УДК 004.056.53

ІМОВІРНОСТІ ДИФЕРЕНЦІАЛІВ LRX-ПЕРЕТВОРЕНЬ СПЕЦІАЛЬНОГО ВИДУ

О. О. Галіца[1,а], С. В. Яковлєв[1,б]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

У даній роботі було розглянуто ряд LRX-перетворень, знайдено аналітичні вирази диференціальних імовірностей для функцій мажоризації та функції логічного ТА. Було сформульовано узагальнену теорему про диференціальні ймовірності для k-кратної функції логічного ТА. Одержані результати дозволять використовувати більш складні конструкції в якості нелінійного перетворення в LRX-криптосистемах та уточнювати вже існуючі оцінки стійкості для них.

Ключові слова: ARX-криптосистеми, диференціальний аналіз, LRX-перетворення

Вступ

Широкий клас алгоритмів симетричної криптографії використовує лише невелику підмножину операцій: додавання за модулем, бітовий зсув та побітове додавання, унаслідок чого такі системи й отримали назву ARX (addition, rotation, xor). Завдяки використанню цих простих операцій, ARX-криптосистеми характеризуються високою швидкодією у порівнянні з іншими класами симетричних криптосистем, а стійкості проти класичних методів криптоаналізу (таких як диференціальний та лінійний криптоаналізи) вони досягають комбінацією лінійних (бітовий зсув та побітове додавання) та нелінійних (модульне додавання) операцій.

На противагу ARX-, також розроблялися LRX-криптосистеми, які замість модульного додавання — найскладнішої операції в трійці A-R-X — використовували деякі інші нелінійні логічні операції. Прикладами таких криптосистем можуть слугувати NORX [1] та SIMON [2].

Один з найбільш потужних видів криптоаналізу симетричних криптосистем є диференціальний криптоаналіз, суть якого полягає в дослідженні ймовірностей диференціалів, які відображають різницю вхідних та вихідних текстів за деякою операцією, зазвичай це операція побітового додавання. Безпосередньо для ARX-шифрів диференційний криптоаналіз почався з роботи [3].

При побудові LRX-криптосистем потрібно аналізувати диференціальні ймовірності обраних перетворень та обирати баланс між бажаним рівнем стійкості та простотою аналізу. Саме тому в цій роботі аналізуються прості за структурою перетворення, які можуть бути використані для побудови більш стійких LRX-криптосистем.

[а] halitsa.oleksandr@lll.kpi.ua
[б] yasv@rl.kiev.ua

1. Диференціальні ймовірності функції логічного ТА

В LRX-криптосистемах замість модульного додавання використовують обчислювально простіші логічні перетворення, зазвичай з використанням операції логічного ТА $\wedge$ (&). Наприклад, розробники шифру NORX (учасник конкурсу CAESAR) використали таку апроксимацію модульного додавання:

$$f(x,y) = (x \oplus y) \oplus ((x \wedge y) \ll 1);$$

функції такого виду достатньо для забезпечення властивості перемішування, водночас вона не є надто складною для криптоаналізу [1].

Шифр SIMON теж належить до класу LRX-шифрів [2], його розробники використали таку функцію в якості заміни додавання за модулем:

$$f(x) = ((x \lll 1) \wedge (x \lll 8)) \oplus (x \lll 2).$$

В роботі по криптоаналізу шифру SIMON [4] були одержані вирази для ймовірності диференціалів для операції логічного ТА:

$$xdp^{\wedge}(\alpha, \beta \to \gamma) =$$
$$= 2^{-n} \cdot \prod_{i=0}^{n-1} ((2 \cdot \overline{(\overline{\alpha_i} \wedge \overline{\beta_i} \wedge \overline{\gamma_i})}) \vee \overline{(\overline{\alpha_i} \wedge \overline{\beta_i})}) \wedge \overline{(\overline{\alpha_i} \wedge \overline{\beta_i} \wedge \gamma_i)}.$$

Виявилося, що цей результат можна спростити й отримати більш зручні для використання формули, тому сформулюємо для цього теорему.

Теорема 1. Для довільних $\alpha, \beta, \gamma \in V_n$ справедливі твердження:

1) $xdp^{\wedge}(\alpha, \beta \to \gamma) \neq 0 \iff \overline{\alpha} \wedge \overline{\beta} \wedge \gamma = 0$;
2) якщо $xdp^{\wedge}(\alpha, \beta \to \gamma) \neq 0$, то

$$xdp^{\wedge}(\alpha, \beta \to \gamma) = 2^{-wt(\alpha \vee \beta)},$$

де $wt(x)$ — функція ваги вектору (кількість одиничних бітів в ньому).

Доведення. Розглянемо рівняння $(x \oplus \alpha)(y \oplus \beta) = xy \oplus \gamma$ побітово:

$$\begin{aligned}(x_i \oplus \alpha_i)(y_i \oplus \beta_i) &= x_i y_i \oplus \gamma_i;\\ \alpha_i y_i \oplus \beta_i x_i &= \alpha_i \beta_i \oplus \gamma_i. \end{aligned} \quad (1)$$

Позначимо через p_i імовірність виконання рівняння (1); оскільки усі біти обчислюються незалежно, то $xdp^{\wedge}(\alpha, \beta \to \gamma) = \prod_{i=0}^{n-1} p_i$.

Розглянемо усі можливі випадки значень параметрів α_i, β_i, γ_i, відповідні форми рівняння (1) та імовірності p_i для кожного випадку. Значення імовірностей наведено у таблиці 1.

Таблиця 1. Рівняння (1) та ймовірність його виконання p_i при усіх можливих значеннях α_i, β_i, γ_i.

α_i	β_i	γ_i	рівняння	p_i
0	0	0	$0 = 0$	1
0	0	1	$0 = 1$	0
0	1	0	$x_i = 0$	1/2
0	1	1	$x_i = 1$	1/2
1	0	0	$y_i = 0$	1/2
1	0	1	$y_i = 1$	1/2
1	1	0	$x_i \oplus y_i = 1$	1/2
1	1	1	$x_i \oplus y_i = 0$	1/2

З таблиці 1 бачимо, що при $\alpha_i = \beta_i = 0$, $\gamma_i = 1$ рівняння не може виконуватись ($p_i = 0$); тому якщо у векторі $\overline{\alpha} \wedge \overline{\beta} \wedge \gamma$ хоча б один біт дорівнює 1, то $xdp^{\wedge}(\alpha, \beta \to \gamma) = 0$.

Якщо ж $xdp^{\wedge}(\alpha, \beta \to 0) \neq 0$, то при $\alpha_i = \beta_i = 0$ маємо $p_i = 1$, а в усіх інших випадках $p_i = \frac{1}{2}$; тому $xdp^{\wedge}(\alpha, \beta \to \gamma) = 2^{-k}$, де k — кількість ненульових пар (α_i, β_i) або, що те саме, кількість одиничних бітів у векторі $\alpha \vee \beta$. Звідси випливає твердження теореми. ■

Особливістю операції логічного ТА є те, що усі інші нелінійні двійкові операції від двох аргументів (а саме $\vee$, $|$, $\downarrow$, $\to$, $\leftarrow$) можна виразити через неї, більше того, їхні диференціальні ймовірності виявилися пов'язані.

Для будь-яких $\alpha, \beta, \gamma \in V_n$ справедливі рівності

$$xdp^{\star}(\alpha, \beta \to \gamma) = xdp^{\wedge}(\alpha, \beta \to \gamma),$$

де $\star \in \{\vee, |, \downarrow, \to, \leftarrow\}$.

2. Диференціальні ймовірності k-кратного логічного ТА

Теорема 1 може бути узагальнена й на операцію k-кратного логічного ТА, але спочатку доведемо допоміжний факт.

Лема 1. Нехай $f(x_1, x_2, \dots, x_k) = (x_1 \oplus \alpha_1) \cdot \dots \cdot (x_k \oplus \alpha_k)$, $x_i, \alpha_i \in \{0, 1\}$, $i = \overline{1, n}$, тоді:

$$wt\left(f(x_1, x_2, \dots, x_k)\right) = 1.$$

Доведення. Розглянемо таке рівняння:

$$(x_1 \oplus \alpha_1) \cdot (x_2 \oplus \alpha_2) \cdot \dots \cdot (x_k \oplus \alpha_k) = 1. \quad (2)$$

З властивостей функції логічного ТА випливає, що рівняння (2) може бути переписане у вигляді системі лінійних рівнянь:

$$\begin{cases} x_1 \oplus \alpha_1 = 1 \\ x_2 \oplus \alpha_2 = 1 \\ \dots \\ x_k \oplus \alpha_k = 1 \end{cases} \iff \begin{cases} x_1 = \alpha_1 \oplus 1 \\ x_2 = \alpha_2 \oplus 1 \\ \dots \\ x_k = \alpha_k \oplus 1 \end{cases}$$

Тобто існує єдиний вектор $(y_1, y_2, \dots, y_k) \in V_k$:

$$(y_1, y_2, \dots, y_k) = (\alpha_1 \oplus 1, \alpha_2 \oplus 1, \dots, \alpha_k \oplus 1),$$

такий, що $f(y_1, y_2, \dots, y_k) = 1$, звідки й випливає рівність:

$$wt\left(f(x_1, x_2, \dots, x_k)\right) = 1,$$

яка й доводить лему. ■

Для більш компактного запису, введемо позначення x^{α}, де $x, \alpha \in \{0, 1\}$:

$$x^{\alpha} = \begin{cases} x, \alpha = 0; \\ \overline{x}, \alpha = 1. \end{cases}$$

Це позначення легко узагальнюється для багатобітових векторів:

$$x^{\alpha} = \left(x_{n-1}^{\alpha_{n-1}}, x_{n-2}^{\alpha_{n-2}}, \dots, x_0^{\alpha_0}\right);\ x, \alpha \in V_n.$$

Теорема 2. Нехай $f(x_1, x_2, \dots, x_k) = x_1 x_2 \cdot \dots \cdot x_k$, $k \geq 2$, $x_i \in V_n$, тоді $\forall \alpha_1, \dots, \alpha_k, \gamma \in V_n$:

1) $xdp^f(\alpha_1, \dots, \alpha_k \to \gamma) \neq 0 \iff \overline{\alpha_1} \cdot \dots \cdot \overline{\alpha_k} \cdot \gamma = 0$;
2) якщо $xdp^f(\alpha_1, \dots, \alpha_k \to \gamma) \neq 0$, то:

$$xdp^f(\alpha_1, \dots, \alpha_k \to \gamma) = \\ = \left(\frac{1}{2^{k-1}}\right)^{wt(\alpha_1 \vee \dots \vee \alpha_k)} \cdot \left(2^{k-1} - 1\right)^{wt((\alpha_1 \vee \dots \vee \alpha_k) \wedge \overline{\gamma})}.$$

Доведення. Оскільки усі використані операції виконуються побітово, то ймовірності розглядатимуться для деякого i-того біту, а далі, користуючись незалежністю бітів, ми отримаємо відповідні ймовірності для усіх бітів. Для спрощення викладок порядковий індекс біту не вказуватиметься, тобто запис $x_1 \oplus x_2$ означатиме бітове додавання лише i-тих бітів векторів x_1 та x_2.

Формула для обчислення диференціальної ймовірності k-кратного застосування операції логічного ТА за операцією побітового додавання $xdp^f(\alpha_1, \dots, \alpha_k \to \gamma)$ має такий вид:

$$\Pr_{x_1, \dots, x_k}\left\{\underbrace{(x_1 \oplus \alpha_1) \dots (x_k \oplus \alpha_k)}_{f_2} = \underbrace{x_1 \dots x_k}_{f_1} \oplus \gamma\right\}.$$

Якщо $\gamma = 0$, то потрібно проаналізувати ймовірність такої події:

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdot \dots \cdot x_k^{\alpha_k} = x_1 x_2 \cdot \dots \cdot x_k.$$

Якщо $\alpha_1 = \alpha_2 = \dots = \alpha_k = 0$, то

$$\Pr_{x_1, \dots, x_k}\left\{x_1 x_2 \cdot \dots \cdot x_k = x_1 x_2 \cdot \dots \cdot x_k\right\} = 1.$$

інакше, з леми 1 випливає, що

$$\begin{cases}\exists!\left(y_1^{(1)}, y_2^{(1)}, \ldots, y_k^{(1)}\right) : f_2\left(y_1^{(1)}, y_2^{(1)}, \ldots, y_k^{(1)}\right) = 1; \\ \left(y_1^{(1)}, y_2^{(1)}, \ldots, y_k^{(1)}\right) \neq \underbrace{(1,1,\ldots,1)}_{k}. \end{cases}$$

З цього випливає, що для всіх бітових векторів $(y_1, y_2, \ldots, y_k) \in V_k$, які не дорівнюють $\left(y_1^{(1)}, y_2^{(1)}, \ldots, y_k^{(1)}\right)$ та $\underbrace{(1,1,\ldots,1)}_{k}$, справедливе таке рівняння:

$$f_1(y_1, y_2, \ldots, y_k) = f_2(y_1, y_2, \ldots, y_k) = 0,$$

звідки й випливає шукана ймовірність:

$$\Pr_{x_1,\ldots,x_k}\left\{x_1^{\alpha_1}x_2^{\alpha_2}\cdot\ldots\cdot x_k^{\alpha_k} = x_1x_2\cdot\ldots\cdot x_k\right\} = \\ = \frac{2^k-2}{2^k} = \frac{2^{k-1}-1}{2^{k-1}}.$$

Якщо ж $\gamma = 1$, то потрібно проаналізувати ймовірність такої події:

$$x_1^{\alpha_1}x_2^{\alpha_2}\cdot\ldots\cdot x_k^{\alpha_k} = x_1x_2\cdot\ldots\cdot x_k \oplus 1 \ \ (f_2 = f_1 \oplus 1).$$

Якщо $\alpha_1 = \alpha_2 = \ldots = \alpha_k = 0$, то

$$\Pr_{x_1,\ldots,x_k}\{x_1x_2\cdot\ldots\cdot x_k = x_1x_2\cdot\ldots\cdot x_k \oplus 1\} = 0,$$

інакше, з леми 1 випливає, що

$$\begin{cases}\exists!\left(y_1^{(2)}, y_2^{(2)}, \ldots, y_k^{(2)}\right) : f_2\left(y_1^{(2)}, y_2^{(2)}, \ldots, y_k^{(2)}\right) = 1; \\ \left(y_1^{(2)}, y_2^{(2)}, \ldots, y_k^{(2)}\right) \neq \underbrace{(1,1,\ldots,1)}_{k}, \end{cases}$$

отже лише для двох векторів значення функцій f_2 та $f_1 \oplus 1$ будуть мати однакові значення:

$$\begin{cases} f_1\left(y_1^{(2)}, y_2^{(2)}, \ldots, y_k^{(2)}\right) \oplus 1 = 1; \\ f_2(1,1,\ldots,1) = f_1(1,1,\ldots,1) = 0. \end{cases}$$

$$\Longrightarrow \Pr_{x_1,\ldots,x_k}\left\{x_1^{\alpha_1}\cdot\ldots\cdot x_k^{\alpha_k} = x_1\cdot\ldots\cdot x_k \oplus 1\right\} = \\ = \frac{2}{2^k} = \frac{1}{2^{k-1}}.$$

Отже нульова ймовірність досягається лише за умови, коли $\alpha_1 = \alpha_2 = \ldots = \alpha_k = 0$ та $\gamma = 1$, тому $xdp^f(\alpha_1, \ldots, \alpha_k \to \gamma) > 0$ тоді та тільки тоді, коли ця умова не виконується для жодного біту, що еквівалентно виконанню такої рівності:

$$\overline{\alpha_1}\cdot\overline{\alpha_2}\cdot\ldots\cdot\overline{\alpha_k}\cdot\gamma = 0.$$

Якщо ж $xdp^f(\alpha_1, \ldots, \alpha_k \to \gamma) > 0$, то, відштовхуючись від розглянутих імовірностей для окремих бітів, отримуємо:

$$xdp^f(\alpha_1, \ldots, \alpha_k \to \gamma) = \\ = \left(\frac{2^{k-1}-1}{2^{k-1}}\right)^{wt((\alpha_1\vee\ldots\vee\alpha_k)\wedge\overline{\gamma})}\cdot\left(\frac{1}{2^{k-1}}\right)^{wt((\alpha_1\vee\ldots\vee\alpha_k)\wedge\gamma)} = \\ = \left(\frac{1}{2^{k-1}}\right)^{wt(\alpha_1\vee\ldots\vee\alpha_k)}\cdot\left(2^{k-1}-1\right)^{wt((\alpha_1\vee\ldots\vee\alpha_k)\wedge\overline{\gamma})},$$

що й доводить теорему. ■

Якщо розглянути перетворення такого виду:

$$g_{\circ,\bullet}(x,y,z) = (x\circ y)\bullet z; \\ h_{\circ,\bullet}(x,y,z) = x\circ(y\bullet z),$$

де $\circ, \bullet \in \{\wedge, \vee, |, \downarrow, \to, \leftarrow\}$, то ймовірності їхніх диференціалів, як і в теоремі 2, можуть бути виражені через диференціальні ймовірності функції $f(x,y,z) = xyz$.

3. Диференціальні ймовірності функції мажоризації

Функція мажоризації $maj : (V_n)^3 \to V_n$ — це бітова функція від трьох аргументів:

$$maj(x,y,z) = xy \oplus yz \oplus xz.$$

Функція мажоризації володіє рядом криптографічних особливостей: з її таблиці істинності одразу видно, що вона є збалансованою, і ця властивість ускладнює проведення кореляційних атак. Також було доведено, що ця функція володіє оптимальною алгебраїчною імунністю [5], що, в свою чергу, ускладнює проведення алгебраїчних атак.

Саме ці властивості розглядаються в першу чергу при виборі фільтрувальної функції для потокових шифрів (які зазвичай і є об'єктами кореляційних та алгебраїчних атак), але функція мажоризації все ж рідко використовується в якості фільтрувальної функції через її не найвищий показний нелінійності [6]. Тим не менше, вона була використана в шифрі `A5/1` [7]; в сучасних потокових криптосистемах її якщо й використовують, то в комбінації з іншими функціями, прикладом може слугувати шифр `ACORN` [8] (учасник конкурсу `CAESAR`). Окрім потокових шифрів, функція мажоризації використовується й у стандартах гешування `SHA-1` та `SHA-2` [9], а також в блоковому шифрі `SHACAL-2` [10], який є фіналістом конкурсу `NESSIE`, та основою якого, власне, і являється `SHA-2`. Тому є сенс розглянути диференціальні ймовірності функції мажоризації.

Теорема 3. $\forall\alpha,\beta,\delta,\gamma \in V_n$ справедливі такі твердження:

1) $xdp^{maj}(\alpha,\beta,\delta\to\gamma) \neq 0 \iff eq(\alpha,\beta,\delta,\overline{\gamma}) = 0$;
2) $xdp^{maj}(\alpha,\beta,\delta\to\gamma) \neq 0$, то

$$xdp^{maj}(\alpha,\beta,\delta\to\gamma) = \left(\frac{1}{2}\right)^{n-wt(eq(\alpha,\beta,\delta))},$$

де $eq(x,y,z)$ — це вектор рівності бітів:

$$\forall i \in \overline{1,n} : eq(x,y,z)_i = 1 \iff x_i = y_i = z_i.$$

Доведення. Ймовірність диференціалу $xdp^{maj}(\alpha,\beta,\delta\to\gamma)$ має такий вид:

$$\Pr_{x,y,z}\{(x\oplus\alpha)(y\oplus\beta)\oplus(y\oplus\beta)(z\oplus\delta)\oplus \\ \oplus(x\oplus\alpha)(z\oplus\delta) = xy\oplus yz\oplus xz\oplus\gamma\}.$$

Розглянемо i-тий біт підімовірнісного рівняння:

$$(x_i\oplus\alpha_i)(y_i\oplus\beta_i)\oplus(y_i\oplus\beta_i)(z_i\oplus\delta_i)\oplus \\ (x_i\oplus\alpha_i)(z_i\oplus\delta_i) = x_iy_i\oplus y_iz_i\oplus x_iz_i\oplus\gamma_i,$$

$$x_i y_i \oplus \beta_i x_i \oplus \alpha_i y_i \oplus \alpha_i \beta_i \oplus y_i z_i \oplus \delta_i y_i \oplus \beta_i z_i \oplus \\ \oplus \beta_i \delta_i \oplus x_i z_i \oplus \delta_i x_i \oplus \alpha_i z_i \oplus \alpha_i \delta_i = \\ = x_i y_i \oplus y_i z_i \oplus x_i z_i \oplus \gamma_i,$$

звідки випливає, що

$$(\beta_i \oplus \delta_i)\, x_i \oplus (\alpha_i \oplus \delta_i)\, y_i \oplus (\alpha_i \oplus \beta_i)\, z_i = \\ = \alpha_i \beta_i \oplus \beta_i \delta_i \oplus \alpha_i \delta_i \oplus \gamma. \quad (3)$$

Позначимо символом p_i ймовірність виконання рівняння (3), значення p_i для всіх можливих наборів $\alpha_i, \beta_i, \delta_i, \gamma_i$ наведені у таблиці 2.

Таблиця 2. Ймовірності p_i виконання рівняння (3).

α_i	β_i	δ_i	γ_i	рівняння	p_i
0	0	0	0	$0 = 0$	1
0	0	0	1	$0 = 1$	0
0	0	1	0	$x_i \oplus y_i = 0$	1/2
0	0	1	1	$x_i \oplus y_i = 1$	1/2
0	1	0	0	$x_i \oplus z_i = 0$	1/2
0	1	0	1	$x_i \oplus z_i = 1$	1/2
0	1	1	0	$y_i \oplus z_i = 1$	1/2
0	1	1	1	$y_i \oplus z_i = 0$	1/2
1	0	0	0	$y_i \oplus z_i = 0$	1/2
1	0	0	1	$y_i \oplus z_i = 1$	1/2
1	0	1	0	$x_i \oplus z_i = 1$	1/2
1	0	1	1	$x_i \oplus z_i = 0$	1/2
1	1	0	0	$x_i \oplus y_i = 1$	1/2
1	1	0	1	$x_i \oplus y_i = 0$	1/2
1	1	1	0	$0 = 1$	0
1	1	1	1	$0 = 0$	1

З таблиці 2 бачимо, що ймовірність p_i дорівнює нулю тоді та тільки тоді, коли $\alpha_i = \beta_i = \delta_i = \overline{\gamma_i}$, тому, якщо хоча б один біт у векторі $eq(\alpha, \beta, \delta, \overline{\gamma})$ є одиничним, то $xdp^{maj}(\alpha, \beta, \delta \to \gamma) = 0$, що доводить першу частину теореми.

Якщо $xdp^{maj}(\alpha, \beta, \delta \to \gamma) \neq 0$ та $\alpha_i = \beta_i = \delta_i$, то рівняння виконується завжди, інакше — з ймовірністю 1/2, тому $xdp^{maj}(\alpha, \beta, \delta \to \gamma) = \left(\frac{1}{2}\right)^{n-k}$, де k — кількість одиничних бітів у векторі $eq(\alpha, \beta, \delta)$, з чого випливає друга частина теореми. ■

Висновки

У даній роботі розглядались диференціальні властивості LRX-перетворень, зокрема отримано аналітичні вирази ймовірностей диференціалів для функції мажоризації та операції логічного ТА. Останній результат був узагальнений для k-кратної функції логічного ТА. Одержані ймовірності можуть бути використати для побудови більш точних оцінок стійкості LRX-криптосистем.

Перелік використаних джерел

1. *Aumasson J.-P.*, *Jovanovic P.*, *Neves S.* Norx v3.0. — 2016. — DOI: 10.1145/2744769.2747946. — URL: https://competitions.cr.yp.to/round3/norxv30.pdf.
2. The SIMON and SPECK Families of Lightweight Block Ciphers / R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers. — 2013. — DOI: 10.1145/2744769.2747946. — URL: https://eprint.iacr.org/2013/404.
3. *Lipmaa H.*, *Moriai S.* Efficient Algorithms for Computing Differential Properties of Addition. — 2001. — DOI: https://doi.org/10.1007/3-540-45473-X_28. — URL: https://eprint.iacr.org/2001/001.
4. *Biryukov A.*, *Roy A.*, *Velichkov V.* Differential Analysis of Block Ciphers SIMON and SPECK. — 2014. — DOI: 10.1007/978-3-662-46706-0_28. — URL: https://eprint.iacr.org/2014/922.
5. *Méaux P.* On the Fast Algebraic Immunity of Majority Functions. — 2019. — DOI: 10.1007/978-3-030-30530-7_5. — URL: https://eprint.iacr.org/2019/999.
6. *Cusick T. W.* Simpler proof for nonlinearity of majority function. — 2017. — DOI: 10.1016/j.dam.2021.02.031. — eprint: arXiv:1710.02034. — URL: https://arxiv.org/abs/1710.02034.
7. *Barkan E.*, *Biham E.*, *Keller N.* Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. — 2003. — DOI: https://doi.org/10.1007/978-3-540-45146-4_35. — URL: https://link.springer.com/chapter/10.1007/978-3-540-45146-4_35.
8. *Wu H.* ACORN: A Lightweight Authenticated Cipher (v3). — 2016. — URL: https://competitions.cr.yp.to/round3/acornv3.pdf.
9. *NIST.* Secure Hash Standard (SHS). — 2015. — DOI: 10.6028/NIST.FIPS.180-4. — URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.
10. The NESSIE Book: Final Report of European Project IST-1999-12324 / S. Murphy, B. Preneel [та ін.]. — 2004. — С. 555—557. — URL: https://pure.royalholloway.ac.uk/en/publications/the-nessie-book-final-report-of-european-project-ist-1999-12324.