КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (9), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.9.623
УДК 621.3.019.3+004.056

Гулак Геннадій Миколайович
кандидат технічних наук, доцент
завідувач лабораторії досліджень кібербезпеки науково-дослідного відділу
ІПММС НАН України, Київ, Україна
ORCID : 0000-0001-9131-9233
h.hulak@ukr.net

СКЛАДНІСТЬ АЛГОРИТМУ ОЦІНЮВАННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ СТВОРЕННЯ ГАРАНТОЗДАТНИХ АВТОМАТИЗОВАНИХ СИСТЕМ

Анотація. Досліджуються складність алгоритму розв'язання систем лінійних рівнянь із спотвореними правими частинами шляхом списочного декодування "вкорочених" кодів ріда-маллера першого порядку, що призначений для використання у методі оцінки функціональної безпеки криптографічних алгоритмів криптографічних підсистем гарантоздатних автоматизованих систем, що використовуються для обробки інформації та управління на об'єктах критичної інфраструктури та суспільно важливих об'єктах . В даної роботі запропоновано розв'язок задачі для оцінювання складності запропонованого алгоритму. Зокрема, отримані верхні оцінки середньої трудомісткості для загального випадку та максимальної трудомісткості запропонованого алгоритму для множин спеціального вигляду, що пов'язані з відновленням спотворених лінійних рекурент максимального періоду над полем з двох елементів. Наведено також досяжну верхню межу обсягу списку, який формується з використанням запропонованого алгоритму. Отримані результати свідчать про те, що при визначених співвідношеннях між параметрами запропонований раніше алгоритм має меншу часову складність у порівнянні з раніше відомим детермінованим алгоритмом аналогічного призначення, який базується на швидкому перетворенні Адамара. Це означає можливість застосування більш ефективного інструменту для оцінки вразливості криптографічних підсистем щодо потужних кібератак, конче забезпечувати більш достовірну оцінку їх функціональної безпеки

Ключові слова: гарантоздатність, достовірність, функціональна безпека, функціональна безпека криптографічної підсистеми, криптографічна атака, стійкість криптографічного перетворення, списочне декодування, відстань Геммінга, швидке перетворення Адамара, перетворення Уолша-Адамара, код Ріда-Маллера.

1. ВСТУП

У роботі [1] відмічено, що гарантоздатність автоматизованих систем переробки та управління, які використовуються на об'єктах критичної інфраструктури суттєво залежить від функціональної безпеки криптографічної підсистеми, та в першу чергу від практичної криптографічної стійкості застосованих алгоритмів. За визначенням, практична стійкість криптосистеми оцінюється як середній обсяг роботи яку необхідно виконати для розв'язання задачі дешифрування [2,3] або, інакше, як середня складність найкращого алгоритму розв'язання вказаної задачі [4]. Однією з поширених атак на криптосистеми є атака на основі методів лінеаризації вихідних криптографічних перетворень [5,6].

Для розв'язання систем лінійних рівнянь із спотвореними правими частинами в роботі [1] запропоновано модифікований детермінований алгоритм списочного декодування "вкорочених" кодів Ріда-Маллера (РМ) першого порядку, що є безпосереднім узагальненням відомого алгоритму И. Думера, Г. Кабатянского та С. Тавернье (ДКТ) списочного декодування звичайних кодів РМ [7]. Нагадаємо, що

ISSN 2663 - 4023

алгоритм [1] формує для даних множини $M \subseteq V_m = \{0,1\}^m$, функції $b: M \to \{0,1\}$ і числа T таких, що $m < t = |M| \le 2^m$, $1 \le T \le 2^m$, список усіх лінійних булевих функцій m змінних, які знаходяться від функції b на відстані не більше за T. Він може бути застосований до розв'язання систем булевих лінійних рівнянь із спотвореними правими частинами, а також повністю випадкових систем лінійних рівнянь (з довільною правою частиною b) від помірної кількості змінних ($m \le 28$).

В [1] зазначено, що оцінювання часової складності запропонованого алгоритму є досить складною задачею. У даної роботі запропоновано її розв'язок. Зокрема, отримані верхні оцінки середньої та максимальної трудомісткості запропонованого алгоритму, остання – для множин M спеціального вигляду, що пов'язані з відновленням спотворених лінійних рекурентних послідовностей максимального періоду над полем з двох елементів. Наведено також досяжну верхню межу обсягу списку, який формується з використанням запропонованого алгоритму.

Отримані результати свідчать про те, що при певних співвідношеннях між параметрами m, t і T алгоритм [1] має меншу часову складність у порівнянні з раніше відомим детермінованим алгоритмом аналогічного призначення [8], який базується на швидкому перетворенні Адамара (ШПА) [9].

2. ОСНОВНІ ПОНЯТТЯ, ДОПОМІЖНІ ВІДОМОСТІ ТА ФОРМУЛЮВАННЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ

Наведемо стислі відомості про алгоритм списочного декодування "вкорочених" кодів РМ першого порядку, що запропоновано в [1].

Зауважимо, що зазначений алгоритм застосовується до вхідних даних $(M,\ b,\ T)$, де $M \subseteq V_m$, $b: M \to \{0,1\}$, $m < t = |M| \le 2^m$, $1 \le T \le 2^m$. Елементи множини M записуються в деякому фіксованому порядку один за одним у вигляді матриці A розміру $t \times m$, а частково визначена функція b ототожнюється з двійковим вектором довжини t її значень, що є правою частиною системи лінійних рівнянь

$$Ax^T = b. \qquad (1)$$

Алгоритм формує за вхідними даними $(M,\ b,\ T)$ список, який складається з усіх лінійних булевих функцій m змінних, що знаходяться від функції b на відстані не більше за T (або, що теж саме, список усіх векторів $x \in V_m$, які задовольняють умові $d(Ax^T, b) \le T$, де $d(u, v)$ – відстань Геммінга між векторами u та v).

Далі вважатимемо, що значення T є менше за $t/2$, тобто

$$T = \delta t = 1/2\,(1-\varepsilon)t,\ \varepsilon \in (0,1). \qquad (2)$$

Введемо також наступні позначення:

- $\Im_M$ – множина усіх часткових БФ, області визначення яких містять множину M;

- $RM(1,m)$ – код РМ першого порядку довжини 2^m, що складається з векторів значень усіх афінних булевих функцій, тобто функцій вигляду

$$c(x) = c(x_1,\ldots,x_m) = c_1x_1 \oplus \ldots \oplus c_mx_m \oplus c_{m+1},\ x = (x_1,\ldots,x_m) \in V_m,$$

де $c_1, \ldots, c_{m+1} \in \{0,1\}$;

ISSN 2663 - 4023

- $RM_0(1,m)=\{c\in RM(1,m): c(0,...,0)=0\}$ – код Адамара [10] довжини 2^m.

Для будь-яких $f,g\in\Im_M$ позначимо

$$d(f,g\,|\,M)=\sum_{x\in M}\delta(f(x),g(x)),$$

де $\delta(u,v)=1$, якщо $u=v$; $\delta(u,v)=0$ – у протилежному випадку. Нарешті, введемо до розгляду множини

$$L_T(M,b)=\{c\in RM(1,m): d(c,b\,|\,M)\le T\} \tag{3}$$

та

$$L_{0,T}(M,b)=L_T(M,b)\cap RM_0(1,m), \tag{4}$$

де T визначається за формулою (2). Зрозуміло, що множина (3) (множина (4)) являє собою сукупність усіх афінних (лінійних) БФ, які знаходяться на відстані не більше за T від часткової функції $b\in\Im_M$. Отже, алгоритм розв'язання СЛР (1) шляхом списочного декодування "вкороченого" коду РМ [1] полягає у побудові множини (4) за вхідними даними (M,b,T).

Наведемо стислий опис цього алгоритму, що необхідно для подальшого аналізу його часової складності.

Для будь-яких $j\in\overline{0,m-1}$, $a=(a_{j+1},\ldots,a_m)\in V_{m-j}$, $f,g\in\Im_M$ позначимо

$$M_a=\{(x_1,\ldots,x_m)\in M:\ x_{j+1}=a_{j+1},\ldots,x_m=a_m\},$$
$$\Delta(f,g\,|\,M_a)=\min\{d(f,g\,|\,M_a),d(f,g\oplus 1\,|\,M_a)\},$$
$$\Delta^{(j)}(f,g)=\sum_{a\in V_{m-j}}\Delta(f,g\,|\,M_a).$$

Покладемо

$$\hat{L}_T^{(j)}(M,b)=\{c^{(j)}\in RM_0(1,j):\ \Delta^{(j)}(c^{(j)},b)\le T\},\ j\in\overline{0,m-1}. \tag{5}$$

Алгоритм побудови множини (4)*, що представлено в* [1], складається з m кроків, на *j*-му з яких ($j\in\overline{1,m-1}$) будується множина $\Lambda_T^{(j)}(M,b)$ така, що

$$\Lambda_T^{(j)}(M,b)\subseteq\hat{L}_T^{(j)}(M,b), \tag{6}$$

для кожного елемента $c^{(j)}$ якої формуються два набори чисел: $D_0(c^{(j)})=(d_0(c^{(j)}\,|\,a):a\in V_{m-j})$ та $D_1(c^{(j)})=(d_1(c^{(j)}\,|\,a):a\in V_{m-j})$, де

$$d_\nu(c^{(j)}\,|\,a)=d(c^{(j)},b\oplus\nu\,|\,M_a),\ a\in V_{m-j},\ \nu\in\{0,1\}. \tag{7}$$

На останньому, *m*-му, кроці алгоритму формується шуканий список, що складається з усіх функцій $c\in L_{0,T}(M,b)$ поряд із відповідними їм відстанями Геммінга $d(c,b\,|\,M)$.

Покладемо

$$c^{(0)}\equiv 0,\ \Lambda_T^{(0)}(M,b)=\{c^{(0)}\}, \tag{8}$$

$$d_{\nu}(c^{(0)} \mid a) = \begin{cases} 0, a \notin M; \\ b(a) \oplus \nu, a \in M, \end{cases} \quad (9)$$

де $b(a)$ – значення часткової БФ b на двійковому наборі $a \in M$, $\nu \in \{0,1\}$.

Нехай $j \in \overline{1, m-1}$ і вже побудовані множина $\Lambda_T^{(j-1)}(M,b)$ та набори чисел $D_0(c^{(j-1)})$, $D_1(c^{(j-1)})$, де $c^{(j-1)} \in \Lambda_T^{(j-1)}(M,b)$. Тоді на j-му кроці алгоритму розглядаються усі функції вигляду $c^{(j)} = c^{(j-1)}(x_1,\ldots,x_{j-1}) \oplus c_j x_j$, де $c^{(j-1)} \in \Lambda_T^{(j-1)}(M,b)$, $c_j \in \{0,1\}$. Для кожної з них

1) за відомими наборами $D_0(c^{(j-1)})$ та $D_1(c^{(j-1)})$ обчислюються значення (7):

$$d_{\nu}(c^{(j)} \mid a) = d_{\nu}(c^{(j-1)} \mid (0,a)) + d_{\nu \oplus c_j}(c^{(j-1)} \mid (1,a)),\ a \in V_{m-j},\ \nu \in \{0,1\}; \quad (10)$$

2) знаходяться числа:

$$\Delta(c^{(j)}, b \mid M_a) = \min\{d_0(c^{(j)} \mid a), d_1(c^{(j)} \mid a)\},\ a \in V_{m-j}; \quad (11)$$

3) перевіряється умова:

$$\Delta^{(j)}(c^{(j)}, b) = \sum_{a \in V_{m-j}} \Delta(c^{(j)}, b \mid M_a) \le T, \quad (12)$$

за виконанням якої функція $c^{(j)}$ включається до множини $\Lambda_T^{(j)}(M,b)$, що формується, та відбраковується – у протилежному випадку.

На останньому кроці алгоритму розглядаються усі функції вигляду $c^{(m)} = c^{(m-1)}(x_1,\ldots,x_{m-1}) \oplus c_m x_m$, де $c^{(m-1)} \in \Lambda_T^{(m-1)}(M,b)$, $c_m \in \{0,1\}$, для кожної з яких за відомими наборами $D_0(c^{(m-1)})$, $D_1(c^{(m-1)})$ обчислюються значення

$$d(c^{(m)}, b \mid M) = d_0(c^{(m-1)} \mid 0) + d_{c_m}(c^{(m-1)} \mid 1). \quad (13)$$

Далі формується множина $\Lambda_T^{(m)}(M,b)$, що складається з усіх функцій $c^{(m)}$, які задовольняють умові $d(c^{(m)}, b \mid M) \le T$.

В [1] показано, що $\Lambda_T^{(m)}(M,b) = L_{0,T}(M,b)$. Отже, елементи множини $\Lambda_T^{(m)}(M,b)$ складають шуканий список усіх лінійних функцій, які знаходяться на відстані не більше за T від часткової функції b.

Для будь-яких $M \subseteq V_m$, $b \in \Im_M$ і T вигляду (2) позначимо $\tau_T(M,b)$ *часову складність викладеного алгоритму*, яка дорівнює числу двійкових операцій, що виконуються при його застосуванні до вхідних даних $(M,\ b,\ T)$. Позначимо

$$\bar{\tau}_T(m,t) = 2^{-t} \binom{2^m}{t}^{-1} \sum_{(M,\ b)} \tau_T(M,b) \quad (14)$$

середню часову складність алгоритму (зауважимо, що підсумування у формулі (14) здійснюється за всіма впорядкованими парами $(M,\ b)$, де $M \subseteq V_m$, $|M| = t$,

$b \in \Im_M$, кількість яких дорівнює $2^t \begin{pmatrix} 2^m \\ t \end{pmatrix}$). Нарешті, позначимо $C_1 j$ та $C_2 j$ відповідно складності алгоритмів додавання та порівняння (більше-менше) двох j-розрядних двійкових цілих чисел. Покладемо $C_3 = \max\{2, C_1\}$,

$$C = 2C_2 + 3C_3. \tag{15}$$

Наступна теорема встановлює верхню межу параметра (14).

Теорема 1. Якщо виконується умова (2),

$$t \geq 2^{m-\mu}(1-h(\delta))^{-1}, \tag{16}$$

де $h(x) = -x\log x - (1-x)\log(1-x)$, $x \in [0,1]$, $\mu \in \mathbf{N}$,

$$\mu \leq m - 1 - \log m, \tag{17}$$

тоді середня часова складність алгоритму задовольняє нерівності

$$\bar{\tau}_T(m,t) \leq t + C(m^2 + 2^{m-1}(\mu+2)(\mu+3)), \tag{18}$$

де C визначається за формулою (15).

Наслідок 1. В умовах теореми 1 за виконанням нерівності $m/t < 1/4(1-h(\delta))$ справедливо таке співвідношення:

$$\bar{\tau}_T(m,t) = O\left(2^m\left(m - \log t(1-h(\delta))\right)^2\right),\ m \to \infty. \tag{19}$$

Зауважимо, що при $t = 2^m$ викладений алгоритм фактично співпадає (з точністю до останнього кроку) з алгоритмом ДКТ [7]. В цьому випадку за виконанням нерівності $\log \varepsilon^{-2} \leq m - \log m - 3$ середню трудомісткість обох алгоритмів можна оцінити за формулою (19):

$$\bar{\tau}_T(m,2^m) = O\left(2^m \log^2(1-h(\delta))^{-1}\right),$$

а максимальну трудомісткість – за формулою [2]

$$\tau_{\text{ДКТ}}(m,T) = O\left(2^m \log^2(\varepsilon^{-2})\right).$$

У таблиці 1 наведено чисельні значення верхньої межі (18) параметра (14), які розраховані для низки значень δ, m, μ та t при $C_1 = 5$, $C_2 = 1$. В двох останніх колонках таблиці показані значення двійкової складності алгоритму [8], що базується на швидкому перетворенні Адамара:

$$\tau_{\text{ШПА}}(t,m) = C_1 m 2^m (\lfloor \log t \rfloor + 1),$$

та виграшу в складності $\omega = \dfrac{\tau_{\text{ШПА}}(t,m)}{\bar{\tau}_T(t,m)}$, який досягається при застосуванні алгоритму [1] у порівнянні з алгоритмом ШПА.

Як видно з таблиці, при $m = 24$, $t = 4 \cdot 10^6$ складання списку усіх лінійних БФ, що знаходяться на відстані не більше за $T = 0{,}40t$ від даної часткової функції b, з використанням викладеного вище алгоритму потребує, в середньому, майже в 3 рази менше двійкових операцій, ніж при застосуванні алгоритму ШПА.

ISSN 2663 - 4023

Таблиця 1

Результати порівняння середньої часової складності алгоритму [1] зі складністю алгоритму ШПА [8]

δ	m	t	μ	$\overline{\tau}_T(t,m)$	$\tau_{ØÏÀ}(t,m)$	ω
0,3	16	20000	5	$0{,}31221\cdot 10^8$	$0{,}8015\cdot 10^8$	2,6
0,4	16	20000	7	$0{,}5015\cdot 10^8$	$0{,}8015\cdot 10^8$	1,6
0,3	18	100000	7	$0{,}1248\cdot 10^9$	$0{,}4154\cdot 10^9$	3,3
0,4	18	100000	7	$0{,}2006\cdot 10^9$	$0{,}4154\cdot 10^9$	2,1
0,3	24	4000000	6	$0{,}1027\cdot 10^{11}$	$0{,}4616\cdot 10^{11}$	4,5
0,4	24	4000000	8	$0{,}1569\cdot 10^{11}$	$0{,}4616\cdot 10^{11}$	2,9

Надалі розглянемо окремий випадок, коли множина M має такий вигляд:

$$M=\{(s(i),s(i+1),\dots,s(i+m-1)):i\in\overline{0,t-1}\},\qquad(20)$$

де $(s(0),s(1),\dots)$ – ненульова лінійна рекурентна послідовність з примітивним характеристичним поліномом $h(x)\in\mathbf{GF}(2)[x]$ степеня $m>1$. Позначимо $\tau_T^*(m,t)$ максимальне значення трудомісткості $\tau_T(M,b)$ за всіма множинами M вигляду (20) та функціями $b:M\to\{0,1\}$, покладемо

$$\nu_{m,t}(h)=\max_{s\neq 0}\left|\sum_{i=0}^{t-1}(-1)^{s(i)}\right|,\qquad(21)$$

де максимум береться за всіма ненульовими лінійними рекурентними послідовностями $s=(s(0),s(1),\dots)$ з характеристичним поліномом $h(x)$.

Теорема 2. Нехай виконується умова (2):

$$t\geq 2^{(m-\mu)/2}\hat{\nu}_{m,T}\,\varepsilon^{-2},\qquad(22)$$

де $\mu\in\mathbf{Z}$, $0\leq\mu\leq m-2$ та $\hat{\nu}_{m,T}\geq\nu_{m,t}(h)$, тоді справедлива нерівність

$$\tau_T^*(m,t)\leq t+C(m^2t2^{(m-\mu)/2+1}(\hat{\nu}_{m,t})^{-1}+2^{m-1}(\mu+2)(\mu+3)),\qquad(23)$$

де C визначається за формулою (15).

Нерівність (23), поряд з відомими оцінками $\hat{\nu}_{m,T}$ параметра (21) [11–13], дозволяє отримати вираз для верхньої межі трудомісткості $\tau_T^*(m,t)$, що явно залежить від m, t, ε. Відзначимо наступне твердження, що випливає з теореми 2 та нерівності $\nu_{m,t}(h)\leq 2^{m/2}(m+1)$ [11].

Наслідок 2. Нехай

$$t\geq 2^m(m+1)^{-\gamma},\ \varepsilon>2^{-(m-2)/4}(m+1)^{(\gamma+1)/2},$$

де $\gamma=\text{const}$, $\gamma>0$, тоді за виконанням умови (2)

$$\tau_T^*(m,t) = O\left(2^m \log^2(\varepsilon^{-2}(m+1)^{\gamma+1})\right),\ m \to \infty.$$

На завершення наведемо верхню оцінку обсягу списку, що формується з використанням алгоритму [1], тобто потужність множини (3):

$$|L_{0,T}(M,b)| \le |L_T(M,b)| \le \varepsilon^{-2} 2^m t^{-1}. \qquad (24)$$

Для доведення формули (24) позначимо

$$\hat{b}(c) = \sum_{x \in M} (-1)^{b(x) \oplus c(x)},\ c \in RM_0(1,m),$$

коефіцієнти Фур'є функції, яка дорівнює $(-1)^{b(x)}$ при $x \in M$ та 0 – при $x \in V_m \setminus M$. З формули $\hat{b}(c) = 2\,d(c,b \mid M) - t$, $c \in RM_0(1,m)$, випливає, що множина $L_T(M,b)$ складається з усіх афінних БФ $\tilde{c} = c(x_1,\ldots,x_m) \oplus c_{m+1}$, де $c = c(x_1,\ldots,x_m) \in RM_0(1,m)$, $c_{m+1} \in \{0,1\}$, які задовольняють умові

$$(c_{m+1} = 0, \hat{b}(c) \ge \varepsilon t) \text{ або } (c_{m+1} = 1, \hat{b}(c) \le -\varepsilon t).$$

Отже,

$$|L_T(M,b)| = |\{c \in RM_0(1,m) : |\hat{b}(c)| \ge \varepsilon t\}| =$$

$$= \sum_{\substack{c \in RM_0(1,m): \\ |\hat{b}(c)| \ge \varepsilon t}} 1 \le \varepsilon^{-2} t^{-2} \sum_{\substack{c \in RM_0(1,m): \\ |\hat{b}(c)| \ge \varepsilon t}} |\hat{b}(c)|^2 \le \varepsilon^{-2} t^{-2} \sum_{c \in RM_0(1,m)} |\hat{b}(c)|^2 = \varepsilon^{-2} 2^m t^{-1},$$

де останнє співвідношення випливає з рівності Парсеваля [14]. Таким чином, справедлива формула (24), що і треба було довести.

Зауважимо, що при $M = V_m$ оцінка (24) не залежить від m: для будь-якої функції $b: V_m \to \{0,1\}$ число афінних БФ m змінних, які знаходяться від b на відстані не більше за $2^{m-1}(1-\varepsilon)$, не перевищує ε^{-2} (наприклад, число афінних БФ, що співпадають з функцією b з імовірністю $p = 0{,}51$, не перевищує $(2p-1)^2 = 2500$). Отже, для помірних значень ε список вигляду (3) не може бути надто великим. Відзначимо також, що оцінку (24), взагалі кажучи, не можна підсилити: при $M = V_m$ вона досягається, якщо b є бент-функцією (і тільки в цьому випадку) [7,[15].

3. ДОВЕДЕННЯ ТЕОРЕМИ 1

Доведемо ряд допоміжних тверджень.

Лема 1. Нехай $M \subseteq V_m$, $b \in \Im_M$, $m < |M| = t \le 2^m$ і T має вигляд (2). Тоді для складності алгоритму при вхідних даних (M, b, T) справедлива нерівність

$$\tau_T(M,b) \le t + 2C \sum_{j=1}^{m} 2^{m-j}(j+1)\,|\Lambda_T^{(j-1)}(M,b)|, \qquad (25)$$

де $\Lambda_T^{(j-1)}(M,b)$ є списком, що формується на $(j-1)$-му кроці алгоритму, $j \in \overline{1,m}$, а C визначається за формулою (15).

ISSN 2663 - 4023

Доведення. Позначимо $\tau_T^{(j)}(M,b)$ двійкову часову складність j-го кроку алгоритму, $j \in \overline{1,m}$. Помітимо, що обчислення чисел (9) на початку алгоритму зводиться до інвертування координат вектору b, що потребує t булевих додавань. Отже,

$$\tau_T(M,b) = t + \sum_{j=1}^{m} \tau_T^{(j)}(M,b). \qquad (26)$$

Зафіксуємо число $j \in \overline{1,m-1}$. Помітимо, перед усім, що, згідно формулам (9) та (10), числа (7) мають розрядність $j+1$ (доведення – індукція по j). Далі, на j-му кроці алгоритму для кожної функції $c^{(j)} = c^{(j-1)}(x_1,\ldots,x_{j-1}) \oplus c_j x_j$, де $c^{(j-1)} \in \Lambda_T^{(j-1)}(M,b)$, $c_j \in \{0,1\}$,

1) обчислення значень (10) потребує $2 \cdot 2^{m-j}(C_1 j + 1)$ двійкових операцій;

2) знаходження чисел (11) вимагає $2^{m-j} C_2 (j+1)$ двійкових операцій;

3) перевірка умови (12) потребує додавання 2^{m-j} чисел розрядності $(j+1)$ та одного порівняння двох чисел, що мають розрядність не більше за $(m+1)$, тобто $2^{m-j} C_1 (j+2) + C_2 (m+1)$ двійкових операцій.

Додаючи наведені значення та приймаючи до уваги, що функція $c^{(j)}$ пробігає множину потужності $2 \mid \Lambda_T^{(j-1)}(M,b) \mid$, отримаємо, що

$$\tau_T^{(j)}(M,b) \le 2 \mid \Lambda_T^{(j-1)}(M,b) \mid (2 \cdot 2^{m-j}(C_1 j + 1) + 2^{m-j} C_2 (j+1) + \\ + 2^{m-j} C_1 (j+2) + C_2 (m+1)), \; j \in \overline{1,m-1}. \qquad (27)$$

Помітимо зараз, що для будь-якого $j \in \overline{1,m-1}$ справедлива нерівність $m+1 \le 2^{m-j}(j+1)$. (Доведення: функція $2^x x^{-1}$ зростає при $x > (\ln 2)^{-1}$; отже, $\frac{2^{j+1}}{j+1} \le \frac{2^{m+1}}{m+1}$ при $j \in \overline{1,m-1}$). Звідси випливає, що

$$2^{m-j} C_2 (j+1) + C_2 (m+1) \le 2 \cdot 2^{m-j} C_2 (j+1), \; j \in \overline{1,m-1}. \qquad (28)$$

Далі, за визначенням константи C_3 (див. формулу (15)) справедливі нерівності

$$2(C_1 j + 1) + C_1 (j+2) \le 2(C_3 (j+1)) + C_3 (j+2) = \\ = 3C_3 j + 2(C_3 + 1) \le 3C_3 (j+1), \; j \in \overline{1,m-1}. \qquad (29)$$

Таким чином, на підставі формул (15), (27) – (29) справедлива наступна оцінка:

$$\tau_T^{(j)}(M,b) \le 2C \mid \Lambda_T^{(j-1)}(M,b) \mid 2^{m-j}(j+1), \; j \in \overline{1,m-1}. \qquad (30)$$

Нарешті, трудомісткість m-го кроку алгоритму складає

$$\tau_T^{(m)}(M,b) \le 2 \mid \Lambda_T^{(m-1)}(M,b) \mid (C_1 m + C_2 (m+1)),$$

що не перевищує значення в правій частині нерівності (30) при $j = m$.

ISSN 2663 - 4023

Отже, на підставі нерівності (26) та нерівності (30) отримаємо остаточну оцінку параметра $\tau_T(M,b)$, яка співпадає з нерівністю (25). Лему доведено.

Зафіксуємо число $j \in \overline{1,m-1}$ та оцінимо зверху середнє значення параметра $|\Lambda_T^{(j)}(M,b)|$ за всіма (M,b). Згідно формулі (6), для будь-якої пари (M,b) справедлива нерівність $|\Lambda_T^{(j)}(M,b)| \le |\hat{L}_T^{(j)}(M,b)|$, тому середнє значення $|\Lambda_T^{(j)}(M,b)|$ за всіма (M,b) не перевищує величини

$$\bar{l}_T^{(j)}(t,m) = 2^{-t}\binom{2^m}{t}^{-1} \sum_{(M,b)} |\hat{L}_T^{(j)}(M,b)|. \qquad (31)$$

Лема 1.2. В умовах леми 1.1 справедливі наступні нерівності:

$$\bar{l}_T^{(j)}(t,m) \le 2^j \cdot 2^{2^{m-j} - t(1-h(\delta))},\ j \in \overline{1,m-1}. \qquad (32)$$

Доведення. Рівність (31) може бути записана у вигляді

$$\bar{l}_T^{(j)}(t,m) = 2^{-t}\binom{2^m}{t}^{-1} \sum_{c^{(j)} \in RM_0(1,j)} \sum_{\substack{(M,b):\\ c^{(j)} \in \hat{L}_T^{(j)}(M,b)}} 1\ , \qquad (33)$$

після чого оцінимо внутрішню суму в правій частині формули (33).

Назвемо функцію $u \in \Im_M$ для кожної множини $M \subseteq V_m$ потужності t *M-припустимою*, якщо виконується умова

$$\Delta^{(j)}(u,0) \le T\,. \qquad (34)$$

Позначимо $\Pi_T^{(j)}(M)$ множину усіх функцій $u \in \Im_M$, що задовольняють умові (34), $p_T^{(j)}(M) = |\Pi_T^{(j)}(M)|$. Помітимо, що на підставі формули (5) співвідношення $c^{(j)} \in \hat{L}_T^{(j)}(M,b)$ рівносильне співвідношенню $c^{(j)} \oplus b \in \Pi_T^{(j)}(M)$. Звідси випливає, що

$$\sum_{\substack{(M,b):\\ c^{(j)} \in \hat{L}_T^{(j)}(M,b)}} 1 \;=\; \sum_{\substack{M \subseteq V_m:\\ |M|=t}} \sum_{u \in \Pi_T^{(j)}(M)} 1 \;=\; \sum_{\substack{M \subseteq V_m:\\ |M|=t}} p_T^{(j)}(M). \qquad (35)$$

Покажемо, що для будь-яких $M \subseteq V_m$, $j \in \overline{1,m-1}$, де $|M| = t$, виконується нерівність

$$p_T^{(j)}(M) \le 2^{2^{m-j} + th(\delta)}. \qquad (36)$$

Тоді на підставі рівнянь (33) та (35) отримаємо

$$\bar{l}_T^{(j)}(t,m) \le 2^{-t}\binom{2^m}{t}^{-1} 2^j \binom{2^m}{t} 2^{2^{m-j} + th(\delta)},\ j \in \overline{1,m-1},$$

що співпадає з формулою (32). Таким чином, для завершення доведення леми залишається переконатися в справедливості нерівності (36).

Нехай $M \subseteq V_m$, $|M| = t$ та $M^{(1)}, \ldots, M^{(k)}$ – усі різні непорожні множини вигляду M_a, де $a \in V_{m-j}$. Відмітимо, що

$$k \le 2^{m-j}. \tag{37}$$

Позначимо $t_i = |M^{(i)}|$, $i \in \overline{1,k}$; для будь-якого $u \in \mathfrak{I}_M$ позначимо $s_i(u)$ мінімум з кількостей одиниць та нулів у векторі значень функції, яка дорівнює обмеженню функції u на множину M_i, $i \in \overline{1,k}$. Іншими словами,

$$s_i(u) = \Delta(u, 0 \mid M^{(i)}),\ i \in \overline{1,k}. \tag{38}$$

Зазначимо, що u є M-припустимою функцією тоді і тільки тоді, коли сума усіх чисел (38) не перевищує T.

Нехай $s_1, \ldots, s_k$ є невід'ємні цілі числа, $0 \le s_i \le t_i/2$, $i \in \overline{1,k}$. Помітимо, що для кожного $i \in \overline{1,k}$ число двійкових векторів $u^{(i)}$ довжини t_i таких, що мінімум з кількостей одиниць та нулів у векторі $u^{(i)}$ дорівнює s_i, є точно $2^{e(s_i)}\binom{t_i}{s_i}$, де $e(s_i) = 1$, якщо $0 \le s_i < t_i/2$; $e(s_i) = 0$, якщо $s_i = t_i/2$ (тобто t_i є парним числом). Звідси випливає, що число функцій $u \in \mathfrak{I}_M$, що задовольняють умовам $s_1(u) = s_1, \ldots, s_k(u) = s_k$, дорівнює

$$2^{e(s_1)+\ldots+e(s_k)}\binom{t_1}{s_1} \ldots \binom{t_k}{s_k}$$

і, отже, число всіх M-припустимих функцій дорівнює

$$p_T^{(j)}(M) = \sum_{\substack{(s_1,\ldots,s_k)\in \mathbf{Z}^k: \\ 0 \le s_i \le t_i/2, i \in \overline{1,k}, \\ s_1+\ldots+s_k \le T}} 2^{e(s_1)+\ldots+e(s_k)}\binom{t_1}{s_1} \ldots \binom{t_k}{s_k}. \tag{39}$$

На підставі формул (37), (39) отримаємо, що

$$p_T^{(j)}(M) \le 2^k \sum_{\substack{(s_1,\ldots,s_k)\in \mathbf{Z}^k: \\ s_1+\ldots+s_k \le T}} \binom{t_1}{s_1} \ldots \binom{t_k}{s_k} \le 2^{2^{m-j}} \sum_{l=0}^{T} \sum_{\substack{(s_1,\ldots,s_k)\in \mathbf{Z}^k: \\ s_1+\ldots+s_k \le T}} \binom{t_1}{s_1} \ldots \binom{t_k}{s_k} =$$

$$= 2^{2^{m-j}} \sum_{l=0}^{T} \binom{t_1+\ldots+t_k}{l} = 2^{2^{m-j}} \sum_{l=0}^{T} \binom{t}{l} \le 2^{2^{m-j}+th(\delta)},$$

де остання нерівність випливає з формули (2) та відомої оцінки Чернова.

Таким чином, справедлива нерівність (36), що і треба було довести. Лему доведено.

Перейдемо безпосередньо до **доведення теореми 1**: переконаємося в тому, що за виконанням співвідношень (2), (16), (17) справедлива оцінка (18).

ISSN 2663 - 4023

На підставі формул (14), (25), (31) має місце нерівність

$$\bar{\tau}_T(t,m) \le t + 2C\sum_{j=1}^{m} 2^{m-j}(j+1)\bar{l}_T^{(j-1)}(t,m),$$

де параметр $\bar{l}_T^{(j-1)}(t,m)$ задовольняє умові (32), а також нерівності $\bar{l}_T^{(j-1)}(t,m) \le 2^{j-1}$, $j \in \overline{1,m}$, яка випливає безпосередньо з його означення. Таким чином,

$$\bar{\tau}_T(t,m) \le t + 2C\sum_{j=1}^{\mu+1} 2^{m-j}(j+1)2^{j-1} + 2C\sum_{j=\mu+2}^{m} 2^{m-j}(j+1)2^{j-1}2^{2^{m-j+1}-t(1-h(\delta))}. \quad (40)$$

Перша сума в правій частині нерівності (40) дорівнює

$$2^m C\sum_{j=1}^{\mu+1}(j+1) \le 2^{m-1}C(\mu+2)(\mu+3), \quad (41)$$

а друга сума в силу нерівності (16) не перевищує значення

$$2^m C\sum_{j=\mu+2}^{m}(j+1)2^{2^{m-j+1}-2^{m-\mu}} \le 2^m C\,2^{m-(\mu+2)+1-2^{m-\mu}}(m+1)(m-(\mu+2)+1) \le$$

$$\le 2^m Cm^2\,2^{-2^{m-\mu-1}} \le 2^m Cm^2\,2^{-m} = Cm^2, \quad (42)$$

де остання нерівність випливає з формули (17).

Отже, на підставі співвідношень (40)–(42) виконується нерівність (18). Теорему доведено.

4. ДОВЕДЕННЯ ТЕОРЕМИ 2

Зафіксуємо множину M вигляду (20) та функцію $b \in \Im_M$. Спочатку отримаємо верхню межу потужності множини (5).

Скористаємося методом, що запропоновано в [7] для випадку, коли $M = V_m$. А саме, кожній функції $f \in RM_0(1,j)$ поставимо у відповідність функцію $f_* : M \to \{0,1\}$, вважаючи для будь-якого $a \in V_{m-j}$ такого, що $M_a \ne \varnothing$,

$$f_*(x) = f(x) \oplus f_a,\ x \in M_a, \quad (43)$$

де $f_a = 0$, якщо $d(f,b \mid M_a) \le d(f \oplus 1, b \mid M_a)$; $f_a = 1$ – в протилежному випадку. Розглянемо код

$$C_* = \{f_* : f \in RM_0(1,j)\}, \quad (44)$$

ISSN 2663 - 4023

що складається не більше ніж з 2^j слів довжини t, які дорівнюють векторам значень функцій f_*. Оцінімо знизу мінімальну відстань коду (44) та застосуємо до нього межу Джонсона.

Нагадаємо формулювання цього результату (див., наприклад, [16], с. 266).

Лема 3. Нехай C – двійковий код довжини t з мінімальною відстанню $d > 2T(1-Tt^{-1})$, де $1 \le T \le t/2$,

$$L_{T,C}(b) = \{c \in C : d(c,b) \le T\},\ b \in V_t. \qquad (45)$$

Тоді

$$|L_{T,C}(b)| \le (1-2T(1-Tt^{-1})d^{-1})^{-1}.$$

Позначимо $L(h)$ векторний простір усіх лінійних рекурент з характеристичним поліномом $h(x)$. Зауважимо, що оскільки $h(x)$ є примітивним поліномом над полем $\mathbf{GF}(2)$, то кожна лінійна рекурентна послідовність $s \in L(h) \setminus \{0\}$ має максимально можливий період $2^m - 1$.

Наступне твердження є ключовим для оцінювання потужності множини (5).

Лема 4. Нехай $j \in \overline{1, m-1}$, $\hat{\nu}_{m,t}$ – довільна верхня межа параметра (21). Тоді для будь-яких різних функцій $f, g \in RM_0(1, j)$ виконується нерівність

$$d(f_*, g_*) \ge \frac{t}{2}(1 - 2^{(m-j)/2}\hat{\nu}_{m,t}t^{-1}). \qquad (46)$$

Доведення. Нехай $c_1x_1 \oplus \cdots \oplus c_jx_j$ – поліном Жегалкіна функції $f \oplus g \ne 0$. Згідно означенню функцій f_*, g_* (див. формулу (43)), обмеження функції $f_* \oplus g_*$ на кожну непорожню множину M_a, де $a \in V_{m-j}$, має вигляд $c_1x_1 \oplus \cdots \oplus c_jx_j \oplus u_a$, де $u_a \in \{0,1\}$. Позначимо символом u продовження функції $a \mapsto u_a$, що задана на множині $\{a \in V_{m-j} : M_a \ne \varnothing\}$, на весь простір V_{m-j}, визначивши її довільним чином на доповненні до цієї множини. Збережемо позначення u_a для значення функції u в довільній точці $a \in V_{m-j}$.

Розглянемо матрицю, що складається з елементів множини M, тобто векторів $(s(i), s(i+1), \ldots, s(i+m-1))$, $i \in \overline{0, t-1}$, які записані один під одним. Помітимо, що стовбці цієї матриці є початковими відрізками довжини t лінійних рекурент $\sigma_1, \ldots, \sigma_m$, де $\sigma_k(i) = s(i+k)$, $i = 0, 1, \ldots$, $k \in \overline{1, m}$, які утворюють базис векторного простору $L(h)$. Задаємо ЛРП $s_1, s_2, \ldots, s_{m-j+1}$, вважаючи для будь-якого $i = 0, 1, \ldots$

$$s_1(i) = c_1\sigma_1(i) \oplus \cdots \oplus c_j\sigma_j(i),\ s_2(i) = \sigma_{j+1}(i), \ldots, \sigma_{m-j+1}(i) = \sigma_m(i). \qquad (47)$$

Зауважимо, що в силу умови $(c_1, \ldots, c_j) \ne 0$ лінійні рекурентні послідовності (47) є лінійно незалежними над полем $\mathbf{GF}(2)$.

На підставі даних означень справедливі наступні рівності:

ISSN 2663 - 4023

$$d(f_*, g_*) = \sum_{a \in V_{m-j}} d(f_* \oplus g_*, 0 \mid M_a) =$$

$$= \sum_{(a_2,\ldots,a_{m-j+1}) \in V_{m-j}} \sum_{i=0}^{t-1} I\{s_1(i) = a_1, s_2(i) = a_2, \ldots, s_{m+j-1}(i) = a_{m+j-1}\}, \quad (48)$$

де $a_1 = \bar{u}_a = u_a \oplus 1$, $a = (a_2,\ldots,a_{m-j+1}) \in V_{m-j}$, I – індикатор зазначеної події.

Перетворимо вираз в правій частині рівності (48):

$$d(f_*, g_*) = \sum_{(a_2,\ldots,a_{m-j+1}) \in V_{m-j}} \sum_{i=0}^{t-1} \prod_{l=1}^{m-j+1} 1/2 \cdot (1 + (-1)^{s_l(i) \oplus a_l}) =$$

$$= 2^{-(m-j+1)} \sum_{a \in V_{m-j}} \sum_{i=0}^{t-1} \sum_{x=(x_1,\ldots,x_{m-j+1}) \in V_{m-j+1}} (-1)^{(s_1(i) \oplus a_1)x_1 \oplus \ldots \oplus (s_{m-j+1}(i) \oplus a_{m-j+1})x_{m-j+1}} =$$

$$= t/2 + 2^{-(m-j+1)} \sum_{\substack{x \in V_{m-j+1}: \\ x \neq 0}} \sum_{i=0}^{t-1} (-1)^{s_1(i)x_1 \oplus \ldots \oplus s_{m-j+1}(i)x_{m-j+1}} \times$$

$$\times \sum_{a \in V_{m-j}} (-1)^{\bar{u}_a x_1 \oplus a_2 x_2 \oplus \ldots \oplus a_{m-j+1}x_{m-j+1}}. \quad (49)$$

Помітимо, що для будь-якого $x = (0, x_2, \ldots, x_{m-j+1}) \in V_{m-j+1} \setminus \{0\}$ сума за всіма $a \in V_{m-j}$ у правій частині формули (49) дорівнює нулю. Отже,

$$d(f_*, g_*) = t/2 +$$

$$+ 2^{-(m-j+1)} \sum_{\tilde{x}=(x_2,\ldots,x_{m-j+1}) \in V_{m-j}} \sum_{i=0}^{t-1} (-1)^{s_1(i) \oplus s_2(i)x_2 \oplus \ldots \oplus s_{m-j+1}(i)x_{m-j+1}} \times$$

$$\times \sum_{a \in V_{m-j}} (-1)^{\bar{u}_a \oplus a_2 x_2 \oplus \ldots \oplus a_{m-j+1}x_{m-j+1}},$$

звідки випливає, що

$$| d(f_*, g_*) - t/2 | \le 2^{-(m-j)} \cdot 1/2 \sum_{\tilde{x} \in V_{m-j}} | \hat{u}_{\tilde{x}} | \left| \sum_{i=0}^{t-1} (-1)^{s_{\tilde{x}}(i)} \right|, \quad (50)$$

де

$$\hat{u}_{\tilde{x}} = \sum_{a \in V_{m-j}} (-1)^{\bar{u}_a \oplus a_2 x_2 \oplus \ldots \oplus a_{m-j+1}x_{m-j+1}}$$

є коефіцієнт Уолша-Адамара функції $\bar{u}: V_{m-j} \to \{0,1\}$ в точці $\tilde{x} = (x_2,...,x_{m-j+1})$, $s_{\tilde{x}}(i) = s_1(i) \oplus s_2(i)x_2 \oplus \cdots \oplus s_{m-j+1}(i)x_{m-j+1}$, $i = 0, 1, ...$

Помітимо зараз, що на підставі лінійної незалежності рекурент (47) та означення параметра (21) справедливі нерівності

$$|\sum_{i=0}^{t-1}(-1)^{s_{\tilde{x}}(i)}| \le \nu_{m,t} \le \hat{\nu}_{m,t},\ \tilde{x} \in V_{m-j}. \qquad (51)$$

Підставляючи оцінку (51) у формулу (50) та застосовуючи рівність Парсеваля $\sum_{\tilde{x} \in V_{m-j}} |\hat{u}_{\tilde{x}}|^2 = 2^{2(m-j)}$, отримаємо, що

$$|d(f_*, g_*) - t/2| \le 1/2 \cdot \left(2^{-(m-j)} \sum_{\tilde{x} \in V_{m-j}} |\hat{u}_{\tilde{x}}|^2\right)^{1/2} \hat{\nu}_{m,t} \le 1/2 \cdot 2^{(m-j)/2}\ \hat{\nu}_{m,t}. \qquad (52)$$

З формули (52) випливає нижня оцінка (46). Лему доведено.

Лема 5. Нехай $j \in \overline{1, m-1}$ і T має вигляд (2). Тоді за виконанням умови

$$\varepsilon^2 > 2^{(m-j)/2} \hat{\nu}_{m,t} t^{-1} \qquad (53)$$

справедлива нерівність

$$|\hat{L}_T^{(j)}(M, b)| \le (\varepsilon^2 - 2^{(m-j)/2} \hat{\nu}_{m,t} t^{-1})^{-1}. \qquad (54)$$

Доведення. Позначимо $L_{T,C_*}(b)$ множину вигляду (45), що відповідає коду (44). Помітимо, що на підставі формули (43) для будь-якої функції $f \in RM_0(1, j)$ виконуються рівності

$$d(f_*, b) = \sum_{a \in V_{m-j}} d(f_*, b \mid M_a) = \sum_{a \in V_{m-j}} \Delta(f, b \mid M_a) = \Delta^{(j)}(f, b),$$

з яких випливає, що $f \in \hat{L}_T^{(j)}(M, b)$ тоді і тільки тоді, коли $f_* \in L_{T,C^*}(b)$. Далі, згідно співвідношенням (46) та (53), для будь-яких різних функцій $f, g \in RM_0(1, j)$ справедливі нерівності

$$d(f_*, g_*) \ge t/2 \cdot (1 - 2^{(m-j)/2} \hat{\nu}_{m,t} t^{-1}) > t/2 \cdot (1 - \varepsilon^2) = 2T(1 - \delta) > 0,$$

з яких випливає, зокрема, що $f_* \ne g_*$.

Таким чином, $|\hat{L}_T^{(j)}(M, b)| = |L_{T,C^*}(b)|$, та на підставі леми 1.3

$$|\hat{L}_T^{(j)}(M, b)| \le \left(1 - \frac{2T(1-\delta)}{t/2 \cdot (1 - 2^{(m-j)/2} \hat{\nu}_{m,t} t^{-1})}\right)^{-1} =$$

$$= \left(\frac{1 - 2^{(m-j)/2} \hat{\nu}_{m,t} t^{-1}}{\varepsilon^2 - 2^{(m-j)/2} \hat{\nu}_{m,t} t^{-1}} \right)^{-1} < (\varepsilon^2 - 2^{(m-j)/2} \hat{\nu}_{m,t} t^{-1})^{-1}.$$

Отже, справедлива нерівність (54), що й треба було довести.

Перейдемо до доведення нерівності (23).

На підставі формули (25) та нерівності $|\hat{L}_T^{(j)}(M,b)| \le 2^{j-1}, \quad j \in \overline{1,m}$, справедливі співвідношення

$$\tau_T(M,b) \le t + 2C\sum_{j=1}^{\mu+1} 2^{m-j}(j+1)2^{j-1} + 2C\sum_{j=\mu+2}^{m} 2^{m-j}(j+1)|\hat{L}_T^{(j-1)}(M,b)| \le$$

$$\le t + C2^{m-1}(\mu+2)(\mu+3) + 2C(m+1)2^{m-\mu-2}\sum_{j=\mu+2}^{m}|\hat{L}_T^{(j-1)}(M,b)|. \qquad (55)$$

Оскільки в силу нерівності (22) для будь-якого $j \in \overline{\mu+2,m}$

$$2^{(m-(j-1))/2}\hat{\nu}_{m,t}t^{-1} \le 2^{(m-(\mu+1))/2}\hat{\nu}_{m,t}t^{-1} < 2^{(m-\mu)/2}\hat{\nu}_{m,t}t^{-1} \le \varepsilon^2,$$

то

$$\varepsilon^2 - 2^{(m-(j-1))/2}\hat{\nu}_{m,t}t^{-1} > (2^{(m-\mu)/2} - 2^{(m-\mu-1)/2})\hat{\nu}_{m,t}t^{-1} = (\sqrt{2}-1)2^{(m-\mu-1)/2}\hat{\nu}_{m,t}t^{-1}$$

,

звідки на підставі леми 5 випливає, що

$$|\hat{L}_T^{(j-1)}(M,b)| \le \frac{\sqrt{2}}{\sqrt{2}-1}2^{-(m-\mu)/2}t\,\hat{\nu}_{m,t}^{-1}, \ j \in \overline{\mu+2,m}. \qquad (56)$$

З формул (55) та (56) отримаємо, що

$$\tau_T(M,b) \le t + C2^{m-1}(\mu+2)(\mu+3) + 1/4\frac{C\sqrt{2}}{\sqrt{2}-1}(m+1)(m-\mu-2)2^{(m-\mu)/2}t\,\hat{\nu}_{m,t}^{-1} \le$$

$$\le t + C2^{m-1}(\mu+2)(\mu+3) + C(1+2^{-1/2})m^2 2^{(m-\mu)/2}t\,\hat{\nu}_{m,t}^{-1} \le$$

$$\le t + C2^{m-1}(\mu+2)(\mu+3) + 2Cm^2 2^{(m-\mu)/2}t\,\hat{\nu}_{m,t}^{-1}.$$

Отже, справедлива нерівність (23). Теорему доведено.

5. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі отримані та обґрунтовані аналітичні оцінки складності детермінованого алгоритму списочного декодування “вкорочених” кодів Ріда-Маллера першого порядку, який запропоновано в [1]. Зазначений алгоритм формує для даної системи рівнянь вигляду (1) список усіх векторів $x \in \{0,1\}^m$, що належать множині (4); він може бути застосований до побудови списків лінійних наближень (статистичних аналогів) частково визначених булевих функцій, розв’язання систем лінійних рівнянь із спотвореними правими частинами, а також повністю випадкових систем лінійних рівнянь від помірної кількості змінних ($m \le 28$).

Головними результатами є теореми 1 та 2, які визначають верхні межі середньої та, відповідно, максимальної двійкової часової складності алгоритму [1] (останню

оцінку отримано для окремого випадку, що пов'язано з відновленням спотворених лінійних рекурент максимального періоду над полем з двох елементів). Наведено також досяжну верхню межу обсягу списку, який формується з використанням запропонованого алгоритму (див. формулу (24)).

За виконанням певних умов, які зазначені у формулюваннях теорем 1, 2 та наслідків з них, часова складність алгоритму [1] є величиною порядку $O\left(2^m \log^2(2^m t^{-1}(1-2p)^{-2})\right)$ двійкових операцій, де m, t і p є відповідно числом змінних, числом рівнянь та ймовірністю спотворень у правій частині системи (1). Зауважимо, що складність раніше відомого детермінованого алгоритму аналогічного призначення, який базується на швидкому перетворенні Адамара [8], дорівнює $O\left(2^m m \log t\right)$ двійкових операцій, що, взагалі кажучи, перевищує складність алгоритму [1]. Так, при $m = 24$, $t = 4 \cdot 10^6$, $p = 0{,}40$ середня складність алгоритму [1] є майже в 3 рази менше складності алгоритму [8] (див. табл. 1).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Гулак, М., 2020. Метод оцінювання функціональної безпеки інформаційних технологій для створення гарантоздатних автоматизованих систем. *Кібербезпека: освіта, наука, техніка*, 3(7), pp.153-164, https://doi.org/10.28925/2663-4023.2020.7.153164

[2] Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В., *Основы криптографии: Учебное пособие*. М.: Гелиос АРВ, 2001, с. 480.

[3] Панасенко С.П., *Алгоритмы шифрования. Специальный справочник*. СПб.: БХВ-Петербург, 2009, с. 576

[4] С.О. Сушко, Г.В. Кузнецов, Л.Я. фомічова, А.В. Корабльов *Математичні основи криптоаналізу: навч. посібник.* – Д.: Національний гірничий університет, 2010. – 465 с.

[5] Бабаш А.В., Шанкин Г.П., Криптография. / Под редакцией В.П. Шерстюка, Э.А. Применко. М.: СОЛОН-Р, 2002. – 512 с.

[6] Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агневич. *Математические и компьютерные основы криптологии: Учебное пособие,* - Мн.: Новое знание, 2003. – 382 с.

[7] Думер И.И., Кабатянский Г.А., Тавернье С. Списочное декодирование двоичных кодов Рида-Маллера первого порядка. *Проблемы передачи информации*. – 2007. – Т. 43. – Вып. 3. – С. 66 – 74.

[8] Сидельников В.М. Быстрые алгоритмы построения набора маркировок дискретных массивов информации // *Труды по дискретной математике*. – Т. 1. – М.: ТВП, 1997. – С. 251 – 264.

[9] Н.Ахмед, К.Р. Рао Ортогональные преобразования при обработке цифровых сигналов: Пер. с англ. / Под ред. И.Б. Фоменко. – М.: Связь, 1980. – 248 с.

[10] Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. *Теория кодов, исправляющих ошибки*: Пер. с англ. — М: Связь, 1979. — 744 с.

[11] Коробов Н.М. *Тригонометрические суммы и их приложения*. – М.: Наука. Гл. ред. физ.-мат. лит., 1989. – 240 с.

[12] Сидельников В.М. Оценки для числа появлений знаков на отрезке рекуррентной последовательности над конечным полем // *Дискретная математика*. – 1991. – Т. 3. – Вып. 2. – С. 87 – 95.

[13] Шпарлинский И.Е. О некоторых свойствах линейных циклических кодов // *Проблемы передачи информации.* – 1983. – Т. 19. – Вып. 3. – С. 106 – 110.

[14] Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. – М.: МЦНМО, 2004. – 470 с.

[15] Молдовян А.А. *Криптография. Скоростные шифры* // БХВ-Петербург, 2002. ISBN 594157214X, ISBN 9785941572144. - 496 с.

[16] Дискретная математика и математические вопросы кибернетики. Т. 1 / Под общ. ред. С.В. Яблонского и О.Б. Лупанова. – М.: Наука, 1974. – 312 с

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (9), 2020
ISSN 2663 - 4023

Hennadii.M. Hulak
Ph.D Technical Sciences,
Head of Laboratory Research Department
Institute of Mathematical Machines and Systems Problems, Kyiv, Ukraine
ORCID: 0000-0001-9131-9233
h.hulak@ukr.net

THE COMPLEXITY OF THE FUNCTIONAL SECURITY ASSESSMENT ALGORITHM FOR INFORMATION TECHNOLOGIES FOR THE CREATION OF WARRANTY AUTOMATED SYSTEMS

Abstract. The complexity of the algorithm of communication of the system of linear levels with open regular parts by means of list decoding of "shortened" codes of reed painters which are intended for use in methods of an estimation of functional safety of cryptographic algorithms of cryptographic subsystems of the guaranteed automated systems creating on objects of critical infrastructure and socially important objects. This paper proposes solving problems to assess the complexity of the proposed algorithm. As a result, the upper estimates of the average labor productivity for the general case and the maximum complexity of the proposed algorithm for many special reviews related to the restoration of the formed linear results of the maximum period over a field of two elements. The achievable upper part of the list, which is formed using the proposed algorithm, is also indicated. The obtained results indicate that with certain collaborations between the parameters of the previously proposed algorithm, the time complexity was changed in comparison with the previously known deterministic algorithm for a similar purpose, which is based on the fast Hadamara transformation. This means that a more effective tool can be used to assess the impact of cryptographic subsystems on powerful cyberattacks to obtain a more accurate assessment of their functional security.

Keywords: guarantee capacity, reliability, functional security, functional security of cryptographic subsystem, cryptographic attack, stability of cryptographic transformation, basic decoding, Hamming distance, fast Hadamard transformation, Walsh-Hadamard transformation, Reed-Muller code.

REFERENCES

[1] Gulak, M., 2020. The method of evaluating the functional safety of information technologies for the establishment of guaranteed publishing automation systems. Cyberbezpeka: education, science, technology, 3 (7), pp.153-164, https://doi.org/10.28925/2663-4023.2020.7.153164
[2] Alferov A.P., Zubov A.Yu., Kuzmin A.S., Cheremushkin A.V., Fundamentals of Cryptography: Textbook. M .: Helios ARV, 2001, p. 480.
[3] Panasenko S.P., Encryption algorithms. Special reference book. SPb .: BHV-Petersburg, 2009, p. 576
[4] S.O. Sushko, G.V. Kuznetsov, L. Ya. Fomichova, A.V. Korablev Mathematical foundations of cryptanalysis: navch. google. - D .: National Girnichiy University, 2010 , 465 p.
[5] Babash A.V., Shankin G.P., Cryptography. / Edited by V.P. Sherstyuk, E.A. Applied. M .: SOLON-R, 2002 , 512 p.
[6] Yu.S. Kharin, V.I. Bernik, G.V. Matveev, S.V. Agnevich. Mathematical and computer foundations of cryptology: Textbook, Minsk: New knowledge, 2003, 382 p.
[7] Dumer II, Kabatiansky GA, Tavernier S. List decoding of first-order Reed-Muller binary codes. Information transfer problems. - 2007. - T. 43. - Issue. 3, p. 66 - 74.
[8] Sidelnikov V.M. Fast algorithms for constructing a set of markings for discrete arrays of information // Proceedings of discrete mathematics. - T. 1. - M .: TVP, 1997 , p. 251 - 264.
[9] N. Ahmed, K.R. Rao Orthogonal transformations in digital signal processing: Per. from English / Ed. I.B. Fomenko. - M .: Communication, 1980, 248 p.
[10] McWilliams F. J., Sloane N. J. A. Theory of error-correcting codes: Trans. from English - M: Communication, 1979, 744 p.
[11] Korobov N.M. Trigonometric sums and their applications. - M .: Science. Ch. ed. physical-mat. lit., 1989, 240 p.

[12] Sidelnikov V.M. Estimates for the number of occurrences of signs on a segment of a recurrent sequence over a finite field // Discrete Mathematics. - 1991. - T. 3. - Issue. 2. - p. 87 - 95.
[13] Shparlinsky I.Ye. On some properties of linear cyclic codes // Problems of information transmission. - 1983. - T. 19. - Issue. 3. - p. 106 - 110.
[14] Logachev O.A., Salnikov A.A., Yashchenko V.V. Boolean functions in coding theory and cryptology. - M .: MTsNMO, 2004 .- 470 p.
[15] Moldovyan A.A. Cryptography. High-speed ciphers // BHV-Petersburg, 2002. ISBN 594157214X, ISBN 9785941572144.496 p.
[16] Discrete mathematics and mathematical problems of cybernetics. T. 1 / Under total. ed. S.V. Yablonsky and O.B. Lupanov. - M .: Nauka, 1974 , - 312 p.