УДК 004.056

МЕТОДИ ПОБУДОВИ MDS-МАТРИЦЬ НАД СКІНЧЕННИМИ ПОЛЯМИ ТА КІЛЬЦЯМИ

В. В. Дідан[1, a]

[1] *Національний технічний університет України «Київський політехнічний інститут»*

Анотація

В роботі розглянуто конструкції лінійних перетворень, що використовуються в сучасних симетричних блокових шифрах та геш-функціях, а саме: конструкції MDS-матриць над скінченними полями характеристики 2, та проаналізована можливість використання цих конструкцій над кільцем лишків за модулем 2^n.

Ключові слова: MDS-матриця, maximum distance separable, розсіюючий шар, циркулянтна матриця, матриця Коші, матриця Вандермонда

Вступ

Лінійні перетворення над скінченними полями характеристики 2, що використовуються в блокових шифрах, на даний час достатньо вивчені, відомий їх вплив на стійкість шифру до різних атак, чого не можна сказати про перетворення над кільцем лишків за модулем 2^n. Але використання перетворень над кільцем дало б змогу побудувати криптографічно стійкі шифри з теоретичної та практичної точки зору. Тому постає задача пошуку MDS-матриць над кільцем лишків за модулем 2^n, яка буде вирішуватися шляхом перенесення відомих алгебраїчних конструкцій MDS-матриць над скінченним полем характеристики 2 на кільце лишків за модулем 2^n [1].

1. Необхідні терміни та позначення

Матриця $m \times n$ – це прямокутна таблиця $A = \|a_{ij}\|$, $1 \le i \le m$, $1 \le j \le n$, де кожен a_{ij} є елементом скінченного поля.

Підматрицею матриці A називається матриця, що отримана шляхом викреслювання рядків або стовпців матриці A.

Матриця над скінченним полем є невиродженою, якщо її визначник не дорівнює 0.

Інволютивною називається така квадратна матриця A, що задовольняє умові $A^2 = I$, де I – це одинична матриця над скінченним полем.

Циркулянтна матриця – це матриця C розмірності $k \times k$, яка записана у вигляді

$$C = \begin{bmatrix} c_1 & c_2 & \dots & c_k \\ c_k & c_1 & \dots & c_{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_2 & c_3 & \dots & c_1 \end{bmatrix},$$

тобто кожен рядок матриці, починаючи з другого, одержується обертанням попереднього рядка праворуч на один елемент.

Мариця Коші – це матриця C розмірності $m \times n$, що складається з двох наборів елементів з $GF(2^n)$, $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ та $\{\beta_1, \beta_2, \dots, \beta_n\}$, така, що $c_{ij} = \frac{1}{\alpha_i + \beta_j}$, $1 \le i \le m$, $1 \le j \le n$. Детермінант квадратної матриці Коші розмірності $k \times k$ визначається за формулою:

$$det(C) = \frac{\prod\limits_{1 \le i < j \le k} (\alpha_j - \alpha_i)(\beta_j - \beta_i)}{\prod\limits_{1 \le i < j \le k} (\alpha_i + \beta_j)}.$$

Матриця Вандермонда – це матриця V розмірності $m \times d$ вигляду

$$V = \begin{bmatrix} 1 & v_1 & v_1^2 & \dots & v_1^{d-1} \\ 1 & v_2 & v_2^2 & \dots & v_2^{d-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & v_m & v_m^2 & \dots & v_m^{d-1} \end{bmatrix},$$

де $v_1, v_2, \dots, v_{m-1}$ – елементи скінченного поля. Визначник квадратної матриці Вандермонда розмірності $m \times m$ визначається за формулою:

$$det(V) = \prod_{1 \le i < j \le m} (v_j - v_i).$$

Індексом розгалуження β матриці M розмірності $k \times k$ над скінченним полем називається найменше число з суми ненульових елементів $k \times 1$-вектора X та $k \times 1$-вектора $Y = M \cdot X$ (позначається як $wt(X)$ та $wt(Y)$ відповідно) серед всіх $X \ne 0$, тобто $\beta = \min\limits_{X \ne 0}\{wt(X) + wt(Y)\}$, де $X = (x_1, x_2, \dots, x_k)^T$ та $Y = (y_1, y_2, \dots, y_k)^T$ - вектори, що складаються з елементів скінченного поля.

Індекс розгалуження β називається максимальним, якщо для матриці M розмірності $k \times k$ він дорівнює $k + 1$.

2. MDS-коди та MDS-матриці

Термін «maximum distance separable» (MDS) походить з теорії кодів виправлення помилок. Наведемо деякі означення з цієї теорії.

[a] vdidan@mail.ru

Лінійний (n, k, d)-код над $GF(2^r)$ – це k-мірний підпростір векторного простору $(GF(2^r))^n$, де d – це відстані Хеммінга між двома різними n-елементними векторами, тобто номер позиції (з n), з якої два вектори розрізняються. Для лінійного (n, k, d)-коду над будь-яким полем виконується умова $d \leq n - k + 1$. Код, для якого $d = n - k + 1$, називається Maximum Distance Separable Code, або MDS-код.

Матриця M розмірності $k \times k$ – це MDS-матриця тоді і тільки тоді, коли генератор $G = [I_k|M]$, де I_k – це одинична матриця розмірності $k \times k$, генерує MDS-код з параметрами $(2k, k, k + 1)$.

MDS-матриці використовуються в теорії кодування і виконують значну роль при побудові блокових шифрів. MDS-матриці дають змогу побудувати розсіюючий шар з максимальним індексом розгалуження, а, як відомо, чим більший цей індекс, тим стійкіший шифр до таких типів атак, як диференціальний та лінійний криптоаналіз.

3. Конструкції MDS-матриць над скінченними полями характеристики 2

В зазначена головна вимога до конструкції MDS-матриці: кожна квадратна підматриця MDS-матриці повинна бути невиродженою. Цю вимогу ще називають MDS-властивістю.

MDS-матриця не обов'язково має бути інволютивною, але це має значний вплив на роботу блокового шифру, в якому вона буде використовуватися. У випадку використання інволютивної MDS-матриці при побудові блокового шифру зашифрування і розшифрування будуть реалізовуватися як дві подібні операції та будуть виконуватися з однаковою швидкістю.

Відомі два основні підходи до побудови MDS-матриць.

Перший з підходів базується на конструюванні випадкової матриці та наступній перевірці того, чи задовольняється MDS-властивість. Але цей спосіб є достатньо трудомістким навіть при побудові MDS-матриць невеликого розміру.

Другий підхід пов'язаний з використанням відомих алгебраїчних конструкцій матриць, які гарантовано володіють MDS-властивістю. Розглянемо докладніше MDS-матриці, що побудовані за цим підходом.

В шифрі AES в операції MixColumn використовується MDS-матриця, що побудована на основі циркулянтної матриці. Було доведено, що ця матриця не є інволютивною, тому, як відомо з конструкції AES, в операції, оберненій до MixColumn, використовується зовсім інша матриця. Розглянемо іншу алгебраїчну конструкцію – матрицю Коші розмірності $k \times k$, що складається з двох різних наборів елементів з $GF(2^n)$, $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ та $\{\beta_1, \beta_2, \ldots, \beta_k\}$. Так як $\alpha_i \neq \alpha_j$, $\beta_i \neq \beta_j$ для всіх $i, j \in \{1, 2, \ldots, k\}$, то матриця Коші невироджена над полем. Також відомо, що будь-яка підматриця матриці Коші є матрицею Коші, і, відповідно, будь-яка підматриця матриці Коші є невиродженою. Таким чином, матриця Коші володіє MDS-властивістю, тому матриця Коші, побудована над скінченним полем характеристики 2, є MDS-матрицею. До того ж, матриця Коші інволютивна над скінченим полем.

MDS-матрицю можна отримати з матриці Вандермонда. У такому випадку розглядається матриця Вандермонда розмірності $m \times m$, у якої всі елементи $v_1, v_2, \ldots, v_m$ різні, тобто для всіх $i \neq j$: $v_i \neq v_j$. MDS-матриця, побудована на основі матриць Вандермонда, є інволютивною. Також виявлено, що за певних умов матриця Вандермонда над скінченним полем може мати вироджені квадратні підматриці, що суперечить MDS-властивості, тому MDS-матрицю можна отримати не з кожної матриці Вандермонда.

В результаті роботи було виявлено, що вищенаведені конструкції MDS матриць справедливі і для $GF(p)$, де p – просте число і $p \geq 3$.

4. Існування MDS-матриць над кільцями

Спробуємо побудувати MDS-матрицю над кільцем лишків за модулем 2^n шляхом перенесення вищерозглянутих конструкцій MDS-матриць над скінченним полем характеристики 2 на кільце $\mathbb{Z}_{2^n}$.

Незалежно від того, з яких елементів буде складатися матриця Коші, парних, непарних, чи їх комбінації, над кільцем вона буде виродженою, тобто її визначник не буде взаємнопростим з 2^n. Отже, бачимо, що матриця Коші побудована над кільцем лишків за модулем 2^n, не володіє MDS-властивістю. Теж саме спостерігаємо і при побудові матриці Вандермонда.

Отже, над кільцем неможливо побудувати MDS-матрицю з матриць Коші та Вандермонда через порушення MDS-властивості.

Висновки

MDS-матриця є важливою складовою сучасних блокових шифрів. Вона дозволяє побудувати розсіюючий шар з максимальним індексом розгалуження, що робить блоковий шифр більш стійким до різного роду атак.

В ході роботи було виявлено, що найбільше використаня отримали MDS-матриці побудовані над скінченним полем характеристики 2 на основі алгебраїчних конструкцій, що гарантовано володіють MDS-властивістю. Доведено, що ці конструкції не дають змогу побудувати MDS-матрицю над кільцем лишків за модулем 2^n. Тому подальші дослідження будуть спрямовані на пошук максимально можливого теоретичного значення індекса розгалуження над кільцем лишків та побудову відповідного йому криптографічного перетворення.

Перелік використаних джерел

1. Shannon C. Communication theory of secrecy systems // Bell System Technical Journal. — 1949. — Vol. 28, no. 4. — P. 656–715.