КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№3 (7), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.7.153164
УДК 621.3.019.3+004.056

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

МЕТОД ОЦІНЮВАННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ СТВОРЕННЯ ГАРАНТОЗДАТНИХ АВТОМАТИЗОВАНИХ СИСТЕМ

Анотація. Досліджуються складові забезпечення гарантоздатності автоматизованих систем, до яких висуваються підвищені вимоги у зв'язку з їх використанням у багатьох чутливих для держави сферах суспільної діяльності, включаючи національну безпеку і оборону, критичні промислові технології, енергетика та зв'язок, банківська сфера, захист навколишнього середовища, технології легітимного дистанційного навчання тощо. Визначені складові можуть суттєво впливати на якість та надійність надання інформаційних послуг у нормативно визначених умовах. Зокрема, показана особлива роль функціональної безпеки криптографічної підсистеми у плані підтримки виконання автоматизованою системою передбачених для неї завдань і функцій загалом, а також у частині забезпечення конфіденційності і цілісності інформації. Визначені складові криптографічної підсистеми, неякісна або некоректна робота яких негативно впливає на безпеку застосування цих підсистем. Проаналізовані види найбільш небезпечних атак на ці підсистеми, наведено їх класифікацію з точки зору можливості реалізації у сучасних науково-технічних умовах та залежно від потужності наявних обчислювальних засобів та технологій, на підставі чого визначено найбільш реальний та небезпечний варіант реалізації віддалених атак на програмну реалізацію криптографічної підсистеми.
На підставі проведеного аналізу запропоновано метод оцінки якості криптографічних перетворень, що базується на модифікованому алгоритмі розв'язання задачі пошуку рішення систем лінійних рівнянь із спотвореними правими частинами з використанням так званого декодування на основі «списків» "вкорочених" кодів Ріда-Маллера першого порядку, Доведено коректність запропонованого алгоритму.

Ключові слова: гарантоздатність, достовірність, функціональна безпека, цілісність, конфіденційність. функціональна безпека криптографічної підсистеми, криптографічна атака, стійкість криптографічного перетворення, код Ріда-Маллера.

1. ВСТУП

Актуальність проблеми створення гарантоздатних систем, забезпечення та оцінки гарантоздатності обумовлена всебічним охопленням усіх сфер життєдіяльності сучасного суспільства інформаційними технологіями та можливими негативними (навіть катастрофічними) наслідками для людини, суспільства, екології тощо у разі відмов відповідних комп'ютерних систем.

Значний внесок у розвиток теорії та практики гарантоздатних систем, у дослідження проблем оцінки якості, надійності, відмовостійкості, живучості інформаційних технологій і систем зробили вітчизняні та іноземні вчені, таки як, В.С. Харченко, О.В. Федухін, В.П. Стрельніков, А. Авиценис, Ж.-К. Лаприе, В.В. Липаев та інші.

За загальним визначенням [1] гарантоздатність це здатність комп'ютерної системи надавати потрібні послуги, яким виправдано можна довіряти. За суттю

ISSN 2663 - 4023

гарантоздатність є комплексною характеристикою системи, що включає, зокрема, такі субхарактеристики, як: готовність, живучість, обслуговуваемость, достовірність, функціональна безпека, цілісність, конфіденційність.

Слід зазначити, що системні дослідження гарантоздатності автоматизованих систем, нажаль, не торкнулись проблем функціональної безпеки їх криптографічних підсистем, зокрема методів їх оцінки. Саме цьому питанню присвячена ця робота.

Відомо [2-5], що складовими безпеки застосування криптографічних систем, є криптографічна стійкість алгоритмів, що утворюють їх криптосхему, якість системи генерації та управління ключами, спеціальні властивості та інженерно-криптографічні властивості програмної або апаратної реалізації криптосхеми, а також організаційні заходи з безпеки.

Практична криптографічна стійкість алгоритмів, що утворюють криптосхему, звичайно, оцінюється як мінімальний час що необхідний атакуючий стороні для знаходження конфіденційних параметрів в заданих умовах наявних обчислювальних потужностей, а також вихідних даних для розв'язання поставлених задач. При цьому реально найменш слабкою є атака на основі лише відомого криптографічного алгоритму та наявних шифрованих повідомлень, найбільш потужною є так звана адаптивна атака на основі підібраних відкритих повідомлень та відповідних їм шифрованих повідомлень [2,6].

На підставі багатьох досліджень (зокрема [7,8]) можливо зробити висновок, що найбільш поширеною на практиці є атака на криптографічну підсистему на основі відомих відкритих та відповідних їм шифрованих повідомлень. При цьому крім методу «грубої сили» [6] припускається можливість часткової лінеаризації криптографічного перетворення, на підставі чого задача атакуючої сторони зводиться до розв'язання системи лінійних рівнянь з викривленими правими частинами [2]. Можливість розв'язання вказаної задачі суттєво залежить від обраного алгоритму пошуку розв'язків та потужності наявних обчислювальних засобів.

Для розв'язання вказаної задачі може бути ефективно застосований метод списочного декодування блокових кодів, що запропонований в [9,10] та значно розвинений у багатьох подальших публікаціях (відзначимо статтю [11], що містить стислий огляд попередніх робіт). На відміну від "класичного" методу декодування у найближче кодове слово, результатом списочного декодування радіуса $T > 0$ є набір (список) усіх або деяких кодових слів, що знаходяться на відстані не більше за T від прийнятого спотвореного слова (зауважимо, що у першому випадку говорять про *детерміноване*, а у другому – про *недетерміноване* або *ймовірнісне списочне декодування*). Як правило, такий метод декодування дозволяє суттєво підвищити надійність виправлення помилок, зокрема, при його застосуванні у кореляційних атаках на потокові шифри (див., наприклад, [12]).

Одним з найбільш відомих алгоритмів декодування двійкових лінійних кодів є алгоритм швидкого перетворення Адамара, що полягає в обчисленні відстаней Геммінга від прийнятого слова до усіх кодових слів даного коду або коефіцієнтів Уолша-Адамара відповідної часткової булевої функції. Зазначений алгоритм використовується також при розв'язанні булевих систем лінійних рівнянь (СЛР) із спотвореними правими частинами і дозволяє формувати повний список з 2^m векторів, що впорядковані за значеннями їх відстаней від вектора у правій частині СЛР, із складністю у $O(m2^m)$ арифметичних (або $O(m^2 2^m)$ двійкових) операцій, де m – число змінних у даній системі рівнянь (див., наприклад, [13], с. 218). Більш ефективні

ISSN 2663 - 4023

за складністю алгоритми списочного декодування відомі лише для окремих класів лінійних кодів. Зокрема, у [14] запропоновано "швидкий" алгоритм списочного декодування кодів Ріда-Маллера (РМ) першого порядку, який формує список з усіх слів коду $RM(1,m)$ довжини 2^m у кулі радіуса $T = 2^{m-1}(1-\varepsilon)$ навколо прийнятого слова із складністю $O\left(2^m \min\{\ln^2 \varepsilon^{-2}, m^2\}\right)$ двійкових операцій, $\varepsilon \in (0,1)$.

У даної роботі запропоновано модифікацію алгоритму [14], яка дозволяє здійснювати детерміноване списочне декодування довільного "вкороченого" РМ-коду першого порядку або отримувати повний список відповідних розв'язків системи лінійних рівнянь із спотвореними правими частинами. Оцінювання складності запропонованого алгоритму потребує проведення окремих досліджень.

2. ОСНОВНІ ПОНЯТТЯ ТА ПОСТАНОВКА ЗАДАЧІ

Розглянемо систему лінійних рівнянь

$$Ax^T = b, \tag{1}$$

де A – булева матриця розміру $t \times m$, $b = Ax_0^T \oplus \varepsilon$, x_0 – невідомий двійковий вектор довжини m (істинний розв'язок СЛР (1)), $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_t)^T$ – випадковий вектор із незалежними у сукупності координатами, що розподілені за законом $\mathbf{P}(\varepsilon_i = 1) = 1 - \mathbf{P}(\varepsilon_i = 0) = p$, де $0 < p < 0{,}5$.

Припустимо, що рядки матриці A є попарно різними і $\operatorname{rank} A = m < t \le 2^m$. Задача знаходження розв'язків СЛР (1) методом (детермінованого) списочного декодування полягає у формуванні для заздалегідь визначеного числа T, $1 \le T \le 2^m$, списку всіх векторів $x \in V_m = \{0,1\}^m$, що задовольняють умові

$$d(Ax^T, b) \le T, \tag{2}$$

де $d(u,v)$ – відстань Геммінга між векторами u та v. Зрозуміло, що поставлена задача включає у себе, як окремий випадок, знаходження найбільш вірогідного розв'язку СЛР (1), тобто такого вектора $\hat{x} \in V_m$, для якого величина $d(A\hat{x}^T, b)$ приймає найменше можливе значення.

Мовою теорії кодування зазначену задачу можна сформулювати таким чином. Нехай G – блоковий код довжини t та вимірності m з твірною матрицею A^T, b – спотворене кодове слово, що отримано на виході двійкового симетричного каналу зв'язку з ймовірністю помилки $p \in (0, 0{,}5)$. Потрібно розробити алгоритм, який формує список усіх кодових слів у кулі радіуса T навколо прийнятого слова b.

Відзначимо також наступне формулювання цієї задачі, що полягає у побудові списку наближень часткової функції b в класі лінійних функцій. Позначимо M множину рядків матриці A; $\Im_M$ – множину усіх часткових булевих функцій, області визначення яких містять множину M; $RM(1,m)$ – код Ріда-Маллера (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 $c_1,\ldots,c_{m+1} \in \{0,1\}$; $RM_0(1,m) = \{c \in RM(1,m) : c(0,\ldots,0) = 0\}$. Зауважимо, що означений вище код G можна розглядати як "*вкорочення*" *коду* $RM_0(1,m)$, словами якого є вектори значень усіх лінійних функцій $c_1x_1 \oplus \ldots \oplus c_mx_m$ на наборах $(x_1,\ldots,x_m)$, що належать множині M. Для будь-яких $f, g \in \Im_M$ позначимо

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

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

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

де $1 \le T \le 2^m$. Безпосередньо з наведених означень випливає, що вектори $x \in V_m$, які задовольняють умові (2), знаходяться у взаємно однозначній відповідності з лінійними функціями c, що належать множині (3). Отже, знаходження розв'язків СЛР (1) методом списочного декодування зводиться до побудови множини $L_{0,T}(b) \overset{\text{def}}{=} L_T(b) \cap RM_0(1,m)$, тобто списку усіх лінійних функцій, які знаходять на відстані не більше за T від часткової функції $b \in \Im_M$.

У [14] запропоновано "швидкий" алгоритм побудови множини (3) у випадку, коли $M = V_m$ (і, отже, матриця коефіцієнтів СЛР (1) складається з усіх 2^m двійкових векторів довжини m). Зазначений алгоритм здійснює списочне декодування радіуса $T = 2^{m-1}(1-\varepsilon)$ коду $RM(1,m)$ із складністю $O\left(2^m \min\{\ln^2 \varepsilon^{-2}, m^2\}\right)$ двійкових операцій, де $\varepsilon \in (0,1)$, та є найкращим з відомих сьогодні алгоритмів детермінованого списочного декодування РМ-кодів першого порядку. Нижче викладено модифікацію алгоритму [14], що дозволяє будувати множину $L_{0,T}(b)$ для довільної СЛР (1), яка задовольняє зазначеним вище умовам, та отримувати повний список радіуса T, $1 \le T \le 2^m$, вірогідних розв'язків цієї СЛР.

3. АЛГОРИТМ РОЗВ'ЯЗАННЯ СЛР ІЗ СПОТВОРЕНИМИ ПРАВИМИ ЧАСТИНАМИ ШЛЯХОМ ДЕТЕРМІНОВАНОГО СПИСОЧНОГО ДЕКОДУВАННЯ "ВКОРОЧЕНИХ" РМ-КОДІВ ПЕРШОГО ПОРЯДКУ

Введемо декілька допоміжних позначень. Для будь-яких $j \in \overline{0,m-1}$, $a = (a_{j+1},\ldots,a_m) \in V_{m-j}$ позначимо

$$M_a = \{(x_1,\ldots,x_m) \in M :\ x_{j+1} = a_{j+1},\ldots,x_m = a_m\}. \qquad (4)$$

Назвемо множину вигляду (4) *j-вимірною М-гранью*, а вектор a *– номером М-грані* M_a. Для довільних $f, g \in \Im_M$ позначимо

$$d(f,g \mid M_a) = \sum_{x \in M_a} \delta(f(x), g(x)), \qquad (5)$$

ISSN 2663 - 4023

$$\Delta(f,g\,|\,M_a)=\min\{d(f,g\,|\,M_a),d(f,g\oplus 1\,|\,M_a)\}, \tag{6}$$

$$\Delta^{(j)}(f,g)=\sum_{a\in V_{m-j}}\Delta(f,g\,|\,M_a). \tag{7}$$

Назвемо *j-м префіксом* функції $c(x_1,\ldots,x_m)=c_1x_1\oplus\ldots\oplus c_mx_m\oplus c_{m+1}$ функцію $c^{(j)}(x_1,\ldots,x_j)=c_1x_1\oplus\ldots\oplus c_jx_j$; саму функцію $c=c(x_1,\ldots,x_m)$ назвемо *продовженням префіксу* $c^{(j)}$, $j\in\overline{0,m-1}$. Зауважимо, що при $j=0$ єдиним префіксом будь-якої функції $c\in RM(1,m)$ є константа 0.

Позначимо $L_T^{(j)}(b)$ множину *j*-х префіксів усіх функцій c, що належать множині (3). Введемо також множини

$$\hat{L}_T^{(j)}(b)=\{c^{(j)}\in RM_0(1,j):\ \Delta^{(j)}(c^{(j)},b)\le T\},\ j\in\overline{0,m-1}. \tag{8}$$

Зауважимо, що з наведенних означень випливають такі співвідношення:

$$L_T^{(j)}(b)\subseteq\hat{L}_T^{(j)}(b),\ j\in\overline{0,m-1}. \tag{9}$$

Дійсно, нехай $L_T^{(j)}(b)\neq\varnothing$ (у протилежному випадку включення (9) очевидно) і $c^{(j)}=c_1x_1\oplus\ldots\oplus c_jx_j$ – довільна функція, що належить множині $L_T^{(j)}(b)$. Позначимо $c=c_1x_1\oplus\ldots\oplus c_mx_m\oplus c_{m+1}$ продовження префіксу $c^{(j)}$ таке, що $c\in L_T(b)$, та помітимо, що обмеження функції c на довільну *M*-грань M_a, $a=(a_{j+1},\ldots,a_m)\in V_{m-j}$, дорівнює $c^{(j)}(x_1,\ldots,x_j)\oplus c_a$, де $c_a=c_{j+1}a_{j+1}\oplus\ldots\oplus c_ma_m\oplus c_{m+1}\in\{0,1\}$. Отже, внаслідок формул (5) та (6), для будь-якого вектора $a\in V_{m-j}$ справедлива нерівність $d(c,b\,|\,M_a)\ge\Delta(c^{(j)},b\,|\,M_a)$. Звідси на підставі рівностей (3) та (7), випливають такі співвідношення:

$$T\ge d(c,b\,|\,M)=\sum_{a\in V_{m-j}}d(c,b\,|\,M_a)\ge\sum_{a\in V_{m-j}}\Delta(c^{(j)},b\,|\,M_a)=\Delta^{(j)}(c^{(j)},b).$$

Отже, $c^{(j)}\in\hat{L}_T^{(j)}(b)$, що й треба було довести.

Перейдемо до викладення алгоритму розв'язання СЛР (1) шляхом детермінованого списочного декодування.

Алгоритм, що пропонується, будує множину $L_{0,T}(b)$ за вхідними даними $(A,\ b,\ T)$, де матриця A та вектор b задовольняють умовам, що зазначені у розділі 1, $1\le T\le 2^m$. Алгоритм складається з m кроків, на *j*-му з яких, $j\in\overline{1,m-1}$, будується певна множина $\Lambda_T^{(j)}(b)$ така, що

$$L_T^{(j)}(b)\subseteq\Lambda_T^{(j)}(b)\subseteq\hat{L}_T^{(j)}(b), \tag{10}$$

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

$$d_\nu(c^{(j)} \mid a) = d(c^{(j)}, b \oplus \nu \mid M_a),\ a \in V_{m-j},\ \nu \in \{0,1\}. \quad (11)$$

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

Покладемо

$$c^{(0)} \equiv 0,\ \Lambda_T^{(0)}(b) = \{c^{(0)}\}, \quad (12)$$

$$d_\nu(c^{(0)} \mid a) = \begin{cases} 0, \text{ якщо } a \notin M; \\ b(a) \oplus \nu - \text{у іншому випадку,} \end{cases} \quad (13)$$

де $b(a)$ – значення часткової функції b на двійковому наборі $a \in M$, тобто значення у правій частині рівняння з вектором коефіцієнтів a СЛР (1), $\nu \in \{0,1\}$.

Нехай $j \in \overline{1, m-1}$ і вже побудовані множина $\Lambda_T^{(j-1)}(b)$ та набори чисел $D_0(c^{(j-1)}),\ D_1(c^{(j-1)})$, де $c^{(j-1)} \in \Lambda_T^{(j-1)}(b)$. На *j*-му кроці алгоритму для кожного префіксу $c^{(j-1)}$, що належить множині $\Lambda_T^{(j-1)}(b)$, розглядаються обидва його можливих продовження, тобто функції вигляду $c^{(j)} = c^{(j-1)}(x_1, \ldots, x_{j-1}) \oplus c_j x_j$, де $c_j \in \{0,1\}$. Для кожної такої функції обчислюються значення (11), за якими знаходяться числа

$$\Delta(c^{(j)}, b \mid M_a) = \min\{d_0(c^{(j)} \mid a), d_1(c^{(j)} \mid a)\},\ a \in V_{m-j}. \quad (14)$$

Далі перевіряється умова

$$\Delta^{(j)}(c^{(j)}, b) = \sum_{a \in V_{m-j}} \Delta(c^{(j)}, b \mid M_a) \le T, \quad (15)$$

за виконанням якої функція $c^{(j)}$ включається до множини $\Lambda_T^{(j)}(b)$, що формується, та не включається до неї (відбраковується) – у протилежному випадку. Таким чином, на *j*-му кроці алгоритму множина $\Lambda_T^{(j)}(b)$ визначається як сукупність тих і тільки тих продовжень префіксів $c^{(j-1)} \in \Lambda_T^{(j-1)}(b)$, які належать множині (8).

Покажемо, як здійснюється обчислення значень (11) за відомими наборами $D_0(c^{(j-1)})$ та $D_1(c^{(j-1)})$, де $c^{(j-1)} \in \Lambda_T^{(j-1)}(b),\ j \in \overline{1, m-1}$. Помітимо, що для будь-якого вектора $a \in V_{m-j}$ *j*-вимірна *M*-грань M_a є об'єднанням двох *M*-граней меншої вимірності, які не перетинаються: $M_a = M_{(0,a)} \cup M_{(1,a)}$. Звідси на підставі рівності $c^{(j)} = c^{(j-1)}(x_1, \ldots, x_{j-1}) \oplus c_j x_j$ та формули (5) випливають такі співвідношення:

$$d_\nu(c^{(j)} \mid a) = d(c^{(j)}, b \oplus \nu \mid M_a) =$$

ISSN 2663 - 4023

$$= \sum_{\substack{x\in V_{j-1}:\\ (x,0,a)\in M}} \delta(c^{(j-1)}(x), b(x,0,a)\oplus \nu) + \sum_{\substack{x\in V_{j-1}:\\ (x,1,a)\in M}} \delta(c^{(j-1)}(x)\oplus c_j, b(x,1,a)\oplus \nu) =$$

$$= d(c^{(j-1)}, b\oplus \nu \mid M_{(0,a)}) + d(c^{(j-1)}, b\oplus \nu\oplus c_j \mid M_{(1,a)}) =$$

$$= d_\nu(c^{(j-1)} \mid (0,a)) + d_{\nu\oplus c_j}(c^{(j-1)} \mid (1,a)),\ a\in V_{m-j},\ \nu\in\{0,1\}. \qquad (16)$$

Отже, значення (11) можна обчислювати за формулами (16).

Опишемо тепер останній крок алгоритму. Вхідними даними на цьому кроці є множина $\Lambda_T^{(m-1)}(b)$ та набори $D_0(c^{(m-1)})$, $D_1(c^{(m-1)})$, сформовані для кожної функції $c^{(m-1)}\in\Lambda_T^{(m-1)}(b)$. Як і на попередніх кроках, розглядаються можливі продовження $c^{(m)} = c^{(m-1)}(x_1,\ldots,x_{m-1})\oplus c_m x_m$, $c_m\in\{0,1\}$, довільного префіксу $c^{(m-1)}\in\Lambda_T^{(m-1)}(b)$, для яких обчислюються значення $d(c^{(m)}, b\mid M)$. Далі формується множина $\Lambda_T^{(m)}(b)$, що складається з усіх функцій $c^{(m)}$, які задовольняють умові $d(c^{(m)}, b\mid M)\le T$. Нижче показано, що

$$\Lambda_T^{(m)}(b) = L_{0,T}(b), \qquad (17)$$

отже, елементи множини $\Lambda_T^{(m)}(b)$ складають шуканий список усіх лінійних функцій, які знаходяться на відстані не більше за T від часткової функції b.

Для обчислення відстаней $d(c^{(m)}, b\mid M)$ представимо множину M у вигляді об'єднання двох (m–1)-вимірних M-граней M_0, M_1 і скористаємося наступними рівностями, аналогічними формулам (16):

$$d(c^{(m)}, b\mid M) = \sum_{\substack{x\in V_{m-1}:\\ (x,0)\in M}} \delta(c^{(m-1)}(x), b(x,0)) + \sum_{\substack{x\in V_{m-1}:\\ (x,1)\in M}} \delta(c^{(m-1)}(x)\oplus c_m, b(x,1)) =$$

$$= d(c^{(m-1)}, b\mid M_0) + d(c^{(m-1)}, b\oplus c_m \mid M_1) = d_0(c^{(m-1)}\mid 0) + d_{c_m}(c^{(m-1)}\mid 1). \qquad (18)$$

Таким чином, в результаті виконання алгоритму формуються множина (17) та набір чисел (18), що дорівнюють відстаням Геммінга від її елементів до часткової функції b.

4. ОБҐРУНТУВАННЯ КОРЕКТНОСТІ МОДИФІКОВАНОГО АЛГОРИТМУ

ISSN 2663 - 4023

Переконаємося у справедливості рівності (17). Для цього доведемо спочатку співвідношення (10) для усіх $j \in \overline{0, m-1}$, використовуючи метод математичної індукції по j.

При $j = 0$, згідно рівностям (12), $L_T^{(0)}(b) = \Lambda_T^{(0)}(b) = \{c^{(0)}\}$, звідки на підставі формули (9) випливає справедливість співвідношення (10).

Нехай $j \in \overline{1, m-1}$; тоді включення $\Lambda_T^{(j)}(b) \subseteq \hat{L}_T^{(j)}(b)$ має місце за визначенням зазначених множин. Отже, залишається переконатися у справедливості включення

$$L_T^{(j)}(b) \subseteq \Lambda_T^{(j)}(b), \tag{19}$$

виходячи з індуктивного припущення $L_T^{(j-1)}(b) \subseteq \Lambda_T^{(j-1)}(b)$.

Нехай $c^{(j)} = c^{(j-1)}(x_1, \ldots, x_{j-1}) \oplus c_j x_j \in L_T^{(j)}(b)$. Тоді $c^{(j)}$ є j-м префіксом деякої функції $c \in L_T(b)$. Отже, $c^{(j-1)}$ є $(j-1)$-м префіксом цієї ж функції, тобто $c^{(j-1)} \in L_T^{(j-1)}(b)$. Звідси за припущенням індукції отримаємо, що $c^{(j-1)} \in \Lambda_T^{(j-1)}(b)$. Далі, згідно формулі (9), виконується умова $c^{(j)} \in \hat{L}_T^{(j)}(b)$. Отже, $c^{(j)}$ є продовженням префіксу $c^{(j-1)} \in \Lambda_T^{(j-1)}(b)$, яке належить множині (8), тобто $c^{(j)} \in \Lambda_T^{(j)}(b)$, що й треба було довести.

Таким чином, справедлива формула (19), і, отже, співвідношення (10) виконується для усіх $j \in \overline{0, m-1}$.

Перейдемо до доведення формули (17). Оскільки включення $\Lambda_T^{(m)}(b) \subseteq L_{0,T}(b)$ випливає безпосередньо з визначення указаних множин, залишається довести співвідношення

$$L_{0,T}(b) \subseteq \Lambda_T^{(m)}(b). \tag{20}$$

Нехай $c = c^{(m-1)}(x_1, \ldots, x_{m-1}) \oplus c_m x_m \in L_{0,T}(b)$. Тоді $c^{(m-1)} \in L_T^{(m-1)}(b)$, згідно визначенню множини $L_T^{(m-1)}(b)$. Звідси, використовуючи формулу (10) при $j = m-1$, отримаємо, що $c^{(m-1)} \in \Lambda_T^{(m-1)}(b)$, і $c^{(m)} \in \Lambda_T^{(m)}(b)$, оскільки $d(c^{(m)}, b \mid M) \le T$. Таким чином, співвідношення (20), а отже й рівність (17), повністю доведені.

5. ВИСНОВКИ

У роботі наведено та обґрунтовано аналітичні оцінки складності та запропоновано алгоритм детермінованого списочного декодування “вкорочених” кодів Ріда-Маллера першого порядку, який для заданої СЛР вигляду (1) формує список усіх двійкових векторів $x \in V_m$, що задовольняють умові (2). Зазначений алгоритм є

модифікацією та узагальненням алгоритму списочного декодування повного РМ-коду першого порядку, який запропоновано у статті [14].

Зауважимо, що викладений алгоритм може буди застосовано до будь-яких матриці A з $t > m$ різними строками (не обов'язково повного рангу m) та вектора b у правій частині СЛР (1) (що не обов'язково є результатом спотворення деякого кодового слова Ax^T, де $x \in V_m$). Отже, цей алгоритм може бути застосовано і до випадкових СЛР, а не тільки до систем лінійних рівнянь із спотвореними правими частинами. У будь-якому випадку результатом роботи алгоритму є список (17), що складається з усіх лінійних функцій, які знаходяться на відстані не більше за T від часткової функції b, поряд з відповідними таким функціям відстанями Геммінга до функції b (див. формулу (18)).

Головною задачею подальших досліджень є аналіз складності запропонованого алгоритму. Як показано у [14], для повного коду $RM(1,m)$, тобто у випадку, коли матриця A складається з усіх 2^m двійкових векторів довжини m, складність оригінального алгоритму [14] не перевищує $O\left(2^m \min\{\ln^2 \varepsilon^{-2}, m^2\}\right)$ двійкових операцій, де число $\varepsilon \in (0,1)$ визначається за радіусом декодування T співвідношенням $T = 2^{m-1}(1-\varepsilon)$. Для обґрунтування зазначеної оцінки автори [14] використовують межу Джонсона для числа кодових слів у кулі радіуса T в просторі Геммінга.

В загальному випадку застосування методики [14] для оцінювання складності алгоритму стає проблематичним, що однак не виключає можливості її застосування до окремих класів систем лінійних рівнянь із спотвореними правими частинами (наприклад, таких, що будуються при відновленні спотворених двійкових лінійних рекурент). Іншою важливою задачею досліджень є оцінювання середньої складності алгоритму (за всіма матрицями A та векторами b, що вибираються з відповідних множин випадково, рівноймовірно та незалежно один від одного).

Отримані результати свідчать про те, що при певних співвідношеннях між параметрами m, t і T алгоритм [9] має меншу часову складність у порівнянні з раніше відомим детермінованим алгоритмом аналогічного призначення [11], який базується на швидкому перетворенні Адамара.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] В.С. Харченко, «Гарантоспособность и гарантоспособные системы: элементы методологи», *Радіоелектронні і комп'ютерні системи*, № 5, с. 7-19, 2006.

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

[3] Г.Н. Гулак, «Моделирование на этапе оценки безопасности шифраторов конфиденциальной информации», *Науково-практичний журнал «Сучасна спеціальна техніка»*, № 1(24), с. 73-81, 2011.

[4] Г.М. Гулак, «Характеристика небезпечних відмов засобів, що реалізують стеганографічні методи перетворення інформації», *Науково-технічний журнал «Захист інформації»*, № 1(42), с. 56-59, 2009.

[5] Гулак Г., Ковальчук Л., «Різні підходи до визначення випадкових послідовностей», *Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні»*, № 3, - К., -2001, - с.127-133.

[6] Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації: підручник. - В.: ВНТУ, 2011. -198с.

[7] А.Г. Конхейм Основы криптографии. Пер. с англ. –М: Радио и связь, 1987. – 412с.

[8] E.L. Bauer Entzifferte Gehemnisse. Methoden und Maximen der Kryptologie. Zweite erweitere Auflage.Springer. 1991. 472s.
[9] Elias P., «List decoding for noisy channels», *Procedings of WESCON Conv. Rec.*, 1957. – P. 94 – 104.
[10] Wozenkraft J.M., «List decoding» , *Quart. Progr. Rep., Res. Lab. Electron*. – MIT. Cambridge, 1958. – Vol. 48.
[11] Guruswami V., Hastad J., Sudan M., Zuckerman D., «Combinatorial bounds for list decoding», *IEEE Trans. on Inform. Theory*. – 2002. – Vol. IT-48(5). – P. 1021 – 1034.
[12] Ekdahl P., Johansson T., «Another attack on A5/1», *IEEE Trans. on Inform. Theory*. – 2003. – Vol. IT-49(1). – P. 284 – 289.
[13] Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. – М.: МЦНМО, 2004. – 470 с.
[14] Думер И.И., Кабатянский Г.А., Тавернье С., «Списочное декодирование двоичных кодов Рида-Маллера первого порядка», *Проблемы передачи информации*. – 2007. – Т. 43. № 3. – с. 66 – 74.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (7), 2020
ISSN 2663 - 4023

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

METHOD OF EVALUATION OF FUNCTIONAL SECURITY OF INFORMATION TECHNOLOGIES FOR CREATION OF WARRANTY AUTOMATED SYSTEMS

Abstract. The components of ensuring the warranty of automated systems, which are subject to increased requirements in connection with their use in many sensitive areas of public activity, including national security and defense, critical industrial technologies, energy and communications, banking, environmental protection , technologies of legitimate distance learning, etc. Certain components can significantly affect the quality and reliability of information services in regulatory conditions. In particular, the special role of the functional security of the cryptographic subsystem in terms of supporting the performance of the automated system for its tasks and functions in general, as well as in terms of ensuring the confidentiality and integrity of information. The components of the cryptographic subsystem have been identified, the poor or incorrect operation of which negatively affects the security of these subsystems. The types of the most dangerous attacks on these subsystems are analyzed, their classification from the point of view of possibility of realization in modern scientific and technical conditions and depending on capacity of available computing means and technologies on the basis of which the most real and dangerous variant of realization of remote attacks on software implementation of cryptographic subsystem is defined. .
Based on the analysis, a method for evaluating the quality of cryptographic transformations based on a modified algorithm for solving the problem of finding solutions of systems of linear equations with distorted right-hand parts using the so-called decoding based on "lists" of first-order "shortened" Reed-Muller codes is proved. the correctness of the proposed algorithm.

Keywords: guarantee capacity, reliability, functional safety, integrity, confidentiality. functional security of cryptographic subsystem, cryptographic attack, stability of cryptographic transformation, Reed-Muller code.

REFERENCES

[1] V.S. Kharchenko, "Guarantee and guarantee systems: elements of methodology", Radio-electronic and computer systems, № 5, p. 7-19, 2006.
[2] Babash AV, Shankin GP Cryptography. Edited by VP Sherstyuka, EA Primenko, - M .: SOLON-R, 2002. - 512p.
[3] G.N. Gulak, “Modeling at the stage of assessing the security of confidential information encoders”, Scientific and practical journal “Modern special equipment”, № 1 (24), p. 73-81, 2011.
[4] G.M. Gulak, "Characteristics of dangerous failures of means that implement steganographic methods of information transformation", Scientific and Technical Journal "Information Protection", № 1 (42), p. 56-59, 2009.
[5] Gulak G., Kovalchuk L., "Different approaches to the definition of random sequences", Scientific and technical collection "Legal, regulatory and metrological support of information security in Ukraine", № 3, - K., -2001, - p. .127-133.
[6] Gulak GM, Mukhachev VA, Khoroshko VO, Yaremchuk YE Fundamentals of cryptographic information protection: a textbook. V .: VNTU, 2011. 198p.
[7] A.G. Conheim Fundamentals of Cryptography. Per. with English - M: Radio and communication, 1987. - 412p.
[8] E.L. Bauer's incomprehensible knowledge. Methods and maxims of cryptology. Two extensions. Springer. 1991. 472p.
[9] Elias P., “List decoding for noisy channels”, Proceedings of WESCON Conv. Rec., 1957. ó P. 94ó 104.
[10] Wozenkraft J.M., “List decoding,” Quart. Progr. Rep., Res. Lab. Electron. - MIT. Cambridge, 1958. Vol. 48.

[11] Guruswami V., Hastad J., Sudan M., Zuckerman D., “Combinatorial bounds for list decoding”, IEEE Trans. on Inform. Theory. - 2002. - Vol. IT-48 (5). - P. 1021 - 1034.
[12] Ekdahl P., Johansson T., “Another attack on A5 / 1”, IEEE Trans. on Inform. Theory. - 2003. - Vol. IT-49 (1). - P. 284 - 289.
[13] Logachev OA, Salnikov AA, Yashchenko VV Boolean functions in coding theory and cryptology. - M .: МЦНМО, 2004. - 470 с.
[14] Dumer II, Kabatyansky GA, Tavernier S., "List decoding of first-order Reed-Muller binary codes", Problems of information transfer. - 2007. - V. 43. № 3. - p. 66 - 74.