

АЛГЕБРАЇЧНИЙ ІМУНІТЕТ НЕЛІНІЙНИХ БЛОКІВ СИМЕТРИЧНИХ ШИФРІВ

1. Вступ

Криптографічне перетворення грає важливу роль в забезпеченні безпеки сучасних інформаційних систем і технологій [1, 2]. Симетричні шифри через свою простоту, ефективність і багатофункціональність застосовуються практично у всіх сучасних криптопротоколах, а також використовуються як складова частина інших криптографічних примітивів: в хешуванні, формуванні псевдовипадкових послідовностей, генерації паролів та ін. Отже, аналіз і дослідження методів синтезу симетричних криптопримітивів, розробка і теоретичне обґрунтування критеріїв і показників ефективності, в тому числі окремих вузлів сучасних шифрів є важливою і актуальною науково-технічною задачею.

Ключовим компонентом сучасних симетричних шифрів є нелінійні вузли (нелінійні підстановки, таблиці заміни, S-блоки), які виконують функції приховування статистичних зв'язків відкритого тексту і шифртексту, перемішування і розсіювання даних, внесення нелінійності в процедуру шифрування для протистояння різним криптоаналітичним і статистичним атакам. Таким чином, від показників ефективності нелінійних вузлів (збалансованості, нелінійності, автокореляції, кореляційної імунності та ін.) безпосередньо залежить ефективність симетричного шифру, його стійкість до більшості відомих криптографічних атак і рівень забезпеченої безпеки інформаційних технологій.

Окремі показники ефективності нелінійних вузлів розглянуті в [3 – 9]. Поняття алгебраїчного імунітету вперше введено в роботах [10, 11] для оцінки стійкості булевих функцій до т.з. алгебраїчного криптоаналізу, запропонованого в [12]. В роботі [13] ці положення були узагальнені для булевих відображень (S-блоків). Для обчислення алгебраїчного імунітету S-блоків використовується математичний апарат базисів Грьобнера [15 – 18].

В даній роботі розглядаються різні методи розрахунку алгебраїчного імунітету, вивчається їх взаємозв'язок, наводяться результати порівняльних досліджень алгебраїчної імунності нелінійних вузлів найбільш відомих сучасних симетричних шифрів.

2. Алгебраїчний імунітет булевих функцій

Поняття алгебраїчного імунітету вперше введено в роботах [10, 11] і докладно розглянуто в дисертації [14]. Введемо необхідні для подальшого викладення визначення та позначення, дотримуючись прийнятих в [14] формулювань.

Нехай $GF(2)$ – двійкове поле та $GF(2)^n$ – n -мірний векторний простір над $GF(2)$.

Булева функція $f(x)$ від n змінних – це відображення $f(x): GF(2)^n \rightarrow GF(2)$.

Таблиця істинності булевої функції $f(x)$ від n змінних – це двійковий вихідний вектор значень функції, який містить 2^n елементів, кожен елемент належить множині $\{0, 1\}$.

Алгебраїчна нормальна форма (поліном Жегалкіна) булевої функції $f(x)$ від n змінних записується у вигляді:

$$f(x) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus a_{13} x_1 x_3 \oplus \dots \oplus a_{(n-1)n} x_{n-1} x_n \oplus \dots \oplus a_{123\dots n} x_1 x_2 x_3 \dots x_n$$

де коефіцієнти $a_i \in \{0, 1\}$ і кожна булева функція реалізується поліномом Жегалкіна єдиним чином, тобто кожне представлення $f(x)$ відповідає унікальній таблиці істинності.

Алгебраїчна ступінь $Deg(f)$ булевої функції $f(x)$ – число змінних в найдовшому доданку алгебраїчної нормальної форми функції, що має ненульовий коефіцієнт a_i . При цьому вважаємо $Deg(0)=0$.

Позначимо V_n через множину всіх відображень $GF(2)^n \rightarrow GF(2)$, тобто це множина всіх можливих булевих функцій $f(x)$ від n змінних.

Множину V_n будемо розглядати і як кільце булевих функцій і як векторний (лінійний) простір над двійковим полем, тобто $V_n = GF(2)^{2^n}$.

Булева функція $g \in V_n$ називається *анігілятором функції* $f \in V_n$, якщо

$$f \cdot g = 0$$

або

$$(f + 1) \cdot g = 0.$$

Множина різних анігіляторів булевої функції $g(x)$ утворює лінійний простір, який позначимо

$$Ann(f) = \{g \in V_n \mid f \cdot g = 0\}.$$

Лінійний простір анігіляторів ступеня $\leq d$ позначимо

$$A_d^n(f) = \{g \in V_n \mid f \cdot g = 0, Deg(g) \leq d\} \subset Ann(f).$$

Поняття анігіляторів булевих функцій тісно пов'язане з оцінкою ефективності алгебраїчного криптоаналізу поточних шифрів [10]. Зокрема, при використанні фільтруючого генератора (див. рис. 1) псевдовипадкових послідовностей (ПВП) пошук початкового стану регістра зсуву з лінійним зворотним зв'язком (РЗЛЗЗ) пов'язаний зі зниженням ступеня спільної системи поліноміальних булевих рівнянь.

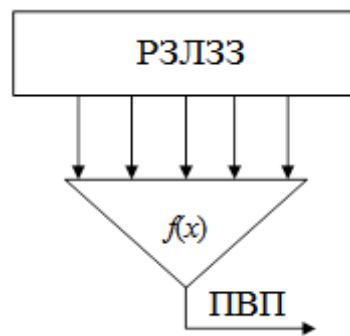


Рис. 1

Алгоритм алгебраїчного криптоаналізу, запропонований в [10], дозволяє, за певних умов, по частині перехопленої вихідної послідовності (ПВП) знаходити початковий стан РЗЛЗЗ з часовою складністю $O(S_n^d)^3$, де

$$S_n^d = \sum_{i=0}^d \frac{n!}{i!(n-i)!}$$

d – найменший ступінь ненульового анігілятора булевої функції $f(x)$, що фільтрується, або її інверсії: $f(x) + 1$.

Таким чином, завданням алгебраїчного криптоаналізу є пошук ненульових анігіляторів або, принаймні, оцінка їх мінімального ступеню. З цією метою в роботі [11] введено визначення *алгебраїчної імунності* $AI(f)$ булевої функції $f \in V_n$:

$$AI(f) = \min\{Deg(g) \mid g \in Ann(f) \text{ або } g \in Ann(f+1)\}.$$

Величина $AI(f)$ чисельно дорівнює мінімальному ступеню такої булевої функції $g \in V_n$, що $f \cdot g = 0$ або $(f+1) \cdot g = 0$.

Використовуючи введене вище поняття лінійного простору анігіляторів ступеня $\leq d$, запишемо:

$$AI(f) = \min\{d \mid A_d^n(f) \neq 0 \text{ или } A_d^n(f+1) \neq 0\}, \quad (1)$$

тобто для оцінки алгебраїчної імунності булевої функції $f \in V_n$ достатньо знайти ненульовий базис простору анігіляторів найменшого ступеню d .

Величина d дозволяє кількісно оцінити складність алгебраїчного криптоанализу і, при досить великому d , гарантувати стійкість поточного криптоалгоритму до алгебраїчної атаки.

Алгоритм обчислення алгебраїчної імунності булевих функцій. Один з алгоритмів розрахунку алгебраїчної імунності булевих функцій представлений в дисертаційній роботі [14]. Він заснований на побудові базису лінійного простору анігіляторів $A_d^n(f)$ заданого ступеня d . Ітеративно збільшуючи d і повторюючи побудову базису простору $A_d^n(f)$ оцінку $AI(f)$ отримуємо за формулою (1), тобто через ненульовий базис анігіляторів найменшого ступеню.

Для викладу суті алгоритму необхідно ввести такі додаткові позначення.

Моном (одночлен) відносно змінних x_1, \dots, x_n запишемо у вигляді

$$x^u = \prod_{i=1}^n x_i^{u_i} = \begin{cases} x_i, u_i = 1, \\ 1, u_i = 0, \end{cases}$$

де вектори $x, u \in V_2^n$, $x = (x_1, \dots, x_n)$, $u = (u_1, \dots, u_n)$.

Ступінь одночлена x^u визначається вагою Хеммінга (числом ненульових координат) $w_h(u)$ вектора $u = (u_1, \dots, u_n)$, тобто

$$Deg(x^u) = w_h(u).$$

З урахуванням цих позначень булеву функцію $f(x)$ в алгебраїчній нормальній формі (у формі полінома Жегалкіна) запишемо у вигляді

$$f(x) = \sum_{u \in GF(2)^n} a_u x^u, \quad a_u \in GF(2). \quad (2)$$

Функцію (анігілятор) $g \in A_d^n(f)$ також представимо у вигляді полінома Жегалкіна

$$g(x) = \sum_{v \in GF(2)^n : w_h(v) \leq d} b_v x^v, \quad (3)$$

де $b_v \in GF(2)$ – невідомі коефіцієнти анігілятора, $w_h(v)$ – вага Хеммінга вектора $v = (v_1, \dots, v_n)$.

Функція g належить простору $A_d^n(f)$ тільки в тому випадку, якщо для будь-якого $x \in GF(2)^n$ виконується рівність $f(x) \cdot g(x) = 0$.

Підставивши (2) та (3) отримуємо:

$$f(x) \cdot g(x) = \left(\sum_{u \in GF(2)^n} a_u x^u \right) \left(\sum_{v \in GF(2)^n : w_h(v) \leq d} b_v x^v \right) = \sum_{u \in GF(2)^n} \left(\sum_{v \in GF(2)^n : w_h(v) \leq d} a_u b_v x^{u \vee v} \right) = 0,$$

де $u \vee v = (u_1 \vee v_1, \dots, u_n \vee v_n)$, \vee – диз'юнкція (логічна операція АБО).

Після групування доданків за загальним множником, отримаємо рівність:

$$\sum_{w \in GF(2)^n} \left(\sum_{a_u, b_v: a_u \vee b_v = w} a_u b_v \right) x^w = 0, \quad (4)$$

яка виконується для будь-якого $w \in GF(2)^n$.

Отже, маємо систему лінійних однорідних рівнянь

$$\left\{ \sum_{a_u, b_v: a_u \vee b_v = w} a_u b_v = 0, \quad \forall w \in GF(2)^n, \right. \quad (5)$$

відносно невідомих коефіцієнтів b_v анілілятора $g(x)$.

Рішення системи (5), наприклад, методом Гауса, задає базис простору $A_d^n(f)$.

Приклад. Для $n = 2$ та $d = 1$ маємо:

$$\begin{aligned} f(x) &= a_{00} + a_{10}x_1 + a_{01}x_2 + a_{11}x_1x_2, \\ g(x) &= b_{00} + b_{10}x_1 + b_{01}x_2. \end{aligned}$$

Після підстановки в $f(x) \cdot g(x) = 0$ отримаємо

$$\begin{aligned} f(x) \cdot g(x) &= a_{00}b_{00} + (a_{00}b_{10} + a_{10}b_{10} + a_{10}b_{00})x_1 + (a_{00}b_{01} + a_{01}b_{01} + a_{01}b_{00})x_2 + \\ &+ (a_{10}b_{01} + a_{01}b_{10} + a_{11}b_{00} + a_{11}b_{10} + a_{11}b_{01})x_1x_2 = 0, \end{aligned}$$

звідки маємо систему лінійних однорідних рівнянь

$$\begin{cases} a_{00}b_{00} = 0, \\ a_{00}b_{10} + a_{10}b_{10} + a_{10}b_{00} = 0, \\ a_{00}b_{01} + a_{01}b_{01} + a_{01}b_{00} = 0, \\ a_{10}b_{01} + a_{01}b_{10} + a_{11}b_{00} + a_{11}b_{10} + a_{11}b_{01} = 0 \end{cases}$$

відносно невідомих b_{00}, b_{10}, b_{01} – коефіцієнтів функції $g(x)$.

Тоді, наприклад, для функції $f(x) = x_1 + x_2$ (тобто при $a_{00} = a_{11} = 0$ та $a_{10} = a_{01} = 1$) отримаємо систему:

$$\begin{cases} b_{10} + b_{00} = 0, \\ b_{01} + b_{00} = 0, \\ b_{01} + b_{10} = 0, \end{cases}$$

котрій задовольняє тільки два рішення:

$$\begin{aligned} b_{00} = b_{10} = b_{01} = 0, \quad \text{тобто } g(x) = 0, \\ b_{00} = b_{10} = b_{01} = 1, \quad \text{тобто } g(x) = 1 + x_1 + x_2. \end{aligned}$$

Безпосередня перевірка показує, що $g(x) = 1 + x_1 + x_2$ дійсно є анілілятором функції $f(x) = x_1 + x_2$:

$$f(x) \cdot g(x) = (x_1 + x_2)(1 + x_1 + x_2) = x_1 + x_2 + x_1 + x_1x_2 + x_1x_2 + x_2 = 0.$$

Узагальнюючи вищевикладене, визначимо основні кроки алгоритму пошуку базису простору аніліляторів [14].

Вхід: $n \in \mathbb{N}$, $d \in \{1, \dots, n\}$, функція $f(x)$ (задана списком одночленів x^u з ненульовими коефіцієнтами a_u в (2)).

Вихід: Лінійний простір $A_d^n(f)$, заданий у вигляді параметричного сімейства багаточленів Жегалкіна від n булевих змінних ступеня $\leq d$.

Крок 1. Представляємо функції $f(x)$ і $g(x)$ у вигляді сум (2) і (3), відповідно.

Крок 2. Відкриваємо дужки в $f(x) \cdot g(x)$ і, групуючи доданки $a_u b_v x^w$ шляхом сортування по $a_u \vee b_v = w$, отримуємо рівняння (4).

Крок 3. Складаємо систему лінійних однорідних рівнянь (5).

Крок 4. Знаходимо загальне рішення системи (5) в параметричному вигляді і подаємо на вихід алгоритму.

У дисертації [14] наводиться оцінка $O\left(m \cdot S_n^d\right)^3$ бітової складності розглянутого алгоритму, де m – кількість ненульових коефіцієнтів a_u в (2).

Використовуючи наведений алгоритм пошуку базису простору анігіляторів можемо обчислити алгебраїчну імунність булевої функції $f(x)$ послідовно перебираючи всі значення $d > 0$ до тих пір, поки не отримаємо нульовий простір анігіляторів $A_d^n(f)$ або $A_d^n(f+1)$. Мінімальне значення $d > 0$, для якого $A_d^n(f) \neq 0$ та/або $A_d^n(f+1) \neq 0$ відповідає значенню алгебраїчної імунності булевої функції $f(x)$.

Алгоритм обчислення алгебраїчної імунності $AI(f)$.

Вхід: $n \in \mathbb{N}$, функція $f(x)$ (задана списком одночленів x^u з ненульовими коефіцієнтами a_u в (2)).

Вихід: Значення алгебраїчної імунності $AI(f)$.

Крок 1. Присвоюємо $d = 1$.

Крок 2. Обчислюємо простір анігіляторів $A_d^n(f)$ і $A_d^n(f+1)$.

Крок 3. Якщо $A_d^n(f) = 0$ і $A_d^n(f+1) = 0$ присвоюємо $d = d+1$ і переходимо до кроку 2.

Крок 4. Якщо $A_d^n(f) \neq 0$ та/або $A_d^n(f+1) \neq 0$ присвоюємо $AI(f) = d$ і подаємо на вихід алгоритму.

3. Алгебраїчний імунітет булевих відображень (S-блоків)

Поняття алгебраїчної імунності булевих функцій в [13] узагальнено на випадок булевих відображень $F: GF(2)^n \rightarrow GF(2)^m$ (векторних булевих функцій), які реалізуються вузлами замін (таблицями підстановок, S-блоками) блокових симетричних шифрів. Для визначення алгебраїчної імунності $AI(F)$ скористаємося термінами та визначеннями з [15].

Зафіксуємо натуральні числа n, m і деяке поле K . Розглянемо кінцеву систему S з m алгебраїчних рівнянь

$$\begin{cases} P_1(x_1, x_2, \dots, x_n) = 0, \\ P_2(x_1, x_2, \dots, x_n) = 0, \\ \dots \\ P_m(x_1, x_2, \dots, x_n) = 0 \end{cases} \quad (6)$$

від змінних x_1, x_2, \dots, x_n з коефіцієнтами над полем K .

Нехай $K[x_1, x_2, \dots, x_n]$ – множина всіх багаточленів від змінних x_1, x_2, \dots, x_n з коефіцієнтами над полем K . На цій множині визначені операції додавання і множення, а саму множину називають *кільцем багаточленів*. Це кільце комутативне (для будь-яких елементів $a, b \in K[x_1, x_2, \dots, x_n]$ виконується рівність $a \cdot b = b \cdot a$), з одиницею (для всіх $a \in K[x_1, x_2, \dots, x_n]$ виконується рівність $a \cdot e = a$, де $e = 1$).

Непуста підмножина I комутативного кільця з одиницею R називається *ідеалом* в R (позначається як $I \triangleleft R$), якщо виконуються наступні дві умови:

- для будь-яких елементів $a, b \in I$ елемент $a - b \in I$;
- для будь-яких $a \in I$ і $c \in R$ елемент $a \cdot c \in R$.

Елементи a_1, a_2, \dots, a_k складають *базис ідеалу*

$$I = (a_1, a_2, \dots, a_k) = \{a_1 \cdot r_1 + a_2 \cdot r_2 + \dots + a_k \cdot r_k; r_1, r_2, \dots, r_k \in R\} \subseteq R$$

Кажуть, що ідеал $I \triangleleft R$ допускає *кінцевий базис*, якщо в ньому знайдуться такі елементи a_1, a_2, \dots, a_k , що $I = (a_1, a_2, \dots, a_k)$.

Фундаментальна *теорема Гілберта про базис* стверджує, що кожен ідеал $I \triangleleft K[x_1, x_2, \dots, x_n]$ допускає кінцевий базис, тобто знайдуться такі $f_1(x_1, x_2, \dots, x_n), f_2(x_1, x_2, \dots, x_n), \dots, f_k(x_1, x_2, \dots, x_n) \in I$, що

$$I = (f_1, f_2, \dots, f_k) = \{f_1 \cdot r_1 + f_2 \cdot r_2 + \dots + f_k \cdot r_k; r_1, r_2, \dots, r_k \in K[x_1, x_2, \dots, x_n]\}$$

З системою S (6) зв'яжемо ідеал I , породжений $P_1(x_1, x_2, \dots, x_n), P_2(x_1, x_2, \dots, x_n), \dots, P_m(x_1, x_2, \dots, x_n)$, що відповідає рівнянням системи:

$$I(S) = (P_1, P_2, \dots, P_m) = \{P_1 \cdot r_1 + P_2 \cdot r_2 + \dots + P_m \cdot r_m; r_1, r_2, \dots, r_m \in K[x_1, x_2, \dots, x_n]\}$$

Якщо $F \in I(S)$, тоді для кожного рішення (X_1, X_2, \dots, X_n) системи (6) буде виконуватися рівність

$$\begin{aligned} F(X_1, X_2, \dots, X_n) &= \\ &= P_1(X_1, X_2, \dots, X_n) \cdot r_1(X_1, X_2, \dots, X_n) + P_2(X_1, X_2, \dots, X_n) \cdot r_2(X_1, X_2, \dots, X_n) + \dots + \\ &+ P_m(X_1, X_2, \dots, X_n) \cdot r_m(X_1, X_2, \dots, X_n) = \\ &= 0 \cdot r_1(X_1, X_2, \dots, X_n) + 0 \cdot r_2(X_1, X_2, \dots, X_n) + \dots + 0 \cdot r_m(X_1, X_2, \dots, X_n) = 0. \end{aligned}$$

Якщо $\{P_1, P_2, \dots, P_m\}$ і $\{\bar{P}_1, \bar{P}_2, \dots, \bar{P}_k\}$ – два базиси одного ідеалу I , тоді системи алгебраїчних рівнянь

$$\begin{cases} P_1(x_1, x_2, \dots, x_n) = 0, \\ P_2(x_1, x_2, \dots, x_n) = 0, \\ \dots \\ P_m(x_1, x_2, \dots, x_n) = 0, \end{cases} \quad \begin{cases} \bar{P}_1(x_1, x_2, \dots, x_n) = 0, \\ \bar{P}_2(x_1, x_2, \dots, x_n) = 0, \\ \dots \\ \bar{P}_k(x_1, x_2, \dots, x_n) = 0 \end{cases}$$

еквівалентні, тобто множини їх рішень збігаються.

Отже, множина рішень системи алгебраїчних рівнянь однозначно визначається ідеалом системи, а різні базиси одного ідеалу відповідають еквівалентним системам [15].

Припустимо, що є деякий багаточлен $h(x_1, x_2, \dots, x_n) \in K[x_1, x_2, \dots, x_n]$ і потрібно за кінцеве число кроків з'ясувати, чи належить він ідеалу $I \triangleleft K[x_1, x_2, \dots, x_n]$, заданому своїм базисом $I = (f_1, f_2, \dots, f_m)$. Іншими словами, потрібно вирішити т.зв. *задачу входження*: з'ясувати, чи існують такі багаточлени $r_1(x_1, x_2, \dots, x_n), r_2(x_1, x_2, \dots, x_n), \dots, r_m(x_1, x_2, \dots, x_n)$, що $h = f_1 \cdot r_1 + f_2 \cdot r_2 + \dots + f_m \cdot r_m$ і $h \in I = (f_1, f_2, \dots, f_m)$.

Задачу входження вирішують за допомогою спрощення виразу $h(x_1, x_2, \dots, x_n)$, використовуючи т.зв. *редукцію багаточлена*. Запишемо поліном $h(x_1, x_2, \dots, x_n)$ у вигляді суми $h = h_C + h_M$, де h_C – старший одночлен (моном), а h_M – сума решти одночленів в h . Припус-

тимо також, що h_C ділиться на старший член f_{iC} одного з багаточленів f_i , тобто $h_C = f_{iC} \cdot Q$ і $h = f_{iC} \cdot Q + h_M$ для деякого одночлена Q . Тоді операція редукації задається виразом

$$h_1 = h - f_i \cdot Q = f_{iC} \cdot Q + h_M - f_{iC} \cdot Q - f_{iM} \cdot Q = h_M + (-f_{iM}) \cdot Q, \quad (7)$$

де f_{iM} – сума решти одночленним в $f_i = f_{iC} + f_{iM}$. При цьому старший член багаточлена h_1 менше старшого члена багаточлена h . Якщо багаточлен h належить ідеалу $I = (f_1, f_2, \dots, f_m)$, тоді і редукований багаточлен h_1 також буде належати до цього ідеалу. Дійсно, якщо $h \in (f_1, f_2, \dots, f_m)$, тоді $h - h_1 = f_i Q \in (f_1, f_2, \dots, f_m)$. Отже, задачу входження тепер можна вирішувати вже не для багаточлена h , а для редукованого багаточлена h_1 . Якщо за кінцеве число редукацій (7) багаточлен h зведеться (редукується) до нуля (нуль належить будь-якому ідеалу), тоді $h \in (f_1, f_2, \dots, f_m)$.

Базис f_1, f_2, \dots, f_m ідеалу називається **базисом Грьобнера** цього ідеалу, якщо всякий багаточлен $h \in I$ редукується до нуля за допомогою f_1, f_2, \dots, f_m . Інакше: набір багаточленів $f_1, f_2, \dots, f_m \in I$ є базисом Грьобнера в ідеалі $I = (f_1, f_2, \dots, f_m)$, якщо для будь-якого $h \in I$ одночлен h_C ділиться на один з одночленів $f_{1C}, f_{2C}, \dots, f_{mC}$ [15].

Для операції редукації багаточленів використовується поняття старшого одночлена (монома). Іншими словами, передбачається, що на множині всіх одночленів кільця $K[x_1, x_2, \dots, x_n]$ заданий **лінійний порядок** (мономіальне упорядкування \prec), який задовольняє наступним властивостям [16]:

– з $x^u \prec x^v$ випливає, що $x^w \cdot x^u \prec x^w \cdot x^v$ для будь-яких одночленів x^u, x^v, x^w (одночлени визначені як в (2), тобто $x, u, v, w \in V_2^n, x = (x_1, \dots, x_n), u = (u_1, \dots, u_n), v = (v_1, \dots, v_n), w = (w_1, \dots, w_n)$);

– $1 \preceq x^v$ для будь-якого одночлена x^v .

Як приклади мономіального упорядкування наведемо:

– **словниковий (лексикографічний) порядок (lex)**: $x^u \prec_{\text{lex}} x^v$, якщо існує таке i , що $u_i < v_i$ і $u_j = v_j$ для $j < i$ (спочатку упорядковуємо змінні в одночленах в необхідному алфавітному порядку, а потім дивимося до першої відмінності в одночленах);

– **ступінево-словниковий порядок (deglex)**: $x^u \prec_{\text{deglex}} x^v$, якщо $w_h(u) < w_h(v)$ або $w_h(u) = w_h(v)$, але при цьому $x^u \prec x^v$ в словниковому порядку (упорядковуємо за сумою ступенів, в разі рівності сум порівнюємо за словниковим порядком);

– **ступінево-зворотній словниковий порядок (degrevlex)**: $x^u \prec_{\text{degrevlex}} x^v$, якщо $w_h(u) < w_h(v)$ або $w_h(u) = w_h(v)$, але при цьому $x^u \succ_{\text{lex}} x^v$ в словниковому порядку (упорядковуємо за сумою ступенів, в разі рівності сум порівнюємо за зворотним словниковим порядком).

Рішення задачі входження, тобто визначення приналежності багаточлена h ідеалу $I = (f_1, f_2, \dots, f_m)$, полягає в побудові всіх можливих редукацій h за допомогою елементів базису Грьобнера ідеалу I . Багаточлен h належить ідеалу $I = (f_1, f_2, \dots, f_m)$ тоді і тільки тоді, коли в результаті редукації одержано нуль [15].

Для кожного ідеалу $I \triangleleft K[x_1, x_2, \dots, x_n]$ існує базис Грьобнера, а сама побудова базису Грьобнера ґрунтується на вирішенні **зачеплень** [15]. Багаточлени f_i і f_j мають зачеплення, якщо їх старші члени діляться одночасно на деякий одночлен ω , відмінний від константи. Нехай $f_{iC} = \omega \cdot q_1$, $f_{jC} = \omega \cdot q_2$, де ω – найбільший спільний дільник старших одночленів f_{iC} і f_{jC} . Розглянемо багаточлен $F_{i,j} = f_i \cdot q_2 - f_j \cdot q_1 \in I$ і редукуємо його за допомогою базису

f_1, f_2, \dots, f_m до тих пір, поки це можливо. Якщо отриманий в результаті багаточлен $F'_{i,j} \equiv 0$, тоді кажуть, що *зачеплення вирішується*. Інакше, додамо до базису f_1, f_2, \dots, f_m ідеалу I отриманий багаточлен $f_{m+1} = F'_{i,j}$, після чого процедуру пошуку і редукування зачеплення продовжимо. Після редукування кінцевого числа зачеплення отримаємо набір $f_1, f_2, \dots, f_m, f_{m+1}, \dots, f_M$, в якому кожне зачеплення вирішується.

Відповідно до *діамантової лемми* базис f_1, f_2, \dots, f_m ідеалу $I \triangleleft K[x_1, x_2, \dots, x_n]$ є базисом Грьобнера тільки тоді, коли в ньому немає *нерозв'язних зачеплень* [15].

Розв'язання зачеплень дозволяє визначити ефективний алгоритм побудови базису Грьобнера ідеалу $I = (f_1, f_2, \dots, f_m)$ (*алгоритм Бухбергера*).

Крок 1. Перевіряємо наявність зачеплень в наборі f_1, f_2, \dots, f_m . Якщо зачеплень немає, тоді набір f_1, f_2, \dots, f_m є базисом Грьобнера ідеалу $I = (f_1, f_2, \dots, f_m)$. Якщо зачеплення є, тоді переходимо до кроку 2.

Крок 2. По знайденому зачепленню багаточленів f_i і f_j складаємо багаточлен $F_{i,j} = f_i \cdot q_2 - f_j \cdot q_1$ і редукуємо його за допомогою набору f_1, f_2, \dots, f_m поки це можливо. Якщо багаточлен $F_{i,j}$ редукувався до ненульового багаточлена переходимо до кроку 3, інакше – до кроку 4.

Крок 3. Додаємо многочлен f_{m+1} до набору f_1, f_2, \dots, f_m і переходимо до кроку 4.

Крок 4. Шукаємо раніше нерозглянуте зачеплення і переходимо до кроку 2. Якщо всі зачеплення розглянуті, тоді виводимо отриманий набір $f_1, f_2, \dots, f_m, f_{m+1}, \dots, f_M$, в якому всі зачеплення можна розв'язати. Це і є базис Грьобнера ідеалу $I = (f_1, f_2, \dots, f_m)$.

На сьогоднішній день відомі й інші алгоритми побудови базису Грьобнера, наприклад алгоритми F4, F5 [17, 18].

Базис Грьобнера можна спростити наступними способами [15].

1. *Мінімізація базису Грьобнера.* Якщо f_i і f_j два елементи базису Грьобнера, причому їх старші члени f_{iC} і f_{jC} діляться один на одного, наприклад $f_{jC} | f_{iC}$, тоді багаточлен f_i можна видалити з набору f_1, f_2, \dots, f_m . Базис Грьобнера називають *мінімальним*, якщо f_{iC} не ділиться на f_{jC} для всіх $i \neq j$.

2. *Редукування базису Грьобнера.* Якщо деякий член q багаточлена f_i ділиться на старший член багаточлена f_j , тоді редукуємо q за допомогою f_j і результат редукації запишемо замість члена q в багаточлен f_i . При цьому базис Грьобнера залишиться базисом Грьобнера, число елементів базису не зміниться, проте ступеня багаточленів f_1, f_2, \dots, f_m понижуються. Базис Грьобнера називають *редукованим*, якщо жоден член багаточлена f_i не ділиться на старший член многочлена f_j для всіх $i \neq j$.

Мінімальний редукований базис Грьобнера ідеалу $I \triangleleft K[x_1, x_2, \dots, x_n]$ визначено однозначно (з одиничними коефіцієнтами при старших ступенях елементів базису), тобто не залежить від вибору вихідного базису ідеалу $I = (f_1, f_2, \dots, f_m)$ і від послідовності операцій, що проводяться (але залежить від упорядкування змінних x_1, x_2, \dots, x_n) [15].

Поняття мінімального редукованого базису Грьобнера використано в роботі Жан-Шарля Фожера (Jean-Charles Faugère) [13] для визначення алгебраїчної імунності S-блоків (нелінійних вузлів ускладнення) блокових симетричних шифрів.

Розглянемо нелінійний вузол (S-блок) блочного симетричного шифру (див. рис. 2), який реалізує булеве відображення $S : GF(2)^n \rightarrow GF(2)^m$ [1-9].

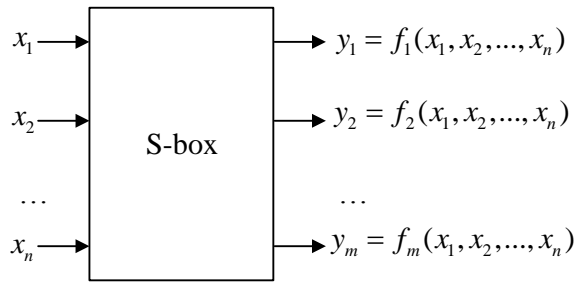


Рис. 2

S-блок задається системою алгебраїчних рівнянь над двійковим полем:

$$\begin{cases} f_1(x_1, x_2, \dots, x_n) = y_1, \\ f_2(x_1, x_2, \dots, x_n) = y_2, \\ \dots \\ f_m(x_1, x_2, \dots, x_n) = y_m, \end{cases} \quad (8)$$

тобто сукупністю булевих багаточленів

$$\begin{aligned} & y_1 - f_1(x_1, x_2, \dots, x_n), \\ & y_2 - f_2(x_1, x_2, \dots, x_n), \\ & \dots, \\ & y_m - f_m(x_1, x_2, \dots, x_n) \end{aligned} \quad (9)$$

в кільці $K[x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m]$ від змінних $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m$ з коефіцієнтами над полем $K = GF(2)$.

З системою рівнянь (8), що алгебраїчно задають структуру S-блоку, зв'яжемо ідеал I , породжений багаточленами (9):

$$\begin{aligned} I(S) &= (y_1 - f_1(x_1, x_2, \dots, x_n), y_2 - f_2(x_1, x_2, \dots, x_n), \dots, y_m - f_m(x_1, x_2, \dots, x_n)) = \\ &= (y_1 - f_1) \cdot r_1 + (y_2 - f_2) \cdot r_2 + \dots + (y_m - f_m) \cdot r_m; r_1, r_2, \dots, r_m \in GF(2)[x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m]. \end{aligned}$$

Алгебраїчна імунність нелінійного вузла блокового симетричного шифру визначається як мінімальна ступінь багаточлена P з ідеалу $I(S)$ [13]:

$$AI(S) = \min\{\deg(P), P \in I(S) \triangleleft GF(2)[x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m]\}, \quad (10)$$

причому мінімальний редукований базис Грьобнера ідеалу $I(S)$ при ступеневому-зворотньому словниковому впорядкуванні (degrevlex) містить лінійний базис поліномів P з $I(S)$, таких, що $AI(S) = \deg(P)$. Іншими словами, для обчислення алгебраїчної імунності досить побудувати мінімальний редукований базис Грьобнера ідеалу $I(S)$, заданого рівняннями (9) і знайти многочлен мінімального ступеня серед елементів цього базису. Значення мінімального ступеня і є значенням алгебраїчної імунності вузла заміни блокового симетричного шифру.

Зв'язок алгебраїчної імунності S-блоку (10) і булевої функції (1) показаний в [19, с. 337]. Розглянемо булеву функцію $f_S(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m) : GF(2)^{2n} \rightarrow GF(2)$, значення якої визначимо наступним чином:

$$f_S(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m) = \begin{cases} 1, \forall i, j : f_i(x_1, x_2, \dots, x_n) = y_j, \\ 0, \forall i, j : f_i(x_1, x_2, \dots, x_n) \neq y_j. \end{cases}$$

Множина рішень рівняння

$$f_S(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m) - 1 = 0.$$

Співпадає з множиною рішень системи (8). Отже, маємо різні базиси $(f_S - 1)$ та $(y_1 - f_1, y_2 - f_1, \dots, y_m - f_m)$ одного ідеалу еквівалентних систем. Тобто

$$I(f_S - 1) = I(y_1 - f_1, y_2 - f_1, \dots, y_m - f_m).$$

Ідеал простору анігіляторів $Ann(f_S)$ в кільці $GF(2)[x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m]$ збігається з ідеалом $I(f_S - 1)$, отже, алгебраїчна імунність (10) булевого відображення $S : GF(2)^n \rightarrow GF(2)^m$ збігається з мінімальним ступенем ненульових поліномів, що належать анігілятору функції f_S :

$$AI(S) = \min\{Deg(g) \mid g \in Ann(f_S)\}.$$

Таким чином, будь-який S-блок можна однозначно описати булевою функцією [19], алгебраїчну імунність цієї функції можна обчислити, наприклад, за допомогою алгоритму з п. 2.

4. Значення алгебраїчної імунності нелінійних вузлів сучасних шифрів

В даній роботі проведено порівняльні дослідження алгебраїчної імунності нелінійних вузлів сучасних симетричних шифрів. Як об'єкти дослідження обрані широко відомі і стандартизовані на національному та/або міжнародному рівні блокові симетричні криптоперетворення:

- криптоалгоритм AES, стандартизований в США як федеральний стандарт обробки даних FIPS-197 [20], а також на міжнародному рівні в ISO/IEC 18033-3 [21];
- криптоалгоритм Camellia, стандартизований в ISO/IEC 18033-3 [21];
- криптоалгоритм CAST, стандартизований в ISO/IEC 18033-3 [21];
- криптоалгоритм SEED, стандартизований в ISO/IEC 18033-3 [21];
- криптоалгоритм «Калина», національний стандарт України ДСТУ 7624: 2014 [22];
- криптоалгоритм «Кузнечик», стандартизований в Росії як ГОСТ 34.12-2015 [23];
- алгоритм «BelT» симетричного шифрування і контролю цілісності Республіки Білорусь, стандартизований в СТБ 34.101.31-2011 [24];
- криптографічна хеш-функція Whirlpool, заснована на використанні блокових симетричних криптоперетворень, стандартизована в ISO/IEC 10118-3: 2004 [25].

Для обчислення алгебраїчного імунітету використовувався вираз (10). Для безпосередніх обчислень використано пакет прикладного програмного забезпечення Magma [26], який реалізує широкий спектр функцій, пов'язаних з алгеброю, теорією груп, кілець і полів, теорією чисел і багатьма іншими розділами математики.

Досліджувані вузли замінь, окрім S-блоку хеш-функції Whirlpool, були детально розглянуті в нашій роботі [9], в таблиці наведено деякі результати досліджень.

Криптоалгоритм	B	N	A	AD	PC	CI	AI
AES	+	112	32	7	0	0	2
SEED	-	110	40	7	0	0	2
CAST-128	-	120	0	4	8	0	2
Camellia	+	112	32	7	0	0	2
«Калина»	+	104	72	7	0	0	3
«Кузнечик»	+	102	72	7	0	0	3
«BelT»	+	104	72	7	0	0	3
Whirlpool	+	95	80	7	0	0	3

У таблиці використані наступні позначення [9]:

- В – збалансованість;
- N – нелінійність;
- А – автокореляція;
- AD – алгебраїчна ступінь;
- PC – критерій поширення;
- CI – кореляційний імунітет.

В останній колонці «AI» таблиці наведено значення алгебраїчної імунності нелінійних вузлів заміни сучасних шифрів. Ці дані отримано за формулою (10) за допомогою побудови базисів Грьобнера ідеалів $I(S)$, заданих сукупностями багаточленів (9) з рівнянь (8) відповідних S-блоків.

Отримані результати дозволяють судити про недостатню алгебраїчну імунність нелінійних вузлів блокових шифрів, які були розроблені в кінці 90-х – початку 2000-х років. Розглянуті алгоритми (AES, SEED, CAST-128, Camellia) представлені в сучасному міжнародному стандарті ISO/IEC 18033-3, мають порівняно низьку алгебраїчну імунність і потенційно можуть розглядатися в якості реальних кандидатів на побудову ефективних алгебраїчних атак.

Блокові симетричні криптоалгоритми «Калина», «Кузнечик», «BelT», а також криптографічна функція хешування Whirlpool були розроблені з урахуванням можливого застосування алгебраїчних атак. Нелінійні вузли заміни цих алгоритмів мають високу алгебраїчну імунність і, вочевидь, залишаться стійкими до нових методів алгебраїчного криптоаналізу.

5. Висновки

Методи алгебраїчного криптоаналізу, з моменту перших публікацій [27, 28], перетворилися з абстрактних і маловживаних математичних ідей в розвинений і широко обговорюваний в науковому співтоваристві розділ сучасної криптології. На сьогоднішній день в цій галузі знань проводиться величезна кількість дослідницьких проектів і, очевидно, слід очікувати в найближчі роки появи ефективних обчислювальних алгоритмів алгебраїчного криптоаналізу сучасних симетричних шифрів.

У даній роботі були розглянуті окремі аспекти алгебраїчного криптоаналізу, зокрема, досліджені методи обчислення алгебраїчної імунності нелінійних вузлів симетричних шифрів. Це поняття, вперше введене для потокових криптоалгоритмів в роботах [10, 11], було узагальнено в [13] на випадок булевих відображень, тобто для нелінійних вузлів з довільною розмірністю входів-виходів. Алгебраїчна імунність в деякому розумінні характеризує складність вирішення системи рівнянь, що описують нелінійний вузол і дозволяє, таким чином, отримати уявлення про стійкість симетричного шифру до алгебраїчного криптоаналізу. Зокрема, в роботі [10] запропонований алгоритм алгебраїчного криптоаналізу потокових шифрів, побудованих за схемою фільтр-генератора, складність реалізації цього алгоритму є функцією від значення алгебраїчної імунності нелінійного вузла ускладнення.

Обчислення алгебраїчної імунності в загальному випадку пов'язане з побудовою базису Грьобнера ідеалу кільця многочленів, заданого многочленами з рівнянь вузла ускладнення. Ця задача вирішується обчислювально ефективними алгоритмами Бухбергера, F4, F5 та ін. [15 – 18]. Крім того, розглянуті математичні методи можуть також використовуватися і для пошуку ефективних алгебраїчних атак [29], що підтверджує перспективність і актуальність проведених робіт в даній області.

У даній роботі наведені значення алгебраїчного імунітету для вузлів заміни деяких сучасних шифрів. Зокрема, встановлено, що криптоалгоритми, розроблені на рубежі 90-х – початку 2000-х років, не володіють граничними значеннями алгебраїчної імунності, тобто потенційно можуть розглядатися як кандидати на побудову ефективних алгебраїчних атак. Блокові шифри останнього покоління («Калина», «Кузнечик», «BelT») розроблялися з урахуванням можливого застосування алгебраїчного криптоаналізу і володіють граничними значеннями алгебраїчного імунітету.

Перспективним напрямком є подальші дослідження методів алгебраїчного криптоаналізу, зокрема, застосування технологій квантових обчислень для вирішення систем алгебраїчних рівнянь, що описують симетричний шифр. На думку авторів даної роботи, саме в цьому напрямку досліджень очікуються найбільш значущі і цікаві наукові результати.

Список літератури: 1. *Alfred, J. Menezes, Paul C. van Oorschot, Scott, A. Vanstone.* Handbook of Applied Cryptography – CRC Press, 1997. – 794 p. 2. *Горбенко, І.Д., Горбенко, Ю.І.* Прикладна криптологія. Теорія. Практика. Застосування: Підручник для вищих навч. закладів. – Харків : Форт, 2013. – 880 с. 3. *Bart Preneel.* Analysis and Design of Cryptographic Hash Functions. [Електронний ресурс] – Режим доступу: homes.esat.kuleuven.be/~preneel/phd_preneel_feb1993.pdf 4. *Carlet, C.* Vectorial Boolean functions for // Cambridge Univ. Press, Cambridge. – 95 p. [Електронний ресурс] – Режим доступу: www.math.univ-paris13.fr/~carlet/chap-vectorial-fcts-corr.pdf 5. *Carlet, C.* Boolean functions for cryptography and error correcting codes // Cambridge Univ. Press, Cambridge. – 2007. – 148 p. [Електронний ресурс] – Режим доступу: www1.spms.ntu.edu.sg/~kkhoongm/chap-fcts-Bool.pdf 6. *Zhuo Zepeng, Zhang Weiguo* On correlation properties of Boolean functions // Chinese Journal of Electronics. Jan, Vol.20, 2011, №1, 143-146 pp. 7. *O'Connor, L.* An analysis of a class of algorithms for S-box construction // J. Cryptology. -1994. – p. 133-151. 8. *Clark J.A., Jacob J.L., Stepney S.* The Design of S-Boxes by Simulated Annealing // New Generation Computing. – 2005. – 23(3). – p.219–231. 9. *Кузнецов, А.А., Белозерцев, И.Н., Андрушкевич, А.В.* Анализ и сравнительные исследования нелинейных узлов замены современных блочных симметричных шифров // Прикладная радиоэлектроника. – Харьков : ХНУРЭ, 2015. – Т. 14. №4. – С.343 – 350. 10. *Courtois, N., Meier, W.* Algebraic Attacks on Stream Ciphers with Linear Feedback, Eurocrypt 2003, LNCS 2656, Springer, 2003. – pp. 345-359. 11. *Meier, W., Pasalic, E., Carlet, C.* Algebraic Attacks and Decomposition of Boolean Functions, Eurocrypt 2004, LNCS 3027, Springer, 2004. – pp. 474-491. 12. *Nicolas Courtois; Josef Pieprzyk* (2002). Cryptanalysis of Block Ciphers with Overdefined Systems of Equations // LNCS. 2501: 267–287. 13. *Gw'eno'le' Ars, Jean-Charles Faug'ere.* Algebraic Immunities of functions over finite fields. [Research Report] RR-5532, INRIA. 2005, pp.17. 14. *Баев, В. В.* Эффективные алгоритмы получения оценок алгебраической иммунности булевых функций : дис. ... канд. физ.-мат. наук : 01.01.09 / Баев Владимир Валерьевич; [Место защиты: Моск. гос. ун-т им. М.В. Ломоносова. Фак. вычислит. математики и кибернетики]. – Москва, 2008. – 101 с. 15. *Аржанцев, И.В.* Базисы Грёбнера и системы алгебраических уравнений. Летняя школа. Современная математика. Дубна, июль 2002. – Москва : МЦНМО, 2003. – 68 с. 16. *Злобин, А.И., Соколова, О.В.* Компьютерная алгебра в системе Sage. Учебное пособие. – Москва : МГТУ им. Баумана, 2011. – 55 с. 17. *Faugère, J.-C.* (June 1999). A new efficient algorithm for computing Gröbner bases (F4). Journal of Pure and Applied Algebra. Elsevier Science. 139 (1): 61–88. 18. *Faugère, J.-C.* (July 2002). A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). Proceedings of the 2002 international symposium on Symbolic and algebraic computation (ISSAC). ACM Press: 75–83. 19. *Massimiliano Sala, Teo Mora, Ludovic Perret, Shojiro Sakata, Carlo Traverso* Gröbner Bases, Coding, and Cryptography. Springer-Verlag Berlin Heidelberg. – 426 p. 20. *FIPS 197.* National Institute of Standards and Technology. [Electronic resource]: Advanced Encryption Standard. – 2001. – Available at: <http://www.nist.gov/aes>. 21. *ISO/IEC 18033-3.* Information technology – Security techniques – Encryption algorithms, Part 3: Block ciphers, 80 p. 22. *ДСТУ 7624:2014.* Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Київ : Мінекономрозвитку України, 2015. – 238 с. 23. *ГОСТ Р 34.12-2015.* Информационная технология. Криптографическая защита информации. Блочные шифры. – Москва : Стандартиформ, 2015. – 25с. 24. *СТБ 34.101.31-2011.* Информационные технологии и безопасность. Криптографические алгоритмы шифрования и контроля целостности. – Минск : Госстандарт, 2011. – 32 с. 25. *ISO/IEC 10118-3:2004.* Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions, 94 p. 26. *Magma* Computational Algebra System. Available at: <http://magma.maths.usyd.edu.au/magma/> 27. *Nicolas Courtois, Alexander Klimov, Jacques Patarin, Adi Shamir.* Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. Proceeding EUROCRYPT'00 Proceedings of the 19th international conference on Theory and application of cryptographic techniques. P. 392-407. 28. *Nicolas Courtois, Josef Pieprzyk.* Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. Advances in cryptology – ASIACRYPT 2002. P.267-287. 29. *Andrey Pyshkin.* Algebraic Cryptanalysis of Block Ciphers Using Grobner Bases. Dissertation zur Erlangung des Grades Doktor rerum naturalium. Technischen Universität Darmstadt. – Darmstadt, 2008, 118 p.