $f_i(v_1, v_2) = (f_i^l(v_1, v_2), f_i^r(v_1, v_2))$, $i = 1,2.$

Нехай $x \in V_{128}$ – вхідний вектор деякого раунду шифрування. Тоді в наших позначеннях вихідний вектор $F_k(x)$ даного раунду має вигляд:

$$\{x_1^r \oplus f_1^r(u_1,u_2),\ x_1^l \oplus x_1^r \oplus f_1^l(u_1,u_2) \oplus f_1^r(u_1,u_2),$$
$$x_2 \oplus f_1\ (u_1,u_2),$$
$$x_3^r \oplus f_2^r(u_1,u_2),\ x_3^l \oplus x_3^r \oplus f_2^l(u_1,u_2) \oplus f_2^r(u_1,u_2),$$
$$x_4 \oplus f_2(u_1,u_2)\},$$

де у кожному рядку записано 32-бітовий вектор.

III.3. Основні різницеві властивості шифру "Мухомор"

Теорема 3.1: шифр "Мухомор – 128" є узагальненим марківським шифром відносно операції побітового додавання.

Доведення: запишемо вираз $\delta(F_k(x \oplus \alpha) \oplus F_k(x), \beta)$ у зручнішому вигляді:

$$\{\delta(\alpha_1^r \oplus f_1^r(v_1,v_2) \oplus f_1^r(u_1,u_2), \beta_1^l) \times$$
$$\times \delta(\alpha_1^l \oplus \alpha_1^r \oplus f_1^l(v_1,v_2) \oplus f_1^l(u_1,u_2) \oplus f_1^r(u_1,u_2) \oplus f_1^r(u_1,u_2), \beta_1^r) \times$$
$$\times \delta(\alpha_2 \oplus f_1\ (v_1,v_2) \oplus f_1\ (u_1,u_2), \beta_2) \times \delta(\alpha_3^r \oplus f_2^r(v_1,v_2) \oplus f_2^r(u_1,u_2), \beta_3^l) \times$$
$$\times \delta(\alpha_3^l \oplus \alpha_3^r \oplus f_2^l(v_1,v_2) \oplus f_2^l(u_1,u_2) \oplus f_2^r(u_1,u_2) \oplus f_2^r(u_1,u_2), \beta_3^r) \times$$
$$\times \delta(\alpha_4 \oplus f_2\ (v_1,v_2) \oplus f_2\ (u_1,u_2), \beta_4)\}, \qquad (34)$$

де $\alpha, \beta \in V_{128}$, $\alpha = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, $\beta = (\beta_1, \beta_2, \beta_3, \beta_4)$, $\alpha_i, \beta_i \in V_{32}$, $i = \overline{1,4}$, $\alpha_i = (\alpha_i^l, \alpha_i^r)$, $\beta_i = (\beta_i^l, \beta_i^r)$, $\alpha_i^l, \alpha_i^r, \beta_i^l, \beta_i^r \in V_{16}$, $i = \overline{1,4}$, $v_1 = (x_1 \oplus x_2 \oplus \alpha_1 \oplus \alpha_2) + k_1$, $v_2 = (x_3 \oplus x_4 \oplus \alpha_3 \oplus \alpha_4) + k_2$.

Формулу (34) перепишемо наступним чином:

$$\delta(f_1^r(v_1,v_2) \oplus f_1^r(u_1,u_2), \alpha_1^r \oplus \beta_1^l) \times$$
$$\times \delta(f_1^l(v_1,v_2) \oplus f_1^l(u_1,u_2) \oplus f_1^r(u_1,u_2) \oplus f_1^r(u_1,u_2),\ \alpha_1^l \oplus \alpha_1^r \oplus \beta_1^r) \times$$
$$\times \delta(f_1\ (v_1,v_2) \oplus f_1\ (u_1,u_2), \alpha_2 \oplus \beta_2) \times \delta(f_2^r(v_1,v_2) \oplus f_2^r(u_1,u_2), \alpha_3^r \oplus \beta_3^l) \times$$
$$\times \delta(f_2^l(v_1,v_2) \oplus f_2^l(u_1,u_2) \oplus f_2^r(u_1,u_2) \oplus f_2^r(u_1,u_2),\ \alpha_3^l \oplus \alpha_3^r \oplus \beta_3^r) \times$$
$$\times \delta(f_2\ (v_1,v_2) \oplus f_2\ (u_1,u_2),\ \alpha_4 \oplus \beta_4) = \delta(f_1^r(v_1,v_2) \oplus f_1^r(u_1,u_2), \alpha_1^r \oplus \beta_1^l) \times$$
$$\times \delta(f_1^l(v_1,v_2) \oplus f_1^l(u_1,u_2),\ \alpha_1^l \oplus \alpha_1^r \oplus \beta_1^r \oplus \alpha_1^r \oplus \beta_1^l) \times$$
$$\times \delta(f_1^l(v_1,v_2) \oplus f_1^l(u_1,u_2),\ \alpha_2^l \oplus \beta_2^l) \times \delta(f_1^r(v_1,v_2) \oplus f_1^r(u_1,u_2), \alpha_2^r \oplus \beta_2^r) \times$$
$$\times \delta(f_2^r(u_1,u_2) \oplus f_2^r(u_1,u_2),\ \alpha_3^r \oplus \beta_3^l) \times$$
$$\times \delta(f_2^l(v_1,v_2) \oplus f_2^l(u_1,u_2),\ \alpha_3^l \oplus \alpha_3^r \oplus \alpha_3^r \oplus \beta_3^r \oplus \beta_3^l) \times$$
$$\times \delta(f_2^l(v_1,v_2) \oplus f_2^l(u_1,u_2), \alpha_4^l \oplus \beta_4^l) \times \delta(f_2^r(v_1,v_2) \oplus f_2^r(u_1,u_2), \alpha_4^r \oplus \beta_4^r) =$$
$$= \delta(\alpha_1^r \oplus \beta_1^l,\ \alpha_2^r \oplus \beta_2^r) \times \delta(f_1^r(v_1,v_2) \oplus f_1^r(u_1,u_2), \alpha_2^r \oplus \beta_2^r) \times$$
$$\times \delta(\alpha_1^l \oplus \beta_1^l \oplus \beta_1^r,\ \alpha_2^l \oplus \beta_2^l) \times \delta(f_1^l(v_1,v_2) \oplus f_1^l(u_1,u_2), \alpha_2^l \oplus \beta_2^l) \times$$
$$\times \delta(\alpha_3^r \oplus \beta_3^l,\ \alpha_4^r \oplus \beta_4^r) \times \delta(f_2^r(v_1,v_2) \oplus f_2^r(u_1,u_2), \alpha_4^r \oplus \beta_4^r) \times$$
$$\times \delta(\alpha_3^l \oplus \beta_3^l \oplus \beta_3^r,\ \alpha_4^l \oplus \beta_4^l) \times \delta(f_2^l(v_1,v_2) \oplus f_2^l(u_1,u_2), \alpha_4^l \oplus \beta_4^l). \qquad (35)$$

Отже, щоб ймовірність диференціала не дорівнювала 0, необхідно, щоб одночасно виконувались наступні умови:

$$\begin{cases} \alpha_1^r \oplus \beta_1^l = \beta_2^r \oplus \alpha_2^r; \\ \alpha_1^l \oplus \beta_1^l \oplus \beta_1^r, = \alpha_2^l \oplus \beta_2^l; \\ \alpha_3^r \oplus \beta_3^l = \alpha_4^r \oplus \beta_4^r; \\ \alpha_3^l \oplus \beta_3^l \oplus \beta_3^r = \alpha_4^l \oplus \beta_4^l. \end{cases} \tag{36}$$

Надалі розглядатимемо лише такі диференціали, для яких виконується (36). У цьому випадку (35) набуде вигляду:

$$\delta(f_1^r(v_1,v_2) \oplus f_1^r(u_1,u_2), \alpha_2^r \oplus \beta_2^r) \times \delta(f_1^l(v_1,v_2) \oplus f_1^l(u_1,u_2), \alpha_2^l \oplus \beta_2^l) \times$$
$$\times \delta(f_2^r(u_1,u_2) \oplus f_2^r(u_1,u_2), \alpha_4^r \oplus \beta_4^r) \times \delta(f_2^l(v_1,v_2) \oplus f_2^l(u_1,u_2), \alpha_4^l \oplus \beta_4^l). \tag{37}$$

Зробимо заміни змінних: $\alpha_2^l \oplus \beta_2^l = \gamma_1$, $\alpha_2^r \oplus \beta_2^r = \gamma_2$, $\alpha_4^l \oplus \beta_4^l = \gamma_3$, $\alpha_4^r \oplus \beta_4^l = \gamma_4$, $\alpha_1 \oplus \alpha_2 = \omega_1$, $\alpha_3 \oplus \alpha_4 = \omega_2$. Позначимо $\gamma = (\gamma_1, \gamma_2, \gamma_3, \gamma_4) = (\alpha_2 \oplus \beta_2, \alpha_4 \oplus \beta_4)$.

Отже, при виконанні умови (36) в наших позначеннях середнє (за ключами) значення (34) дорівнює

$$2^{-n} \sum_{k \in V_n} \{\delta(f_1^l((y_1 \oplus \omega_1) + k_1, (y_2 \oplus \omega_2) + k_2) \oplus f_1^l(y_1 + k_1, y_2 + k_2), \gamma_1) \times$$
$$\times \delta(f_1^r((y_1 \oplus \omega_1) + k_1, (y_2 \oplus \omega_2) + k_2) \oplus f_1^r(y_1 + k_1, y_2 + k_2), \gamma_2) \times$$
$$\times \delta(f_2^l((y_1 \oplus \omega_1) + k_1, (y_2 \oplus \omega_2) + k_2) \oplus f_2^l(y_1 + k_1, y_2 + k_2), \gamma_3) \times$$
$$\times \delta(f_2^r((y_1 \oplus \omega_1) + k_1, (y_2 \oplus \omega_2) + k_2) \oplus f_2^r(y_1 + k_1, y_2 + k_2), \gamma_4)\} =$$

$$= 2^{-n} \sum_{k_1, k_2 \in V_{n/2}} \delta(f((y_1 \oplus \omega_1) + k_1, (y_2 \oplus \omega_2) + k_2) \oplus f(y_1 + k_1, y_2 + k_2), \gamma). \tag{38}$$

Теороема 3.2: кандидат на новий національний стандарт БШ "Мухомор" ([4]) також є УМШ у широкому сенсі.

Доведення: розглянемо БШ "Мухомор-128". В цьому випадку

$$G = V_{128},\ G' = V_{64},\ d^f(x;\alpha,\beta) = \psi(\alpha,\beta) d^{\varphi}(x';\alpha',\beta'),$$

де

$$\psi(\alpha,\beta) = \delta(\alpha_1^r \oplus \alpha_2^r, \beta_1^r \oplus \beta_2^r) \delta(\alpha_1^l \oplus \alpha_2^l, \beta_1^l \oplus \beta_1^r \oplus \beta_2^l) \times$$
$$\times \delta(\alpha_3^r \oplus \alpha_4^r, \beta_3^r \oplus \beta_4^r)\ \delta(\alpha_3^l \oplus \alpha_4^l, \beta_3^l \oplus \beta_3^r \oplus \beta_4^l),$$
$$x = (x_1, x_2, x_3, x_4),\ \alpha = (\alpha_1, \alpha_2, \alpha_3, \alpha_4),\ \beta = (\beta_1, \beta_2, \beta_3, \beta_4),\ \alpha_i = (\alpha_i^l, \alpha_i^r),\ \beta_i = (\beta_i^l, \beta_i^r),\ i = \overline{1,4},$$
$$x'(x) = (x_1 \oplus x_2, x_3 \oplus x_4),\ \alpha'(\alpha,\beta) = (\alpha_1 \oplus \alpha_2, \alpha_3 \oplus \alpha_4),\ \beta'(\alpha\alpha,\beta = (\alpha_2 \oplus \beta_2, \alpha_4 \oplus \beta_4),$$

φ_k – раундове перетворення, яке є УМВ.

Згідно з означенням, шифр «Мухомор» буде УМШ у широкому сенсі, якщо його функція ускладнення є УМВ. Доведемо цю властивість функції ускладнення.

Для $a, b \in V_{32}$ позначимо $\nu(a,b) = (a \oplus b) - a - b$, де двійкові вектори a, b природнім чином ототожнюються з цілими числами від 0 до $2^{32} - 1$. В наших позначеннях формула (38) може бути записана наступним чином:

$$2^{-n} \sum_{k_1, k_2 \in V_{n/2}} \delta(f(y_1 + \omega_1 + \nu(y_1, \omega_1) + k_1, y_2 + \omega_2 + \nu(y_2, \omega_2) + k_2) \oplus f(y_1 + k_1, y_2 + k_2), \gamma).$$

У останньому виразі зробимо заміну змінної $y_i + k_i = \tilde{k}_i$, а також позначимо $\omega_i + \nu(y_i, \omega_i) = \sigma_{y_i}(\omega_i)$, $i = 1,2$. Після цього вираз перетвориться на наступний:

$$2^{-n} \sum_{k_1, k_2 \in V_{n/2}} \delta(f(\tilde{k}_1 + \sigma_{y_1}(\omega_1), \tilde{k}_1 + \sigma_{y_2}(\omega_2)) \oplus f(\tilde{k}_1, \tilde{k}_2), \gamma).$$

Для завершення доведення залишилося зазначити, що відображення $\omega \to \sigma_y(\omega)$ при кожному фіксованому $y \in V_{32}$ є перестановкою на V_{32}, отже функція ускладнення є УМВ. Доведення завершене.

Наслідки з теореми 3.2. 1) Нехай $\Omega = (\omega_0, \omega_1, ..., \omega_r)$, $\omega_i \in V_{128}$ – різницева характеристика шифру "Мухомор-128". Позначимо $\omega_i = (\omega_{i1}, \omega_{i2}, \omega_{i3}, \omega_{i4})$, $\omega_{ij} \in V_{32}$, $\omega_{ij} = (\omega_{ij}^l, \omega_{ij}^r)$, $\omega_{ij}^l, \omega_{ij}^r \in V_{16}$, $j = \overline{1,4}$, $i = \overline{0,r}$. Тоді, якщо $EDP(\Omega) \neq 0$, то виконані наступні умови:

$$\begin{cases} \omega_{i1}^r \oplus \omega_{i2}^r = \omega_{i+1,1}^l \oplus \omega_{i+1,2}^r; \\ \omega_{i1}^l \oplus \omega_{i2}^l = \omega_{i+1,1}^l \oplus \omega_{i+1,1}^r \oplus \omega_{i+1,2}^l; \\ \omega_{i3}^r \oplus \omega_{i4}^r = \omega_{i+1,3}^l \oplus \omega_{i+1,4}^r; \\ \omega_{i3}^l \oplus \omega_{i4}^l = \omega_{i+1,3}^l \oplus \omega_{i+1,3}^r \oplus \omega_{i+1,4}^l, i = \overline{0,r-1}. \end{cases} \tag{39}$$

2) В наших позначеннях $\forall \alpha, \beta \in V_{128}$:

$$2^{-64} \sum_{k \in V_{64}} \cdot 2^{-128} \sum_{k \in V_{128}} \delta(F_k(x \oplus \alpha) \oplus F_k(x), \beta) =$$

$$= 2^{-64} \sum_{k \in V_{64}} \cdot 2^{-128} \sum_{k \in V_{128}} \delta(f(y_1 + \omega_1) + k_1, (y_2 + \omega_2) + k_2) \oplus f(y_1 + k_1, y_2 + k_2), \gamma),$$

де $\omega_1 = \alpha_1 \oplus \alpha_2$, $\omega_2 = \alpha_3 \oplus \alpha_4$, $\omega_1, \omega_2 \in V_{32}$, $\gamma = (\gamma_1, \gamma_2)$, $\gamma_1, \gamma_2 \in V_{32}$, $\gamma_1 = \alpha_2 \oplus \beta_2$, $\gamma_2 = \alpha_4 \oplus \beta_4$.

$$3)\ \max EDP(\Omega) \le (\max_{\omega, \gamma \neq 0} 2^{-64} \sum_{k \in V_{64}} \delta(f(\omega + k) \oplus f(k), \gamma))^S. \tag{40}$$

Наслідки 1) та 2) випливають безпосередньо з доведення теореми 3.1, наслідок 3) випливає з теореми 3.2 і властивостей УМШ.

Таким чином, у даному підрозділі ми довели, що шифр «Мухомор» є УМШ у широкому сенсі. Отже, його різницеві властивості залежать від різницевих властивостей функції ускладнення, які ми будемо досліджувати далі.

IV. Висновки

Дана робота містить подальший розвиток теорії оцінювання стійкості УМШ до різницевого криптоаналізу, що була започаткована в роботах [5, 6, 15, 16] та застосована до шифрів ГОСТ 28147-89 та «Калина». Введене поняття УМШ у широкому сенсі дозволяє застосувати дану теорію і до шифру «Мухомор» та отримати оцінку (40). Проте отримані чисельні оцінки, які можна вивести з (40) не дають можливості стверджувати, що шифр «Мухомор» є практично стійким до методу криптоаналізу. Тому метою подальших досліджень є, з одного боку, більш глибоке вивчення різницевих характеристик функції $f(x)$ раундового перетворення шифру, а з іншого – отримання результатів щодо оцінки індексу галуження та особливостей його використання в УМШ у широкому сенсі, в ключовому суматорі яких реалізовано модульне додавання.

Література: ***1.*** *National Institute of Standards and Technology: The Advanced Encryption Standard (AES) – Режим доступу:*. http://csrc.nist.gov/aes/ *– Заголовок з екрану.* ***2.*** *NESSIE Project – New European Schemes for Signatures, Integrity and Encryption – Режим доступу: /* http://cryptonessie.org. *– Заголовок з екрану.* ***3.*** *Горбенко И. Д., Долгов В. І. та ін. Перспективний блоковий шифр "Калина" – основні положення та специфікація // Прикладна радіоелектроніка. – 2007. – т.6. №2. – С.195-210.* ***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.*** *Алексейчук А. Н., Ковальчук Л. В., Скрынник Е. Н. Оценки практической стойкости блочного шифра «Калина» относительно методов разностного, линейного криптоанализа и алгебраических атак, основанных на гомоморфизмах. // Прикладная радиоэлектроника. – 2008. – т. 7. – с. 203 – 210.* ***6.*** *Алексейчук А. Н., Ковальчук Л. В., Скрыпник Л. В., Шевцов А. С. Оценки практической стойкости блочного шифра «Калина» относительно*

разностного линейного и билинейного методов криптоанализа. // Труды седьмой общероссийской научной конфиренции ***7.*** *ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Госстандарт СССР, 1989. – 28 с.* ***8.*** *Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems // Journal of Cryptology. – 1991. – V. 4. – № 1. – P. 3 – 72.* ***9.*** *Lai X., Massey J. L., Murphy S. Markov ciphers and differential cryptanalysis // Advances in Cryptology – EUROCRYPT'91, Proceedings. – Springer Verlag, 1991. – P. 17 – 38.* ***10.*** *S. K. Langford, M. E. Hellman. Differential-linear cryptoanalisis // Advanced in Cryptology. – CRYPTO'94 (LNCS 839). – 1994. – P. 17-25.* ***11.*** *Vaudenay S. On the security of CS-cipher // Fast Software Encryption. – FSE'99, Proceedings. – Springer Verlag, 1999. – P. 260 – 274.* ***12.*** *Kanda M., Takashima Y., Matsumoto T., Aoki K., Otha K. A strategy for constructing fast raund functions with practical security against differential and linear cryptanalysis // Selected Areas in Cryptography. – SAC 1998, Proceedings. – Springer Verlag, 1999. – P. 264 – 279.* ***13.*** *Алексейчук А. Н., Ковальчук Л. В. Верхние границы максимальных значений вероятностей дифференциальных и линейных характеристик шифра Фейстеля, содержащего сумматор по модулю* 2^m *// Прикладная радиоэлектроника. – 2006. – Т. 5. – № 1. – С. 74 – 82.* ***14.*** *Скрипник Л. В., Ковальчук Л. В., Верхние оценки средних вероятностей дифференциалов булевых отображений // Захист інформації – 2006. – №3. – С. 7-13.* ***15.*** *Олексійчук А. Н., Ковальчук Л. В., Кальченко 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.* ***16.*** *Ковальчук Л. Обобщёные 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* ***17.*** *Бондаренко М. Ф., Горбенко І. Д. та ін. Обґрунтування вимог та розробка основних рішень з побудови та властивості перспективного БСШ «Мухомор» // Прикладна радіоелектроніка. – 2007. – т. 6. №2. – С.174 – 185.* ***18.*** *Горбенко И. Д., Долгов В. І. та ін. Криптостійкість шифра «Мухомор» // Прикладна радіоелектроніка. – 2007. – т.6. №2. – С.186-194.* ***19.*** *Олейников Р. В., Лисицкая И. В. Исследование свойств подстановок ГОСТ 28147-89, построенных на основе анализа свойств координатных функций // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ, 2002. – Вип. 3. – С. 123 – 130.* ***20.*** *Олейников Р. В. Дифференциальный криптоанализ алгоритма шифрования ГОСТ 28147-89 // Радиотехника. – 2001. – Вып. 119. – С. 146 – 152.* ***21.*** *Лисицкая И. В., Руженцев В. И. Цепи Фейстеля и дифференциальный криптоанализ // Радиотехника. – 2002. – Вып. 126. – С. 158 – 165.* ***22.*** *Долгов В. И., Лисицкая И. В., Олейников Р. В., Голованич С. Д., Коряк А. С. Дополнительные требования к отбору таблиц подстановок для ГОСТ 28147-89 // Радиотехника. – 2001. – Вып. 119. – С. 153 – 159.* ***23.*** *Долгов В. И., Лисицкая И. В., Олейников Р. В., Шумов А. И. "Слабые" ключи в алгоритме шифрования ГОСТ 28147-89 // Радиотехника. – 2000. – Вып. 114. – С. 63 – 69.* ***24.*** *Лисицкая И. В. Противоречивые подстановки в алгоритме ГОСТ 28147-89 // Информационные системы: Сборник научных трудов. – Харьков, 1995. – НАНУ, ПАНУ, ХВУ. – 9 с.* ***25.*** *Seki H., Toshinobu K. Differential cryptanalysis of redused round of GOST // Selected Areas in Cryptography. – SAC 2000, Proceedings. – Springer Verlag, 2001. – P. 315 – 323.* ***26.*** *Лисицкая И. В., Цепурит Т. В., Лесняк В. В., Пинчук М. В., Мелецкий А. П. Исследование возможностей модернизации шифра ГОСТ 28147-89 с целью дальнейшего повышения его безопасности // Радиотехника. – 2001. – Вып. 119. – С. 160 – 165.*

УДК 003.26 : 004.424.47

ПІДХОДИ ДО ПОБУДОВИ ШВИДКИХ АЛГОРИТМІВ ХЕШУВАННЯ

Володимир Лужецький, Юрій Баришев
Вінницький національний технічний університет

Анотація: **Розглянуто конструкції хешування та підходи до їх розпаралелення. Запропоновано узагальнену конструкцію паралельного хешування, стійку до відомих атак. Визначено оцінки тривалості хешування для різних реалізацій цієї конструкції. Дані оцінки були порівняні з аналогічними оцінками для відомих конструкцій.**

Summary: **Hash constructions and approaches of their parallel computation are considered. The generalized construction of parallel hashing, that is infeasible to known attacks, is proposed. The hash computation durations of this construction different implementations are evaluated. The results of the evaluations were compared with ones of the known constructions.**

Ключові слова: **конструкція хешування, паралельні обчислення, атака Жукса.**