نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال دهم، شماره ۴، زمستان ۱۳۹۸؛ ص ۴۱۷-۴۰۷

طراحی و ساخت ماتریس‌های سبک‌وزن MDS شبه خودمعکوس بر اساس ساختارهای بازگشتی و ماتریس‌های خلوت دودویی

علی زاغیان[۱*]، سید محسن موسوی[۲]

۱- دانشیار، ۲- دانشجوی دکتری، دانشگاه صنعتی مالک اشتر اصفهان

(دریافت: ۹۷/۰۷/۰۹، پذیرش: ۹۷/۱۰/۱۵)

چکیده

ماتریس‌های MDS یکی از مهم‌ترین اجزای طراحی در رمزهای قالبی است. یکی از ویژگی‌های اصلی یک ماتریس MDS برای ساختارهای SPN، سرعت قابل‌قبول پیاده‌سازی ماتریس MDS و معکوس آن، ازنظر سخت‌افزاری است. در این مقاله، نوعی جدید از ماتریس‌های بلوکی دودویی بنام ماتریس‌های شبه خودمعکوس استفاده شده است که هزینه پیاده‌سازی این ماتریس‌ها و معکوس آن‌ها برابر است. در ابتدا، با به‌کارگیری توابع خطی دودویی در ماتریس‌های خلوت دودویی، یک ماتریس MDS ۴×۴ شبه خودمعکوس پیشنهاد شده است که هزینه پیاده‌سازی این ماتریس پیشنهادی برای ورودی ۸ بیتی، برابر با ۶۸ XOR یک بیتی است. ماتریس ۴×۴ پیشنهادی و معکوس آن، پیاده‌سازی مناسبی از نظر سخت‌افزاری دارند زیرا ساختار این ماتریس‌ها، بر اساس ساختارهای DSI است. در ادامه، با استفاده از ساختارهای DSI، یک ماتریس MDS ۸×۸ شبه خودمعکوس پیشنهاد شده که برای ورودی ۸ بیتی، با ۳۲۰ XOR یک بیتی پیاده‌سازی شده است. مهم‌ترین نتیجه این مقاله، پیشنهاد ماتریس MDS ۸×۸ شبه خودمعکوس با هزینه ۳۲۰ XOR است زیرا بهترین نتیجه برای ساخت ماتریس MDS ۸×۸ با استفاده از الگوریتم‌های ذاتی و برای ورودی ۸ بیتی ۳۹۲ XOR است. همچنین، با استفاده از ماتریس‌های مناسب دودویی خلوت، ماتریس MDS ۴×۴ پیشنهاد شده با هزینه $8m+4$ XOR برای ورودی $m \geq 4$ بیتی پیاده‌سازی شده است.

کلیدواژه‌ها: ماتریس MDS، رمزنگاری سبک، لایه‌های انتشار بازگشتی، شمارش XOR، رمز قالبی

Design and Construction of Lightweight MDS Semi Involutory Matrices Based on the Recursive Structures and Binary Sparse Matrices

A. Zaghian[*], M. Mousavi
Malek Ashtar University of Technology, Isfahan
(Received: 01/10/2018; Accepted: 05/01/2019)

Abstract

MDS matrices are one of the most important components in designing block ciphers. Based on the hardware terminologies, the acceptable speed of the implementation of MDS matrix and its inverse is one of the main features of MDS matrix for SPN structures. In this paper, a new type of binary block matrices called semi involutory is used such that the cost of implementation of these matrices and their inverses are equal. At first, by using binary linear functions over binary sparse matrices, a 4×4 semi involutory MDS matrix is proposed so that the cost of implementation of the proposed matrix is 68 bitwise XOR for 8 bit input. The structure of proposed 4×4 MDS matrix and its inverse are based on the DSI structures, so they have suitable implementation from hardware point of view. Next, a 8×8 semi involutory MDS matrix is proposed by applying DSI structures such that the proposed 8×8 matrix is implemented with the 320 bitwise XOR for 8 bit input. The proposed 8×8 semi involutory MDS matrix is the major result, since the best known result in the implementation of a 8×8 semi involutory MDS matrix for 8 bit input, based on the heuristic algorithm, is 392 bitwise XOR while 320 bitwise XOR was obtained in this research. Moreover, the proposed 4×4 MDS matrix is implemented with $8m+4$ XOR for $m\geq4$ bit input by applying suitable binary sparse matrices.

Keywords: MDS Matrix, Lightweight Cryptography, Recursive Diffusion Layers, XOR Count, Block Ciphers

[*]Corresponding Author E-mail: a_zaghian@mut-es.ac.ir

۱. مقدمه

دو مشخصه مهم در طراحی سامانه‌های رمزنگاری مانند رمزهای قالبی و توابع چکیده‌ساز عبارت است از ویژگی‌های پخش[1] و انتشار[2]. در بیشتر سامانه‌های رمزنگاری متقارن از جدول‌های جانشینی به‌عنوان مشخصه پخش و ماتریس‌های MDS[3] به‌عنوان مشخصه انتشار، استفاده می‌شود. یک ماتریس $n\times n$ مانند $\mathbf{A}$ را بر روی میدان $\mathbb{F}$ یک ماتریس MDS گویند اگر و فقط اگر تمام زیر ماتریس‌های مربعی $\mathbf{A}$ معکوس‌پذیر باشند [۱]. ماتریس‌های MDS نه‌فقط نقش مهمی در طراحی لایه انتشار سامانه‌های رمزنگاری برای ایجاد بیشترین انتشار را دارند، بلکه در جلوگیری از تحلیل رمزهای خطی و تفاضلی نیز مؤثر هستند [۲].

تعریف دیگری از ماتریس MDS که معادل با تعریف اول است به‌صورت زیر بیان می‌شود. به ازای هر بردار n تایی غیرصفر مانند $\mathbf{x}$، با m_1 درایه غیرصفر، اگر تعداد درایه‌های غیرصفر بردار $\mathbf{Ax}$ برابر m_2 باشد آن‌گاه $m_1+m_2\geq n+1$. به عدد $n+1$، عدد انشعاب[4] ماتریس $\mathbf{A}$ گویند [۲]. ماتریس MDS را به‌جز میدان می‌توان بر روی حلقه‌ها با ویژگی جابه‌جایی به‌صورت زیر تعریف نمود. عدد انشعاب ماتریس $n\times n$ $\mathbf{A}$ بر روی حلقه جابه‌جایی $\mathbf{R}$ برابر $n+1$ است اگر دترمینان تمام زیر ماتریس‌های مربعی $\mathbf{A}$ بر روی $\mathbf{R}$ معکوس‌پذیر باشند [۳]. در گزاره ۱ مقاله [۴] ثابت شده است که اگر درایه‌های $\mathbf{A}$، ماتریس‌های دودویی $m\times m$ باشند آن‌گاه $\mathbf{A}$ بر روی $\mathbf{R}$ یک ماتریس MDS است اگر و فقط اگر دترمینان تمام زیر ماتریس‌های $\mathbf{A}$، ماتریس‌های معکوس‌پذیر در میدان $\mathbb{F}_2$ باشند.

ماتریس‌های MDS نه‌فقط در رمزنگاری بلکه در ابتدا برای ساخت کدهای MDS استفاده شده‌اند [۵]. درواقع، اگر $\mathbf{A}$ یک ماتریس $n\times n$ MDS بر روی یک میدان $\mathbb{F}$ باشد و $\mathbf{I}_n$ ماتریس همانی از مرتبه n باشد آنگاه ماتریس $n\times 2n$ به فرم $[\mathbf{I}_n|\mathbf{A}]$ یک مولد کد MDS است [۶]. همچنین، ماتریس‌های MDS چندگانه[5] را می‌توان در افزایش جعبه‌های جانشینی فعال[6] در ساختارهای فیستل[7] با تابع دور جایگشتی جانشینی[8]، به کاربرد [۷-۸]. به‌جز روش جستجوی کامل [۹]، می‌توان با استفاده از ماتریس واندرموند [۱۰] و ماتریس کوشی [۱۱]، شکل‌های مختلفی از ماتریس MDS را به‌دست آورد.

اگرچه که ماتریس‌های MDS به شکل‌های مختلفی ساخته شده‌اند اما سه دسته از ماتریس‌های MDS اهمیت و کاربرد بیشتری در رمزنگاری دارند. دسته اول شامل ماتریس‌های MDS ای هستند که از طریق بازگشتی[9] ساخته شده‌اند [۱۵-۱۲]. این دسته، مناسب پیاده‌سازی برای سخت‌افزار است مانند ماتریس استفاده‌شده در تابع چکیده‌ساز PHOTON [۱۶]. دسته دوم از ماتریس‌های MDS به شکل ماتریس هادامارد است که در توابع چکیده‌سازی مانند Khazad [۱۷] و Maelstrom [۱۸] مورد استفاده قرار گرفته‌اند. دسته سوم از ماتریس‌های MDS به شکل ماتریس چرخشی هستند که در رمزهای قالبی مانند AES [۱۹] و تابع چکیده‌ساز *Grostl* [۲۰] به‌کار برده شده‌اند.

یکی از دلایل مهم استفاده از دسته‌های بازگشتی در ساخت ماتریس MDS، پیاده‌سازی سخت‌افزاری ساده و یکسان این دسته از ماتریس‌ها در رمزنگاری و رمزگشایی است. برای ساخت ماتریس‌های بازگشتی دو روش معروف وجود دارد. در روش اول با استفاده از توان nام یک ماتریس $n\times n$ LFSR[10]، به‌شرط غیرصفر بودن درایه‌های سطر آخر آن، یک ماتریس MDS بازگشتی به‌دست می‌آید [۱۶]. محدودیت روش اول در غیرصفر بودن سطر آخر ماتریس LFSR است که هزینه پیاده‌سازی آن را افزایش می‌دهد. روش دوم در ساخت ماتریس بازگشتی، بر اساس ساختارهای فیستلی مانند ساختار GFS[11] [۲۱] یا DSI[12] است [۲۲] که به ما اجازه می‌دهد از ماتریس‌های خلوت‌تری نسبت به ماتریس LFSR، برای ساخت ماتریس MDS، استفاده نماییم. برای مثال، فرض کنید که میدان $\mathbb{F}_{2^4}$ با استفاده از چندجمله‌ای اولیه $\mathbf{f}=x^4+x^3+1$ ساخته شده است. همچنین، فرض نمایید که α یک ریشه از $\mathbf{f}$ است. حال دو ماتریس ۴×۴ زیر را بر روی میدان $\mathbb{F}_{2^4}$ در نظر بگیرید:

$$\mathbf{A}=\begin{bmatrix}0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 1 & \alpha+1 & 1 & \alpha\end{bmatrix},\quad \mathbf{B}=\begin{bmatrix}1 & 0 & 0 & \alpha\\ 1 & 0 & 0 & 0\\ 0 & 1 & \alpha+1 & 0\\ 0 & 0 & 1 & 0\end{bmatrix}.$$

ماتریس $\mathbf{A}$ از نوع LFSR و ماتریس $\mathbf{B}$ از نوع DSI است. می‌توان بررسی نمود که ماتریس‌های $\mathbf{A}^4$ و $\mathbf{B}^4$ بر روی میدان $\mathbb{F}_{2^4}$، ماتریس MDS هستند. اگرچه که تمام عناصر ماتریس‌های $\mathbf{A}$ و $\mathbf{B}$ یکی هستند، اما برای محاسبه $\mathbf{A}\cdot\mathbf{x}^T$، $\mathbf{x}=[x_1,x_2,x_3,x_4]$، به سه XOR (چهارعنصر غیرصفر سطر آخر) و برای محاسبه $\mathbf{B}\cdot\mathbf{x}^T$ تنها به دو XOR (یکی در سطر اول و دیگری در سطر سوم) نیاز است. درواقع داریم:

[1] Confusion
[2] Diffusion
[3] Maximum Distance Spreadable
[4] Branch Number
[5] Multiple MDS Matrices
[6] Active S-Boxes
[7] Feistel Structures
[8] Substitution Permutation Round Function
[9] Recursive
[10] Linear Feedback Shift Register
[11] Generalized Feistel Structure
[12] Diagonal-Serial Invertible

$$\mathbf{A}\cdot\mathbf{x}^T = [x_2, x_3, x_4, x_1+(\alpha+1)x_2+x_3+\alpha x_4]^T,$$
$$\mathbf{B}\cdot\mathbf{x}^T = [x_1+\alpha x_4, x_1, x_2+(\alpha+1)x_3, x_3]^T.$$

بنابراین، نتیجه می‌گیریم که ماتریس $\mathbf{B}$ با ۴ XOR (یک بیتی) کمتر از ماتریس $\mathbf{A}$ می‌تواند پیاده‌سازی شود زیرا میدان $\mathbb{F}_{2^4}$ از عناصر ۴ بیتی تشکیل شده است. همچنین، می‌توان نتیجه گرفت که ماتریس MDS $\mathbf{B}^4$، با ۱۶ XOR کمتر از ماتریس MDS $\mathbf{A}^4$ می‌تواند ازنظر سخت‌افزاری پیاده‌سازی شود.

دیگر محدودیت در ساخت ماتریس MDS با استفاده از ساختار DSI این است که اگر $\mathbf{A}$ یک ماتریس $n\times n$ از نوع DSI باشد آن‌گاه در قضیه ۲ مقاله [۲۲] ثابت شده است که اگر ماتریس $\mathbf{A}^k$ بخواهد MDS باشد آنگاه $k \geq n$. به‌تازگی در مقاله [۲۳] پیشنهاد شده است که برای ساخت یک ماتریس MDS $n\times n$ از ماتریس‌های متمایز بازگشتی استفاده شود. این راه‌کار پیشنهادی باعث می‌شود که هزینه پیاده‌سازی ماتریس MDS به‌طور قابل‌ملاحظه‌ای نسبت به پیاده‌سازی‌های موجود کم شود. به‌عنوان نمونه در قسمت ۴ این مقاله، با استفاده از چهار ماتریس متمایز DSI ۸×۸، یک ماتریس MDS ۸×۸ پیشنهاد شده است که هزینه پیاده‌سازی آن برای ورودی ۸ بیتی برابر ۳۲۰ XOR یک بیتی است و این در حالی است که بهترین نتیجه شناخته شده ۳۹۲ XOR یک بیتی است [۲۴] که با استفاده از جستجو از طریق الگوریتم‌های ذاتی[1] شناخته شده به‌دست آمده است.

یکی از ویژگی‌های مهم و کاربردی یک ماتریس MDS، ساختار معکوس آن است. اگر معکوس یک ماتریس برابر با خود ماتریس باشد به آن خودمعکوس[2] گویند اما اگر هزینه پیاده‌سازی یک ماتریس برابر با هزینه پیاده‌سازی معکوس آن باشد به آن شبه خودمعکوس[3] گوییم. یکی از دلایل مهم استفاده از ماتریس‌های خودمعکوس و یا شبه خودمعکوس در رمزهای قالبی یکسان‌سازی سرعت عملیات رمزنگاری و رمزگشایی است.

در قسمت ۴ این مقاله نشان می‌دهیم که ماتریس MDS ۸×۸ پیشنهادی یک ماتریس شبه خودمعکوس است؛ به عبارت دیگر، هزینه پیاده‌سازی معکوس ماتریس MDS پیشنهادی ۳۲۰ XOR یک بیتی برای ورودی ۸ بیتی است. همچنین ماتریس MDS ۴×۴ پیشنهادی نیز یک ماتریس شبه خودمعکوس برای هر ورودی m بیتی برای $m \geq 4$ است.

[1] Heuristic Algorithm
[2] Involutory
[3] Semi Involutory

۱-۱. پیش‌نیازها

تعاریف و نمادهای مورد استفاده در این مقاله به شرح زیر است. میدان متناهی با q عضو را با $\mathbb{F}_q$ نمایش می‌دهیم. حلقه چندجمله‌ای‌ها با متغیر $\mathbf{L}$ بر پیمانه ۲ با نماد $\mathbb{F}_2[\mathbf{L}]$ نمایش داده می‌شود. ترانهاده و معکوس ماتریس $\mathbf{A}$ به‌ترتیب با نمادهای $\mathbf{A}^T$ و $\mathbf{A}^{-1}$، نمایش داده شده است. ماتریس‌های $m\times m$ صفر و همانی را به‌ترتیب با نمادهای $\mathbf{0}_m$ و $\mathbf{I}_m$ نشان می‌دهیم. ماتریس $\mathbf{A}$ $n\times n$ را بر روی میدان $\mathbb{F}_q$ خود معکوس گوییم اگر و فقط اگر داشته باشیم $\mathbf{A}^2=\mathbf{I}_n$ [۱۱].

در سرتاسر این مقاله منظور ما از نمادهای $\mathbf{L}_{(i,m)}$ برای $1\leq i\leq n$، ماتریس‌های دودویی $m\times m$ معکوس‌پذیر بر روی میدان $\mathbb{F}_2$ است. به ماتریس‌های $\mathbf{L}_{(i,m)}$، توابع خطی دودویی نیز گفته می‌شود [۱۲]. همچنین اگر داشته باشیم $\mathbf{A}=\mathbf{L}_m$، $\mathbf{B}=\mathbf{L}_m^{-1}$ و $\mathbf{C}=\mathbf{L}_m^2$ آن‌گاه ماتریس‌های $\mathbf{B}$ و $\mathbf{C}$ به‌ترتیب، معکوس و توان دوم ماتریس دودویی $\mathbf{A}$ هستند.

در ادامه تعریف ماتریس مربعی DSI بلوکی m بیتی آورده می‌شود. درواقع، تعریف ۱، یک ویرایش از تعریف ۵ در مقاله [۲۲] است که بر روی میدان متناهی، ماتریس DSI تعریف شده است.

تعریف ۱. ماتریس DSI $2n\times 2n$ بلوکی m بیتی با نماد $\mathbf{D}_{n,m}$ نمایش داده شده و به‌صورت زیر تعریف می‌شود:

$$\mathbf{D}_{n,m}=\begin{pmatrix}
\mathbf{L}_{(1,m)} & \mathbf{0}_m & \mathbf{0}_m & \cdots & \cdots & \mathbf{0}_m & \mathbf{0}_m & \mathbf{L}_{(n+1,m)}\\
\mathbf{L}_{(n+2,m)} & \mathbf{0}_m & \mathbf{0}_m & \ddots & \cdots & \cdots & \mathbf{0}_m & \mathbf{0}_m\\
\mathbf{0}_m & \mathbf{L}_{(n+3,m)} & \mathbf{L}_{(2,m)} & \mathbf{0}_m & \ddots & \cdots & \cdots & \mathbf{0}_m\\
\mathbf{0}_m & \mathbf{0}_m & \mathbf{L}_{(n+4,m)} & \mathbf{0}_m & \mathbf{0}_m & \ddots & \cdots & \mathbf{0}_m\\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots\\
\mathbf{0}_m & \vdots & \cdots & \mathbf{0}_m & \mathbf{L}_{(2n-2,m)} & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m\\
\mathbf{0}_m & \vdots & \cdots & \cdots & \mathbf{0}_m & \mathbf{L}_{(2n-1,m)} & \mathbf{L}_{(n,m)} & \mathbf{0}_m\\
\mathbf{0}_m & \mathbf{0}_m & \cdots & \cdots & \cdots & \mathbf{0}_m & \mathbf{L}_{(2n,m)} & \mathbf{0}_m
\end{pmatrix}$$

که $\mathbf{L}_{(i,m)}$ برای $1\leq i\leq 3n$ ماتریس‌های $m\times m$ دودویی معکوس‌پذیر بر روی میدان $\mathbb{F}_2$ هستند.

فرض نمایید هزینه پیاده‌سازی ماتریس $\mathbf{L}_{(i,m)}$ را با $\#\mathbf{L}_{(i,m)}$ نشان دهیم. آن‌گاه بر اساس جدول (۱) مقاله [۲۲] هزینه پیاده‌سازی $\mathbf{D}_{n,m}$، نشان داده شده با $\#\mathbf{D}_{n,m}$، به‌صورت زیر است:

$$\#\mathbf{D}_{n,m}=\sum_{i=1}^{3n}\#\mathbf{L}_{(i,m)}+n\times m \qquad (1)$$

در رابطه (۱) علت در نظر گرفتن عامل $n\times m$ به این دلیل است که در n سطر از ماتریس $\mathbf{D}_{n,m}$ دو ماتریس دودویی m بیتی با یکدیگر XOR می‌شوند. همچنین، لازم به‌ذکر است که اگر در یک سطر از ماتریس $\mathbf{D}_{n,m}$ دو ماتریس یکسان داشته باشیم

آن‌گاه در شمارش هزینه پیاده‌سازی ماتریس $\mathbf{D}_{n,m}$ در رابطه (۱)، فقط هزینه یکی از آن دو ماتریس در نظر گرفته می‌شود.

مثال ۱. ماتریس DSI ۴×۴ بلوکی ۸ بیتی زیر را در نظر بگیرید. با توجه به رابطه (۱) هزینه پیاده‌سازی آن عبارت است از:

$$\mathbf{D}_{۲,۸}=\begin{bmatrix}\mathbf{L}_۸ & \mathbf{0}_۸ & \mathbf{0}_۸ & \mathbf{L}_۸\\ \mathbf{I}_۸ & \mathbf{0}_۸ & \mathbf{0}_۸ & \mathbf{0}_۸\\ \mathbf{0}_۸ & \mathbf{I}_۸ & \mathbf{L}_۸^۲ & \mathbf{0}_۸\\ \mathbf{0}_۸ & \mathbf{0}_۸ & \mathbf{L}_۸^{-۱} & \mathbf{0}_۸\end{bmatrix},\quad \#\mathbf{D}_{۲,۸}=\#\mathbf{L}_۸+\#\mathbf{L}_۸^۲+\#\mathbf{L}_۸^{-۱}+۲\times 8$$

برای سادگی در نمایش ماتریس‌های دودویی، آن‌ها را با یک لیست نمایش می‌دهیم به‌طوری‌که هر درایه از این لیست شامل موقعیت‌های عناصر غیرصفر در هر سطر است. برای مثال داریم:

$$\mathbf{L}_۴=\begin{bmatrix}۱ & ۰ & ۰ & ۱\\ ۱ & ۰ & ۰ & ۰\\ ۰ & ۱ & ۱ & ۰\\ ۰ & ۰ & ۱ & ۰\end{bmatrix}=[[۱,۴],[۱],[۲,۳],[۳]] \qquad (۲)$$

حال فرض کنید $\mathbf{x}=[x_۱,x_۲,x_۳,x_۴]$ که x_i برای $۱\le i\le ۴$، یک بیتی هستند. آنگاه داریم:

$$\mathbf{L}_۴\cdot\mathbf{x}^T=[x_۱+x_۴,x_۱,x_۲+x_۳,x_۲]^T \qquad (۳)$$

تفسیر رابطه (۳) به زبان پیاده‌سازی در سخت‌افزار، به این معنی است که هزینه پیاده‌سازی[1] ماتریس $\mathbf{L}_۴$ در رابطه (۲) دو XOR یک بیتی است. همچنین به دلیل ساده‌نویسی، منظور از XOR در ادامه مقاله، XOR یک بیتی است.

ادامه ساختار مقاله به‌صورت زیر آورده شده است. در بخش دوم، ماتریس شبه خودمعکوس، ازنظر پیاده‌سازی بر اساس تعداد XOR، تعریف شده است. در بخش سوم با استفاده از دو ماتریس متمایز ۴×۴ DSI بلوکی ۸ بیتی یک ماتریس ۴×۴ MDS شبه خودمعکوس با هزینه ۶۸ XOR، برای ورودی ۸ بیتی، پیشنهاد شده است. همچنین، ماتریس ۴×۴ DSI پیشنهادی برای هر ورودی $m\ge ۴$ بیتی، با هزینه $۸m+۴$ پیاده‌سازی شده است. در پایان بخش ۳ به این نکته اشاره شده است که ماتریس پیشنهادی در این بخش چه برتری نسبت به ماتریس ۴×۴ MDS داده شده در مقاله [۲۳] دارد. در بخش چهارم با به‌کارگیری چهار ماتریس متمایز ۸×۸ DSI بلوکی ۸ بیتی، یک ماتریس ۸×۸ MDS شبه خودمعکوس پیشنهاد شده است به‌طوری‌که هزینه پیاده‌سازی ماتریس پیشنهاد شده برای ورودی ۸ بیتی برابر با ۳۲۰ XOR است که مهم‌ترین نتیجه این مقاله نیز است. همچنین در بخش چهارم، ماتریس ۸×۸ MDS پیشنهادی با هزینه ۳۴۴ XOR بر روی میدان متناهی $\mathbb{F}_{۲^۸}$ نیز پیاده‌سازی شده است. در پایان، خلاصه نتایج مقاله در بخش پنجم آورده شده است.

۲. معرفی ماتریس‌های $\mathbf{D}_{n,m}$ شبه خودمعکوس

در این بخش می‌خواهیم ماتریس‌های شبه خودمعکوس را تعریف نماییم. در بخش‌های سوم و چهارم، ماتریس‌های ۴×۴ و ۸×۸ MDS شبه خودمعکوسی پیشنهاد شده است که هزینه پیاده‌سازی این ماتریس‌ها برای ورودی‌های ۸ بیتی، به‌ترتیب ۶۸ و ۳۲۰ XOR است.

مفهوم شبه خودمعکوسی رابطه مستقیمی با نحوه پیاده‌سازی دارد. برای نمونه اگر روش پیاده‌سازی گفته‌شده در مقاله [۲۵] را ملاک قرار دهیم تمام ماتریس‌ها هزینه پیاده‌سازی خودشان و وارونشان برابر است.

تعریف ۲. ماتریس مربعی $\mathbf{A}$ را شبه خودمعکوس توسط روش پیاده‌سازی P گویند هرگاه هزینه پیاده‌سازی ماتریس $\mathbf{A}$ و معکوس آن از طریق روش P یکسان باشد.

با توجه به تعریف ۲، آن دسته از ماتریس‌های DSI $۲n\times ۲n$ بلوکی m بیتی را در نظر می‌گیریم که تعداد XOR های لازم برای پیاده‌سازی سخت‌افزاری این ماتریس‌ها و معکوس آن‌ها یکسان باشد.

مثال ۲. ماتریس $\mathbf{D}_{۲,m}^{(۱)}$ و معکوس آن را که در رابطه (۴) داده شده است در نظر بگیرید:

$$\mathbf{D}_{۲,m}^{(۱)}=\begin{bmatrix}\mathbf{L}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{I}_m\\ \mathbf{I}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{I}_m & \mathbf{L}_m^۲ & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{I}_m & \mathbf{0}_m\end{bmatrix},\quad \left(\mathbf{D}_{۲,m}^{(۱)}\right)^{-۱}=\begin{bmatrix}\mathbf{0}_m & \mathbf{I}_m & \mathbf{0}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{I}_m & \mathbf{L}_m^۲\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{I}_m\\ \mathbf{I}_m & \mathbf{L}_m & \mathbf{0}_m & \mathbf{0}_m\end{bmatrix}. \qquad (۴)$$

حال فرض کنید که $\mathbf{x}=[x_۱,x_۲,x_۳,x_۴]$ یک بردار ۴ تایی است که هر عنصر آن m بیتی است؛ بنابراین داریم:

$$\begin{aligned}\mathbf{D}_{۲,m}^{(۱)}\cdot\mathbf{x}^T &= [\mathbf{L}_m x_۱+x_۴,\ \ x_۱,\ \ x_۲+\mathbf{L}_m^۲ x_۳,\ \ x_۳]^T\\ \left(\mathbf{D}_{۲,m}^{(۱)}\right)^{-۱}\cdot\mathbf{x}^T &= [x_۲,\ \ x_۳+\mathbf{L}_m^۲ x_۴,\ \ x_۴,\ \ x_۱+\mathbf{L}_m x_۲]^T\end{aligned} \qquad (۵)$$

رابطه (۵) نتیجه می‌دهد که ماتریس $\mathbf{D}_{۲,m}^{(۱)}$ شبه خودمعکوس است زیرا اگر $\#\mathbf{L}_m$ هزینه پیاده‌سازی $\mathbf{L}_m$ باشد آنگاه با استفاده از رابطه (۵) هزینه پیاده‌سازی ماتریس $\mathbf{D}_{۲,m}^{(۱)}$ و معکوس آن برابر با $۲m+\#\mathbf{L}_m+\#\mathbf{L}_m^۲$ است. حال دو ماتریس زیر را در نظر بگیرید:

$$\mathbf{D}_{۲,m}^{(۲)}=\begin{bmatrix}\mathbf{L}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{L}_m^{-۱}\\ \mathbf{I}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{L}_m^{-۱} & \mathbf{L}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{I}_m & \mathbf{0}_m\end{bmatrix},\left(\mathbf{D}_{۲,m}^{(۲)}\right)^{-۱}=\begin{bmatrix}\mathbf{0}_m & \mathbf{I}_m & \mathbf{0}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{L}_m & \mathbf{L}_m^۲\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{I}_m\\ \mathbf{L}_m & \mathbf{L}_m^۲ & \mathbf{0}_m & \mathbf{0}_m\end{bmatrix}. \qquad (۶)$$

[1] The Cost of Implementation

آن‌گاه داریم:

$$\begin{aligned}\mathbf{D}_{۲,m}^{(۲)}\cdot\mathbf{x}^T &= [\mathbf{L}_m x_۱+\mathbf{L}_m^{-۱}x_۴,\ x_۱,\ \mathbf{L}_m^{-۱}x_۲+\mathbf{L}_m x_۳,\ x_۲]^T\\ \left(\mathbf{D}_{۲,m}^{(۲)}\right)^{-۱}\cdot\mathbf{x}^T &= [x_۲,\ \mathbf{L}_m(x_۲+\mathbf{L}_m x_۴),\ x_۴,\ \mathbf{L}_m(x_۱+\mathbf{L}_m x_۲)]^T\end{aligned}\qquad (۷)$$

اگرچه که بر اساس رابطه (۷) هزینه پیاده‌سازی ماتریس $\mathbf{D}_{۲,m}^{(۲)}$ و معکوس آن یکی نیست اما اگر هزینه پیاده‌سازی $\mathbf{L}_m$ و $\mathbf{L}_m^{-۱}$ یکسان باشد آنگاه ماتریس $\mathbf{D}_{۲,m}^{(۲)}$ نیز شبه خودمعکوس است.

یک روش برای ساخت ماتریس MDS استفاده از توابع خطی دودویی به‌جای عناصر میدان است. ایده این روش بر اساس این نکته است که عناصر غیرصفر میدان متناهی با مشخصه ۲ را می‌توان با ماتریس‌های دودویی معکوس‌پذیر در میدان $\mathbb{F}_۲$ نمایش داد. به‌عبارت‌دیگر فرض نمایید α ریشه چندجمله‌ای اولیه‌ای از درجه m باشد که میدان با استفاده از آن چندجمله‌ای ساخته شده است. حال اگر $\mathbf{L}_m$ نمایش ماتریس دودویی مربوط به α باشد آن‌گاه نمایش ماتریسی سایر عناصر غیر صفر میدان در $\mathbb{F}_۲$، توانی از ماتریس $\mathbf{L}_m$ است.

در پایان این بخش یک الگوریتم تصادفی برای ساخت ماتریس MDS $۲n\times۲n$ سبک‌وزن برای ورودی m بیتی ارائه می‌دهیم.

مرحله ۱: انتخاب ماتریس‌های شبه خودمعکوس $\mathbf{D}_{n,m}^{(i)}$ برای $۱\le i\le ۲n$ به‌طوری که ماتریس‌های انتخابی در دو شرط زیر صدق کنند: اول این‌که حاصل‌ضرب این ماتریس‌ها که با نماد $\mathbf{H}_n$ نشان می‌دهیم، بر روی حلقه $\mathbb{F}_۲[\mathbf{L}]$ یک ماتریس MDS باشد. شرط دوم این است که در ساخت ماتریس‌های $\mathbf{D}_{n,m}^{(i)}$ حداقل تعداد توابع خطی دودویی استفاده شود.

نکته مهم در مرحله اول این است که با توجه به گزاره ۱ مقاله [۴] کافی است که دترمینان تمام زیر ماتریس‌های $\mathbf{H}_n$ بر روی $\mathbb{F}_۲[\mathbf{L}]$ غیرصفر شود زیرا در مرحله سوم قصد داریم به‌جای توابع دودویی خطی، ماتریس‌های $m\times m$ معکوس‌پذیر قرار دهیم.

مرحله ۲: تمام مؤلفه‌های تحویل‌ناپذیر مربوط به دترمینان زیر ماتریس‌های $\mathbf{H}_n$ را در میدان $\mathbb{F}_۲$ به‌دست می‌آوریم.

مرحله ۳: ماتریس‌های $m\times m$ معکوس‌پذیر مانند $\mathbf{L}_m$ را در میدان $\mathbb{F}_۲$ جستجو می‌کنیم که ویژگی زیر را داشته باشند: تمام مؤلفه‌های تحویل‌ناپذیر به‌دست‌آمده در مرحله ۲، به‌ازای $\mathbf{L}_m$ ماتریس‌های معکوس‌پذیر بر روی میدان $\mathbb{F}_۲$ شوند. توجه شود که برای شروع مرحله ۳، ماتریس $\mathbf{L}_m$ باید حداقل هزینه پیاده‌سازی را داشته باشد و در صورت نداشتن ویژگی ذکر شده، هزینه پیاده‌سازی ماتریس $\mathbf{L}_m$ را افزایش می‌دهیم.

۳. پیاده‌سازی ماتریس MDS ۴×۴ شبه خودمعکوس با هزینه $۸m+۴$ XOR برای ورودی $m\ge ۴$ بیتی

دو ماتریس DSI ۴×۴ شبه خودمعکوس بلوکی زیر را بر روی ورودی m بیتی در نظر بگیرید:

$$\mathbf{D}_{۲,m}^{(۱)}=\begin{bmatrix}\mathbf{I}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{I}_m\\ \mathbf{I}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{I}_m & \mathbf{I}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{I}_m & \mathbf{0}_m\end{bmatrix},\quad \mathbf{D}_{۲,m}^{(۲)}=\begin{bmatrix}\mathbf{L}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{L}_m^{-۱}\\ \mathbf{I}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{L}_m^{-۱} & \mathbf{L}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{I}_m & \mathbf{0}_m\end{bmatrix}.$$

ماتریس $\mathbf{H}_۴=\mathbf{D}_{۲,m}^{(۱)}\times\mathbf{D}_{۲,m}^{(۲)}\times\left(\mathbf{D}_{۲,m}^{(۱)}\right)^۲$ در میدان $\mathbb{F}_۲$ به شکل زیر است:

$$\mathbf{H}_۴=\begin{bmatrix}\mathbf{L}_m+\mathbf{I}_m & \mathbf{L}_m^{-۱}+\mathbf{I}_m & \mathbf{L}_m+\mathbf{L}_m^{-۱}+\mathbf{I}_m & \mathbf{L}_m\\ \mathbf{L}_m & \mathbf{L}_m^{-۱} & \mathbf{L}_m+\mathbf{L}_m^{-۱} & \mathbf{L}_m\\ \mathbf{L}_m+\mathbf{L}_m^{-۱}+\mathbf{I}_m & \mathbf{L}_m & \mathbf{L}_m+\mathbf{I}_m & \mathbf{L}_m^{-۱}+\mathbf{I}_m\\ \mathbf{L}_m+\mathbf{L}_m^{-۱} & \mathbf{L}_m & \mathbf{L}_m & \mathbf{L}_m^{-۱}\end{bmatrix}\qquad (۸)$$

می‌توان بررسی نمود که تعداد زیر ماتریس‌های مربعی یک ماتریس $n\times n$ برابر است با $\sum_{i=۱}^{n}\binom{n}{i}\binom{n}{i}=\binom{۲n}{n}-۱$؛ بنابراین، تعداد زیر ماتریس‌های مربعی ماتریس $\mathbf{H}_۴$ برابر با $\binom{۸}{۴}-۱=۶۹$ ماتریس است. همچنین، می‌توان بررسی نمود که دترمینان این ۶۹ ماتریس بر روی $\mathbb{F}_۲[\mathbf{L}]$ غیرصفر است. حال اگر دترمینان این ۶۹ ماتریس را به‌عنوان چندجمله‌ای بر روی $\mathbb{F}_۲[\mathbf{L}]$ در نظر گرفته شود آن‌گاه عامل‌های تحویل‌ناپذیر متمایز این ۶۹ چندجمله‌ای، شرط‌های داده شده در رابطه (۹) است.

$$\begin{aligned}&\{\mathbf{L}_m,\ \mathbf{L}_m+\mathbf{I}_m,\ \mathbf{L}_m^۲+\mathbf{L}_m+\mathbf{I}_m,\\ &\mathbf{L}_m^۳+\mathbf{L}_m+\mathbf{I}_m,\ \mathbf{L}_m^۳+\mathbf{L}_m^۲+\mathbf{I}_m,\ \mathbf{L}_m^۴+\mathbf{L}_m+\mathbf{I}_m\}\end{aligned}\qquad (۹)$$

در ادامه با استفاده از جستجوی کامپیوتری، ماتریس‌های $m\times m$ دودویی معکوس‌پذیر را جستجو می‌کنیم که در شرایط زیر صدق کنند. در ابتدا بنابر رابطه (۷) در مثال ۲، هزینه پیاده‌سازی ماتریس‌های جستجو شده و معکوس آن‌ها باید یکسان باشد تا اینکه ماتریس $\mathbf{H}_۴$ شبه خودمعکوس شود. همچنین، با جایگذاری ماتریس‌های جستجو شده در رابطه (۹)، تمام شش ماتریس رابطه (۹) در میدان $\mathbb{F}_۲$ معکوس‌پذیر شوند.

فرض کنید تعداد XOR موردنیاز برای پیاده‌سازی ماتریس $\mathbf{L}_m$ و معکوس آن را به‌ترتیب با $\#\mathbf{L}_m$ و $\#\mathbf{L}_m^{-۱}$ نشان دهیم. آنگاه با استفاده از سطر اول رابطه (۷)، تعداد XOR موردنیاز برای پیاده‌سازی ماتریس $\mathbf{D}_{۲,m}^{(۲)}$ عبارت است از $۲m+۲\#\mathbf{L}+۲\#\mathbf{L}^{-۱}$. همچنین، هزینه پیاده‌سازی ماتریس $\mathbf{D}_{۲,m}^{(۱)}$ نیز برابر $۲m$ است. بنابراین، تعداد XOR های موردنیاز برای پیاده‌سازی ماتریس $\mathbf{H}_۴$

و معکوس آن برای ورودی m بیتی، برابر است با $\left(\#\mathbf{L}_m=\#\mathbf{L}_m^{-1}\right)$:

$$\begin{aligned}&2m+(2m+2\#\mathbf{L}_m+2\#\mathbf{L}_m^{-1})+\\&2m+2m=8m+2\#\mathbf{L}_m+2\#\mathbf{L}_m^{-1}\end{aligned} \quad (10)$$

حال ماتریس‌های 4×4 دودویی زیر را در نظر بگیرید. چهار ماتریس دودویی داده شده، در میدان $\mathbb{F}_2$ معکوس‌پذیر هستند.

$$\begin{aligned}&\mathbf{L}_{(1,4)}=[[1,4],[1],[2],[3]],\quad \mathbf{L}_{(2,4)}=[[4],[1,2],[2],[3]],\\&\mathbf{L}_{(3,4)}=[[4],[1],[2,3],[3]],\quad \mathbf{L}_{(4,4)}=[[4],[1],[2],[3,4]].\end{aligned} \quad (11)$$

هزینه پیاده‌سازی چهار ماتریس داده شده در رابطه (۱۱) و معکوس آن‌ها یک XOR است. همچنین، شرط‌های داده شده در رابطه (۹) به‌ازای ماتریس‌های $\mathbf{L}_{(i,4)}$ برای $1\le i\le 4$، ماتریس‌های معکوس‌پذیر در میدان $\mathbb{F}_2$ هستند؛ بنابراین، با به‌کارگیری رابطه (۱۰)، پیاده‌سازی ماتریس‌های $\mathbf{H}_4$ و $\mathbf{H}_4^{-1}$ برای ورودی ۴ بیتی، با استفاده از ماتریس‌های $\mathbf{L}_{(i,4)}$ برای $1\le i\le 4$، برابر با $8\times4+2\times1+2\times1=36$ XOR است.

حال می‌خواهیم ماتریس‌های $\mathbf{H}_4$ و $\mathbf{H}_4^{-1}$ را با ۶۸ XOR برای ورودی‌های ۸ بیتی، پیاده‌سازی نماییم. البته به‌تازگی نتیجه ۶۷ XOR برای پیاده‌سازی ماتریس 4×4 در حالت ورودی ۸ بیتی در مقاله [۲۳] هم گزارش شده است که در پایان این بخش به مزیت ماتریس پیشنهادی در این قسمت نسبت به ماتریس گزارش شده در [۲۳] اشاره می‌شود. همچنین، کمترین تعداد XOR برای پیاده‌سازی ماتریس‌های شبه خودمعکوس 4×4 با استفاده از ساختارهای بازگشتی و برای ورودی‌های ۸ بیتی، ۸۰ XOR است که در مقاله [۲۲] با استفاده از روش زیر میدان پیاده‌سازی شده است.

در ابتدا هفت ماتریس دودویی معکوس‌پذیر بر روی میدان $\mathbb{F}_2$ پیشنهاد می‌دهیم که هزینه پیاده‌سازی ماتریس‌های پیشنهادی و معکوس آن‌ها یک XOR است.

$$\begin{aligned}&\mathbf{L}_{(1,8)}=[[2,8],[1],[2],[3],[4],[5],[6],[7]],\quad \mathbf{L}_{(2,8)}=[[8],[1,3],[2],[3],[4],[5],[6],[7]],\\&\mathbf{L}_{(3,8)}=[[8],[1],[2,4],[3],[4],[5],[6],[7]],\quad \mathbf{L}_{(4,8)}=[[8],[1],[2],[3,5],[4],[5],[6],[7]],\\&\mathbf{L}_{(5,8)}=[[8],[1],[2],[3],[4,6],[5],[6],[7]],\quad \mathbf{L}_{(6,8)}=[[8],[1],[2],[3],[4],[5,7],[6],[7]],\\&\mathbf{L}_{(7,8)}=[[8],[1],[2],[3],[4],[5],[6,8],[7]].\end{aligned} \quad (12)$$

می‌توان بررسی نمود که شرط‌های داده شده در (۹)، به‌ازای ماتریس‌های به‌دست‌آمده در (۱۲)، ماتریس‌های معکوس‌پذیر بر روی میدان $\mathbb{F}_2$ هستند؛ بنابراین، با به‌کارگیری رابطه (۱۰) و استفاده از ماتریس‌های داده شده در (۱۲)، ماتریس‌های $\mathbf{H}_4$ و $\mathbf{H}_4^{-1}$ با $8\times8+2\times1+2\times1=68$ XOR، برای ورودی ۸ بیتی پیاده‌سازی می‌شود.

در ادامه این بخش می‌خواهیم یک ماتریس $2^n\times2^n$ دودویی بنام $\mathbf{R}_n$ با هزینه پیاده‌سازی یک XOR معرفی نماییم به‌طوری‌که هزینه پیاده‌سازی ماتریس $\mathbf{H}_4$ و معکوس آن برابر با $8\times m+4$ XOR برای ورودی $m=2^n$ بیتی است. ماتریس $\mathbf{R}_n$ به‌صورت زیر تعریف می‌شود:

$$\mathbf{R}_n=\left[\left[2^{n-2},2^n\right],[1],[2],[3],\cdots,\left[2^n-1\right]\right] \quad (13)$$

فرض کنید که چندجمله‌ای مشخصه[1] ماتریس $\mathbf{R}_n$ را با $\mathrm{Char}(\mathbf{R}_n)$ نمایش دهیم. آن‌گاه در ضمیمه الف ثابت شده است که $\mathrm{Char}(\mathbf{R}_n)$ در میدان $\mathbb{F}_2$، به فرم داده شده در رابطه (۱۴) است.

$$\mathrm{Char}(\mathbf{R}_n)=\left(x^4+x^3+1\right)^{2^{n-2}} \quad (14)$$

حال می‌خواهیم ثابت کنیم با جایگذاری ماتریس $\mathbf{R}_n$ در شرط‌های (۹) ماتریس‌های معکوس‌پذیر بر روی میدان $\mathbb{F}_2$ به‌دست می‌آید. می‌توان بررسی نمود که عنصر $\mathbf{L}_m^4+\mathbf{L}_m^2+\mathbf{I}_m$ در بین این شرط‌ها وجود ندارد. از طرفی اگر شش شرط به‌دست‌آمده در رابطه (۹) را به‌عنوان چندجمله‌ای در میدان $\mathbb{F}_2$ در نظر بگیرم آن‌گاه می‌توان بررسی نمود که این چندجمله‌ای‌ها بر روی میدان $\mathbb{F}_2$ نیز تحویل‌ناپذیر هستند. فرض کنید این شش چندجمله‌ای تحویل‌ناپذیر را با $\mathbf{h}_k$ برای $1\le k\le 6$، نشان دهیم. رابطه (۱۴) نتیجه می‌دهد که چندجمله‌ای مینیمال $\mathbf{R}_n$ در میدان $\mathbb{F}_2$ برابر با $\mathbf{f}=x^4+x^3+1$ است؛ بنابراین اگر به ازای یک $1\le k\le 6$، در میدان $\mathbb{F}_2$ داشته باشیم $\mathbf{h}_k(\mathbf{R}_n)=\mathbf{0}_{2^n}$ آنگاه چندجمله‌ای $\mathbf{f}$ باید عاملی از $\mathbf{h}_k$ باشد که این تناقض با تحویل‌ناپذیری چندجمله‌ای‌های $\mathbf{h}_k$ است.

فرض کنید که میدان متناهی $\mathbb{F}_{2^4}$ با استفاده از چندجمله‌ای $\mathbf{f}$ ساخته شده است. از مباحث مربوط به میدان متناهی می‌دانیم که ریشه‌های $\mathbf{f}$ در میدان $\mathbb{F}_{2^4}$ قرار دارند. به میدان $\mathbb{F}_{2^4}$ یک میدان گسترش‌یافته از طریق $\mathbf{f}$ نیز می‌گویند. اگر α یک ریشه از $\mathbf{f}$ باشد آن‌گاه چهار ریشه $\mathbf{f}$ در میدان $\mathbb{F}_{2^4}$ برابر با α^{2^i} برای $0\le i\le 3$ است زیرا مشخصه میدان ۲ است. حال فرض کنید یک $1\le k\le 6$ وجود داشته باشد به‌طوری‌که ماتریس $2^n\times2^n$ دودویی $\mathbf{C}_{(k,n)}=\mathbf{h}_k(\mathbf{R}_n)$ بر روی میدان $\mathbb{F}_2$ معکوس‌پذیر نباشد. آنگاه نتیجه می‌گیریم که دترمینان ماتریس $\mathbf{C}_{(k,n)}$ در میدان $\mathbb{F}_2$ صفر است؛ بنابراین، سخت نیست که بررسی شود حداقل یک $0\le i\le 3$ وجود دارد به‌طوری‌که $\mathbf{h}_k\left(\alpha^{2^i}\right)=0$؛ اما این یک تناقض است زیرا دو چندجمله‌ای تحویل‌ناپذیر متمایز نمی‌توانند ریشه

[1] Characteristic Polynomial

مشترک در میدان گسترش‌یافته یکدیگر داشته باشند. درواقع اگر $\mathbf{h}_k$ ریشه مشترکی با $\mathbf{f}$ داشته باشد آن‌گاه $\mathbf{f}$ باید عاملی از $\mathbf{h}_k$ باشد.

فرم ماتریس $\mathbf{R}_n$ در رابطه (۱۳) نتیجه می‌دهد که هزینه پیاده‌سازی $\mathbf{R}_n$ و معکوس آن، یک XOR است؛ بنابراین، با استفاده از رابطه (۱۰) نتیجه می‌گیریم که هزینه پیاده‌سازی $\mathbf{H}_۴$ و معکوس آن با استفاده از ماتریس $\mathbf{R}_n$، برابر با $۸\times m+۴$ XOR برای ورودی $m=۲^n$ بیتی است. برای مثال، ماتریس ۲۵۶×۲۵۶ دودویی معکوس‌پذیر $\mathbf{R}_۸$ را در نظر بگیرید. ماتریس $\mathbf{R}_۸$، درواقع یک ورودی ۲۵۶ بیتی است؛ بنابراین، با استفاده از ماتریس $\mathbf{R}_۸$ می‌توان $\mathbf{H}_۴$ و $\mathbf{H}_۴^{-۱}$ را با هزینه ۲۰۵۲ XOR برای ورودی ۲۵۶ بیتی پیاده‌سازی نمود. یکی از مزیت‌های استفاده از ماتریس $\mathbf{R}_n$ در پیاده‌سازی سخت‌افزاری این است که دیگر نیازی به استفاده مستقیم از مباحث میدان متناهی در پیاده‌سازی ماتریس‌های MDS نیست.

در پایان این بخش به این نکته مهم اشاره می‌شود که در گزارش قبلا منتشر شده [۲۳]، ماتریس MDS ۴×۴ با هزینه ۶۷ XOR پیشنهاد شده است به‌طوری که بنا بر شکل (۸)، ماتریس پیشنهادی از سه ماتریس متمایز DSI و یک ماتریس جایگشتی تشکیل شده است. همچنین بنابر همین شکل (۸)، بیشترین تعداد XOR و توابع دودویی خطی در هر مسیر از ورودی به خروجی عدد ۶ است؛ اما بنابر ضمیمه ب، بیشترین تعداد XOR و توابع دودویی خطی در هر مسیر از ورودی به خروجی برابر عدد ۵ است؛ به عبارت دیگر، تنها مزیت ماتریس پیشنهادی شبه خودمعکوس در این مقاله نسبت به ماتریس پیشنهادی در آن گزارش [۲۳] این است که ما در ساخت ماتریس MDS ۴×۴ تنها از دو ماتریس متمایز DSI استفاده نمودیم.

۳. پیاده‌سازی ماتریس MDS ۸×۸ شبه خودمعکوس با تعداد عملیات ۳۲۰ XOR برای ورودی ۸ بیتی

نتایج داده شده در این بخش، مهم‌ترین نتایج به‌دست‌آمده در این مقاله است. در این بخش، می‌خواهیم با استفاده از چهار ماتریس متمایز $\mathbf{D}_{۴,m}$، یک ماتریس شبه خودمعکوس MDS ۸×۸ پیشنهاد دهیم که هزینه پیاده‌سازی آن برای ورودی ۸ بیتی برابر با ۳۲۰ XOR و هزینه پیاده‌سازی آن بر روی $\mathbb{F}_{۲^۸}$ ۳۴۴ XOR است. فرض کنید k یک عدد صحیح باشد. ماتریس ۸×۸ DSI بلوکی m بیتی زیر را در نظر بگیرید:

$$\mathbf{D}_{۴,m}^{(k)}=\begin{bmatrix}\mathbf{L}_m^k & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{1}_m\\ \mathbf{1}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{1}_m & \mathbf{L}_m^k & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{1}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{1}_m & \mathbf{L}_m^k & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{1}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{1}_m & \mathbf{L}_m^k & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{1}_m & \mathbf{0}_m\end{bmatrix} \quad (۱۵)$$

که در ماتریس رابطه (۱۵)، منظور از عبارت $\mathbf{L}_m^k$، توان kام ماتریس $m\times m$ معکوس‌پذیر $\mathbf{L}_m$ بر روی میدان $\mathbb{F}_۲$ است. می‌توان بررسی نمود که معکوس ماتریس $\mathbf{D}_{۴,m}^{(k)}$ بر روی میدان $\mathbb{F}_۲$ به شکل زیر است:

$$\left(\mathbf{D}_{۴,m}^{(k)}\right)^{-۱}=\begin{bmatrix}\mathbf{0}_m & \mathbf{1}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{1}_m & \mathbf{L}_m^k & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{1}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{1}_m & \mathbf{L}_m^k & \mathbf{0}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{1}_m & \mathbf{0}_m & \mathbf{0}_m\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{1}_m & \mathbf{L}_m^k\\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{1}_m\\ \mathbf{1}_m & \mathbf{L}_m^k & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m & \mathbf{0}_m\end{bmatrix} \quad (۱۶)$$

عناصر ماتریس‌های $\mathbf{D}_{۴,m}^{(k)}$ و $(\mathbf{D}_{۴,m}^{(k)})^{-۱}$، داده شده در (۱۵) و (۱۶)، یکسان هستند بنابراین، هزینه پیاده‌سازی ماتریس‌های $\mathbf{D}_{۴,m}^{(k)}$ و معکوس آن یکسان است؛ که نتیجه می‌دهد ماتریس $\mathbf{D}_{۴,m}^{(k)}$ شبه خودمعکوس می‌باشد. در ابتدا، هزینه پیاده‌سازی ماتریس $\mathbf{D}_{۴,m}^{(k)}$ را به ازای ورودی هشت‌تایی m بیتی، محاسبه می‌شود.

فرض کنید $\mathbf{x}=[x_۱,x_۲,\cdots,x_۷,x_۸]^T$ که مؤلفه‌های $\mathbf{x}$ عناصر m بیتی هستند. آن‌گاه حاصل $\mathbf{D}_{۴,m}^{(k)}\cdot\mathbf{x}^T$ به‌صورت زیر به‌دست می‌آید:

$$\begin{aligned}\mathbf{D}_{۴,m}^{(k)}\cdot\mathbf{x}^T \;=\; &[\mathbf{L}_m^k x_۱+x_۸,\;\; x_۱,\;\; x_۲+\mathbf{L}_m^k x_۳,\\ &x_۳,\;\; x_۴+\mathbf{L}_m^k x_۵,\;\; x_۵,\;\; x_۶+\mathbf{L}_m^k x_۷,\;\; x_۷]^T\end{aligned} \quad (۱۷)$$

حال با استفاده از رابطه (۱۷) نتیجه می‌گیریم که هزینه پیاده‌سازی ماتریس $\mathbf{D}_{۴,m}^{(k)}$ و معکوس آن برای ورودی m بیتی برابر با $۴m+۴\#\mathbf{L}_m^k$ است. برای مثال، فرض کنید هزینه پیاده‌سازی $\mathbf{D}_{۴,m}^{(k)}$ را با نماد $\#\mathbf{D}_{۴,m}^{(k)}$ نمایش دهیم آن‌گاه داریم:

$$\begin{aligned}&\#\mathbf{D}_{۴,m}^{(-۱)}=۴m+۴\#\mathbf{L}_m^{-۱}, \qquad \#\mathbf{D}_{۴,m}^{(۰)}=۴m,\\ &\#\mathbf{D}_{۴,m}^{(۱)}=۴m+۴\#\mathbf{L}_۱, \quad \#\mathbf{D}_{۴,m}^{(۲)}=۴m+۴\#\mathbf{L}_m^۲.\end{aligned} \quad (۱۸)$$

در ادامه می‌خواهیم یک ماتریس MDS ۸×۸ با استفاده از ماتریس‌های داده شده در رابطه (۱۸) پیشنهاد دهیم. ماتریس داده‌شده در رابطه (۱۹) را در نظر بگیرید (ضمیمه د):

$$\mathbf{H}_۸=\mathbf{D}_{۴,m}^{(۰)}\times\mathbf{D}_{۴,m}^{(۱)}\times\mathbf{D}_{۴,m}^{(۲)}\times\mathbf{D}_{۴,m}^{(-۱)}\times\mathbf{D}_{۴,m}^{(-۱)}\times\mathbf{D}_{۴,m}^{(۲)}\times\mathbf{D}_{۴,m}^{(۱)}\times\mathbf{D}_{۴,m}^{(۰)} \quad (۱۹)$$

می‌توان بررسی نمود که ماتریس $\mathbf{H}_۸$ دارای ۱۲۸۶۹ زیر ماتریس مربعی است و دترمینان‌های این ۱۲۸۶۹ ماتریس بر

روی حلقه چندجمله‌ای‌های $\mathbb{F}_۲[\mathbf{L}]$ غیرصفر است. همچنین اگر دترمینان‌های این ۱۲۸۶۹ ماتریس را به‌عنوان چندجمله‌ای بر روی $\mathbb{F}_۲[\mathbf{L}]$ در نظر بگیریم آنگاه عامل‌های تحویل‌ناپذیر متمایز این ۱۲۸۶۹ چندجمله‌ای، شرط‌های داده شده در ضمیمه ج است که تعداد آن ۶۰۴ چندجمله‌ای تحویل‌ناپذیر است. حال با استفاده از رابطه‌های (۱۸) و (۱۹) هزینه پیاده‌سازی ماتریس $\mathbf{H}_۸$، به‌صورت زیر به‌دست می‌آید:

$$\begin{aligned}&(۴m+(۴m+۴\#\mathbf{L}_m)+(۴m+۴\#\mathbf{L}_m^۲)+(۴m+\#\mathbf{L}_m^{-۱}))\times ۲\\&=۳۲m+۸\#\mathbf{L}_m+۸\#\mathbf{L}_m^۲+۸\#\mathbf{L}_m^{-۱}\end{aligned}\qquad(۲۰)$$

در ادامه با استفاده از جستجوی کامپیوتری به دنبال ماتریس‌های $m\times m$ معکوس‌پذیر روی میدان $\mathbb{F}_۲$ هستیم که ویژگی‌های زیر را داشته باشند. در ابتدا، پیاده‌سازی ماتریس‌های جستجو شده و معکوس آن‌ها، یک XOR (حداقل مقدار ممکن) هزینه داشته باشد. همچنین، با جایگذاری ماتریس‌های جستجو شده در ۶۰۴ شرط به‌دست‌آمده در ضمیمه ج، ۶۰۴ ماتریس معکوس‌پذیر بر روی میدان $\mathbb{F}_۲$ حاصل شود.

در یکی از گزارش‌ها [۲۴]، ابتدا با استفاده از الگوریتم‌های ذاتی یک ماتریس MDS ۸×۸ بر روی ورودی ۴ بیتی پیاده‌سازی شده است. سپس با استفاده از روش زیرمیدان یک ماتریس MDS ۸×۸ با هزینه XOR ۳۹۲ برای ورودی ۸ بیتی به‌دست آورده است. در این قسمت قصد داریم با استفاده از توابع دودویی خطی، ماتریس $\mathbf{H}_۸$ در رابطه (۱۹) و معکوس آن را با هزینه XOR ۳۲۰ بر روی ورودی ۸ بیتی پیاده‌سازی نماییم. همچنین ماتریس $\mathbf{H}_۸$ را با هزینه XOR ۳۴۴ بر روی میدان متناهی $\mathbb{F}_{۲^۸}$ پیاده‌سازی نماییم. در ابتدا، ماتریس‌های ۸×۸ دودویی داده شده در رابطه زیر را در نظر بگیرید. می‌توان بررسی نمود که ماتریس‌های $\mathbf{L}_{(i,۸)}$ برای $۱\le i\le ۱۸$ بر روی میدان $\mathbb{F}_۲$ معکوس‌پذیر هستند.

$\mathbf{L}_{(۱,۸)}=[[۱,۸],[۱],[۲,۵],[۳],[۴],[۵],[۶],[۷]]$, $\mathbf{L}_{(۲,۸)}=[[۱,۸],[۱],[۲],[۳,۶],[۴],[۵],[۶],[۷]]$,
$\mathbf{L}_{(۳,۸)}=[[۱,۸],[۱],[۲],[۳],[۴,۷],[۵],[۶],[۷]]$, $\mathbf{L}_{(۴,۸)}=[[۳,۸],[۱],[۲],[۳],[۴,۵],[۵],[۶],[۷]]$,
$\mathbf{L}_{(۵,۸)}=[[۳,۸],[۱],[۲],[۳],[۴],[۵,۶],[۶],[۷]]$, $\mathbf{L}_{(۶,۸)}=[[۳,۸],[۱],[۲],[۳],[۴],[۵],[۶,۷],[۷]]$,
$\mathbf{L}_{(۷,۸)}=[[۸],[۱,۲],[۲],[۳,۶],[۴],[۵],[۶],[۷]]$, $\mathbf{L}_{(۸,۸)}=[[۸],[۱,۲],[۲],[۳],[۴,۷],[۵],[۶],[۷]]$,
$\mathbf{L}_{(۹,۸)}=[[۸],[۱,۲],[۲],[۳],[۴],[۵,۸],[۶],[۷]]$, $\mathbf{L}_{(۱۰,۸)}=[[۸],[۱,۴],[۲],[۳],[۴],[۵,۶],[۶],[۷]]$,
$\mathbf{L}_{(۱۱,۸)}=[[۸],[۱,۴],[۲],[۳],[۴],[۵],[۶,۷],[۷]]$, $\mathbf{L}_{(۱۲,۸)}=[[۸],[۱,۴],[۲],[۳],[۴],[۵],[۶],[۷,۸]]$,
$\mathbf{L}_{(۱۳,۸)}=[[۸],[۱],[۲,۳],[۳],[۴,۷],[۵],[۶],[۷]]$, $\mathbf{L}_{(۱۴,۸)}=[[۸],[۱],[۲,۳],[۳],[۴],[۵,۸],[۶],[۷]]$,
$\mathbf{L}_{(۱۵,۸)}=[[۸],[۱],[۲,۵],[۳],[۴],[۵],[۶,۷],[۷]]$, $\mathbf{L}_{(۱۶,۸)}=[[۸],[۱],[۲,۵],[۳],[۴],[۵],[۶],[۷,۸]]$,
$\mathbf{L}_{(۱۷,۸)}=[[۸],[۱],[۲],[۳,۴],[۴],[۵,۸],[۶],[۷]]$, $\mathbf{L}_{(۱۸,۸)}=[[۸],[۱],[۲],[۳,۶],[۴],[۵],[۶],[۷,۸]]$.

با جستجوی کامپیوتری بررسی شد که با جایگذاری ماتریس‌های ۸×۸ $\mathbf{L}_{(i,۸)}$ برای $۱\le i\le ۱۸$، در ۶۰۴ شرط داده شده در ضمیمه ج، ماتریس‌های معکوس‌پذیر در میدان $\mathbb{F}_۲$ حاصل می‌شود. همچنین، هزینه پیاده‌سازی ماتریس‌های $\mathbf{L}_{(i,۸)}$ برای $۱\le i\le ۱۸$ و معکوس آن‌ها دو XOR است؛ بنابراین، هزینه پیاده‌سازی توان دوم ماتریس‌های $\mathbf{L}_{(i,۸)}$ چهار XOR است. حال با استفاده از رابطه (۲۰)، هزینه پیاده‌سازی ماتریس $\mathbf{H}_۸$ و معکوس آن برابر ۳۲۰ XOR است زیرا داریم:

$$۳۲\times ۸+۸\times ۲+۸\times ۴+۸\times ۲=۳۲۰$$

در ادامه، می‌توان بررسی نمود که چندجمله‌ای تحویل‌ناپذیر $\mathbf{f}=x^۸+x^۷+x^۵+x^۴+۱$ در بین شرط‌های داده‌شده در ضمیمه ج نیست؛ بنابراین، می‌توان ماتریس $\mathbf{H}_۸$ را بر روی میدان $\mathbb{F}_{۲^۸}$ با استفاده از چندجمله‌ای $\mathbf{f}$ پیاده‌سازی نمود. فرض کنید α ریشه $\mathbf{f}$ باشد. نمایش ماتریسی α در میدان $\mathbb{F}_۲$ به‌صورت زیر است:

$$\mathbf{L}=[[۸],[۱],[۲],[۳],[۴,۸],[۵,۸],[۶],[۷,۸]]$$

هزینه پیاده‌سازی ماتریس‌های $\mathbf{L}$، $\mathbf{L}^{-۱}$ و $\mathbf{L}^۲$ به ترتیب ۳، ۳ و ۵ XOR است. برای مثال فرض نمایید $\mathbf{x}=[x_۱,\cdots,x_۸]$. آنگاه هزینه پیاده‌سازی ماتریس $\mathbf{L}^۲$ برابر ۵ است زیرا داریم:

$$\mathbf{L}^۲\cdot\mathbf{x}^T=[x_۷+x_۸,x_۸,x_۱,x_۲,x_۳+x_۷+x_۸,x_۴+x_۷,x_۵+x_۸,x_۶+x_۷+x_۸]^T,$$
$$u_۱=x_۷+x_۸,u_۲=u_۱+x_۳,u_۳=x_۴+x_۷,u_۴=x_۵+x_۸,u_۵=u_۱+x_۶.$$

بنابراین، هزینه پیاده‌سازی ماتریس $\mathbf{H}_۸$ در رابطه (۱۶)، با استفاده از ماتریس $\mathbf{L}$در رابطه (۲۱)، برابر با ۳۴۴ XOR است زیرا با استفاده از رابطه (۲۰) داریم:

$$۳۲\times ۸+۸\times ۳+۸\times ۵+۸\times ۳=۳۴۴$$

به‌عبارت دیگر، ماتریس $\mathbf{H}_۸$ را می‌توان بر روی میدان متناهی $\mathbb{F}_{۲^۸}$، ساخته شده با چندجمله‌ای $\mathbf{f}$، با هزینه ۳۴۴ XOR پیاده‌سازی نمود. مقایسه نتایج به‌دست‌آمده در این مقاله، با بهترین نتیجه‌های موجود در جدول (۱) آورده شده است.

جدول ۱. مقایسه نتایج این مقاله با نتایج موجود، برای ورودی ۸ بیتی

اندازه ماتریس	نوع ماتریس	هزینه پیاده سازی ماتریس	هزینه پیاده سازی معکوس	مرجع
۴×۴	DSI	۸۰	۸۰	[۲۲]
۴×۴	*Hadamard*	۷۲	---	[۲۴]
۴×۴	DSI	۶۸	۶۸	قسمت ۳
۴×۴	DSI	۶۷	۶۷	[۲۳]
۸×۸	LFSR	۵۷۶	۵۷۶	[۲۲]
۸×۸	LFSR	۵۲۰	۵۲۰	[۴]
۸×۸	*Cauchy*	۳۹۲	---	[۲۴]
۸×۸	DSI	۳۲۰	۳۲۰	قسمت ۴

۴. نتیجه‌گیری

در این مقاله با استفاده از به‌کارگیری ماتریس‌های دودویی خلوت در ساختارهای DSI، دو ماتریس MDS ۴×۴ و ۸×۸ پیشنهاد شده است به‌طوری‌که هزینه پیاده‌سازی این ماتریس‌ها و معکوس آن‌ها، برای ورودی ۸ بیتی، به ترتیب ۶۸ و ۳۲۰ XOR یک بیتی است. به‌دلیل اینکه ساختارهای ماتریس‌های MDS پیشنهاد شده، بر اساس ساختارهای DSI است، پیاده‌سازی این ماتریس‌ها و معکوس آن‌ها در سخت‌افزار به‌سادگی انجام می‌شود. همچنین، ماتریس ۴×۴ پیشنهادی در این مقاله را برای ورودی $m \geq 4$ بیتی با هزینه $8m+4$ پیاده‌سازی نمودیم. در پایان، ماتریس ۸×۸ پیشنهادی بر روی میدان متناهی $\mathbb{F}_{2^8}$ با هزینه ۳۴۴ XOR پیاده‌سازی شد.

۵. مرجع‌ها

[1] Blaum, M.; Roth, R. M. “On Lowest Density MDS Codes”; IEEE Trans. Inform. Theory 1999, 45, 46-59.

[2] Junod, P.; Vaudenay, S. “Perfect Diffusion Primitives for Block Ciphers Building Efficient MDS Matrices”; Selected Areas in Cryptography 2004, 3357, 84-99.

[3] Augot, D.; Finiasz, M. “Exhaustive Search for Small Dimension Recursive MDS Diffusion Layers for Block Ciphers and Hash Functions”; Proc. IEEE ISIT 2013, 1551-1555.

[4] Wu, S.; Wang, M.; Wu, W. “Recursive Diffusion Layers for (Lightweight) Block Ciphers and Hash Functions”; Selected Areas of Cryptography 2012, 7707, 355-371.

[5] MacWilliams, F. J.; Sloane, N. J. A. “The Theory of Error Correcting Codes”; North-Holland 1977.

[6] Roth, R. M.; Seroussi, G. “On Generator Matrices of MDS Codes”; IEEE Trans. Inform. Theory 1985, 31, 826-830.

[7] Shirai, T.; Shibutani, K. “On Feistel Structures Using a Diffusion Switching Mechanism”; Fast Software Encryption 2006, 4047, 41-56.

[8] Mirghadri, A.; Yosefipour, M.; Khadem, B.; Sajadieh, M. “Two New Methods for Designing 192-bit Block Ciphers Based on Switching Structure and Recursive Diffusion Layers”; J. Passive Defence Sci. & Technol. 2016, 7, 251-259.

[9] Sim, S. M.; Khoo, K.; Oggier, F.; Peyrin, T. “Lightweight MDS Involution Matrices”; Fast Software Encryption 2015, 9054, 471-493.

[10] Sajadieh, M.; Dakhilalian, M.; Mala, H.; Omoomi, B. “On Construction of Involutory MDS Matrices from Vandermonde Matrices”; Design Code Cryptogr. 2012, 64, 287-308.

[11] Youssef, A. M.; Mister, S.; Tavares, S. E. “On the Design of Linear Transformations for Substitution Permutation Encryption Networks”; Selected Areas of Cryptography 1997, 40-48.

[12] Sajadieh, M.; Dakhilalian, M.; Mala, H.; Sepehrdad, P. “Recursive Diffusion Layers for Block Ciphers and Hash Functions”; Fast Software Encryption 2012, 7549, 385-401.

[13] Berger, T. P. “Construction of Recursive MDS Diffusion Layers from Gabidulin Codes”; Int. Conf. Cryptol. India (INDOCRYPT) 2013, 8250, 274-285.

[14] Augot, D.; Finiasz, M. “Direct Construction of Recursive MDS Diffusion Layers Using Shortened BCH Codes”; Fast Software Encryption 2014, 8540, 3-17.

[15] Gupta, K. C.; Pandey, S. K.; Venkateswarlu, A. “Almost Involutory Recursive MDS Diffusion Layers”; Design Code Cryptogr. 2018, 1-18.

[16] Guo, J.; Peyrin, T.; Poschmann, A. “The PHOTON Family of Lightweight Hash Functions”; Adv. Cryptol. 2011, 684, 222–239.

[17] Barreto, P.; Rijmen, V. “The Khazad Legacy-Level Block Cipher”; Proc. of the 1st Open NESSIE Workshop, Belgium, 2000.

[18] Filho, G. D.; Barreto, P.; Rijmen, V. “The Maelstrom-0 Hash Function”; Proc. 6th Brazilian Sym. Inform. Computer Syst. Secur. 2006.

[19] Daemen, J.; Rijmen, V. “The Design of Rijndael: AES-The Advanced Encryption Standard”; Springer-Verlag 2002.

[20] Gauravaram, P.; Knudsen, L. R.; Matusiewicz, K.; Mendel, F.; Rechberger, C.; Schlaffer, M.; Thomsen S. “Grøstl a SHA-3 Candidate”; http://www.groestl.info, 2008.

[21] Shibutani K. “On the Diffusion of Generalized Feistel Structures Regarding Differential and Linear Cryptanalysis”; Selected Areas of Cryptography 2011, 6544, 211-228.

[22] Toh, D.; Teo, J.; Khoo, K.; Sim, S. M. “Lightweight MDS Serial-Type Matrices with Minimal Fixed XOR Count”; Int. Conf. Cryptol. (AFRICACRYPT) 2018, 10831, 51-71.

[23] Duval, S.; Leurent, G. “MDS Matrices with Lightweight Circuits”; IACR Trans. Symmetric Cryptol. 2018, 48-78.

[24] Kranz, T.; Leander, G.; Stoelen, K.; Wiemer, F. “Shorter Linear Straight-Line Programs for MDS Matrices”; IACR Trans. Symmetric Cryptol. 2017, 188-211.

[25] Zhao, R.; Wu, B.; Zhang, R.; Zhang, Q. “Designing Optimal Implementations of Linear Layers (Full Version)”; Cryptology ePrint Archive, 2016, 1118.

ضمیمه الف

چندجمله‌ای مشخصه ماتریس $\mathbf{R}_n$ بر روی میدان $\mathbb{F}_2$ به‌صورت $\mathrm{Char}(\mathbf{R}_n)=\left|x\mathbf{I}_{2^n}+\mathbf{R}_n\right|$ به‌دست می‌آید. اگر دترمینان را بر روی ستون آخر ماتریس $x\mathbf{I}_{2^n}+\mathbf{R}_n$ انجام دهیم آنگاه داریم:

$$\mathrm{Char}(\mathbf{R}_n)=1\times\left|\mathbf{R}_n^1\right|+x\times\left|\mathbf{R}_n^n\right| \qquad (22)$$

در رابطه (۲۲) ماتریس $\mathbf{R}_n^1$ یک ماتریس بالا مثلثی است که روی قطر اصلی آن، عدد یک است که نتیجه می‌دهد $\left|\mathbf{R}_n^1\right|=1$. همچنین ماتریس $\mathbf{R}_n^n$ یک ماتریس $\left(2^n-1\right)\times\left(2^n-1\right)$ به شکل زیر است:

$$\mathbf{R}_n^n=\begin{bmatrix} x & 0 & \cdots & 0 & 1 & 0 & \cdots & 0\\ 1 & x & 0 & 0 & 0 & 0 & \cdots & 0\\ 0 & 1 & x & 0 & 0 & 0 & \cdots & 0\\ 0 & 0 & 1 & x & 0 & 0 & \cdots & 0\\ 0 & \cdots & 0 & \vdots & \vdots & 0 & \cdots & 0\\ 0 & \cdots & 0 & 0 & 1 & x & 0 & 0\\ 0 & \cdots & 0 & 0 & 0 & 1 & x & 0\\ 0 & \cdots & 0 & 0 & 0 & 0 & 1 & x \end{bmatrix}.$$

در ماتریس $\mathbf{R}_n^n$، عدد یک در سطر اول در 2^{n-2}امین موقعیت قرار دارد. حال اگر عمل دترمینان گیری را بر روی سطر اول ماتریس $\mathbf{R}_n^n$ انجام دهیم آنگاه داریم:

$$\left|\mathbf{R}_n^n\right|=x\times\left|\mathbf{H}_1\right|+1\times\left|\mathbf{H}_2\right| \qquad (23)$$

در رابطه (۲۳) ماتریس $\mathbf{H}_1$ یک ماتریس $\left(2^n-2\right)\times\left(2^n-2\right)$ پایین مثلثی است که روی قطر آن x واقع شده است؛ بنابراین داریم $\left|\mathbf{H}_1\right|=x^{2^n-2}$. همچنین، ماتریس $\mathbf{H}_2$ به‌صورت زیر است:

$$\mathbf{H}_2=\begin{bmatrix} 1 & x & 0 & 0 & 0 & 0 & \cdots & 0\\ 0 & \ddots & \ddots & 0 & 0 & 0 & \cdots & 0\\ 0 & 0 & 1 & x & 0 & 0 & \cdots & 0\\ 0 & \cdots & 0 & 1 & 0 & 0 & \cdots & 0\\ 0 & \cdots & 0 & 0 & x & 0 & \cdots & 0\\ 0 & \cdots & 0 & 0 & 1 & x & 0 & 0\\ 0 & \cdots & 0 & 0 & 0 & \ddots & \ddots & 0\\ 0 & \cdots & 0 & 0 & 0 & 0 & 1 & x \end{bmatrix}.$$

تعداد اعداد یک بر روی قطر اصلی ماتریس $\mathbf{H}_2$ برابر با $2^{n-2}-1$ تا است. اگر عمل دترمینان گیری را روی ستون اول ماتریس $\mathbf{H}_2$ انجام دهیم آنگاه باکمی محاسبه می‌توان نشان داد:

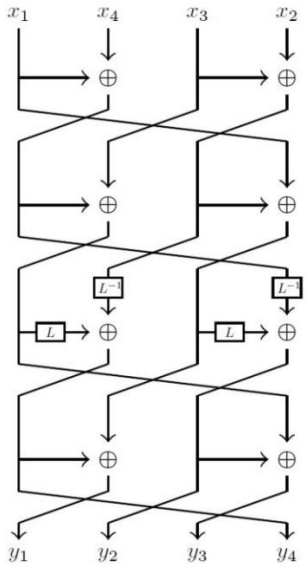
$$\left|\mathbf{H}_2\right|=x^{2^n-2^{n-2}-1}=x^{3\times2^{n-2}-1} \qquad (24)$$

با استفاده از رابطه‌های (۲۳) و (۲۴) در رابطه (۲۲) داریم:

$$\begin{aligned}\mathrm{Char}(\mathbf{R}_n)&=1\times1+x\times\left(x^{2^n-1}+x^{3\times2^{n-2}-1}\right)\\&=x^{2^n}+x^{3\times2^{n-2}}+1=\left(x^4+x^3+1\right)^{2^{n-2}}\end{aligned} \qquad (25)$$

در رابطه (۲۵) از این واقعیت استفاده نمودیم که در میدان متناهی با مشخصه ۲ داریم $(a+b)^2=a^2+b^2$.

ضمیمه ب



ضمیمه ج

ماتریس $\mathbf{H}_8$ در رابطه (۱۹)، به‌صورت زیر به‌دست آمده است:

$$\mathbf{H}_8=$$

$$\begin{bmatrix} L^4+1 & L^2+L+L^{-1}+1 & L^4+1 & L^5+L^2+L^{-2}+1\\ L^4 & 1 & L^2+L+L^{-1}+1 & L^2+L^{-2}\\ L^6 & L^4 & L^4+1 & L^2+L+L^{-1}+1\\ L^6+L^3 & L^4 & L^4 & 1\\ L^{-2} & L^6+L^3 & L^6 & L^4\\ L^5+L^2+L^{-2}+1 & L^6 & L^6+L^3 & L^4\\ L^4+1 & L^5+L^2+L^{-2}+1 & L^{-2} & L^6+L^3\\ L^2+L+L^{-1}+1 & L^2+L^{-2} & L^5+L^2+L^{-2}+1 & L^6 \end{bmatrix}$$

$$\begin{bmatrix} L^{-2} & L^6+L^3 & L^6 & L^4\\ L^5+L^2+L^{-2}+1 & L^6 & L^6+L^3 & L^4\\ L^4+1 & L^5+L^2+L^{-2}+1 & L^{-2} & L^6+L^3\\ L^2+L+L^{-1}+1 & L^2+L^{-2} & L^5+L^2+L^{-2}+1 & L^6\\ L^4+1 & L^2+L+L^{-1}+1 & L^4+1 & L^5+L^2+L^{-2}+1\\ L^4 & 1 & L^2+L+L^{-1}+1 & L^2+L^{-2}\\ L^6 & L^4 & L^4+1 & L^2+L+L^{-1}+1\\ L^6+L^3 & L^4 & L^4 & 1 \end{bmatrix}.$$

ضمیمه د

بخاطر ساده‌نویسی، چندجمله‌ای‌های تحویل‌ناپذیر را با استفاده از مقادیر هگزا نمایش داده‌ایم. برای مثال چندجمله‌ای x^4+x+1 به صورت 0x13 نمایش داده شده است.

0x2, 0x3, 0x7, 0xB, 0xD, 0x13, 0x19, 0x1F,
0x25, 0x29, 0x2F, 0x37, 0x3B, 0x3D, 0x43, 0x49,
0x61, 0x57, 0x5B, 0x67, 0x6D, 0x73, 0x75, 0x83,
0x89, 0x91, 0xC1, 0x8F, 0x9D, 0xA7, 0xAB, 0xB9,
0xCB, 0xD3, 0xD5, 0xE5, 0xF1, 0xBF, 0xEF, 0xF7,
0xFD, 0x11B, 0x11D, 0x12B, 0x12D, 0x139, 0x14D,
0x163, 0x165, 0x169, 0x171, 0x187, 0x18B, 0x18D,
0x1A3, 0x1A9, 0x1C3, 0x13F, 0x15F, 0x177, 0x17B,
0x19F, 0x1CF, 0x1D7, 0x1DD, 0x1E7, 0x1F3, 0x1F5,
0x1F9, 0x221, 0x301, 0x217, 0x21B, 0x22D, 0x233,
0x24B, 0x265, 0x269, 0x287, 0x295, 0x299, 0x2A5,
0x2D1, 0x315, 0x323, 0x331, 0x349, 0x361, 0x385,
0x3A1, 0x25F, 0x277, 0x27D, 0x2B7, 0x2BD, 0x2CF,
0x2DB, 0x2F5, 0x2F9, 0x31F, 0x33B, 0x34F, 0x36B,
0x36D, 0x373, 0x38F, 0x3B9, 0x3CB, 0x3CD, 0x3D5,
0x3D9, 0x3E3, 0x3E9, 0x37F, 0x3FB, 0x409, 0x481,
0x41B, 0x41D, 0x435, 0x453, 0x4A9, 0x50B, 0x519,
0x523, 0x543, 0x585, 0x613, 0x623, 0x625, 0x631,
0x651, 0x685, 0x6C1, 0x721, 0x781, 0x4D7, 0x4F3,
0x557, 0x567, 0x56B, 0x58F, 0x597, 0x59B, 0x5B9,
0x637, 0x64F, 0x65B, 0x679, 0x6A7, 0x6CD, 0x6D3,
0x70F, 0x747, 0x763, 0x787, 0x78D, 0x793, 0x7A9,
0x5F7, 0x5FB, 0x6BF, 0x6F7, 0x6FD, 0x77B, 0x7DB,
0x7F9, 0x7FF, 0x805, 0x863, 0x871, 0x895, 0x8A9,
0x8B1, 0x8D1, 0x8E1, 0x913, 0x929, 0xA07, 0xA49,
0xC0B, 0xC89, 0xE81, 0x89F, 0x8CF, 0x8E7, 0x8F5,
0x95B, 0x9AD, 0x9C7, 0xA6D, 0xA9D, 0xAA7, 0xAAB,
0xAD5, 0xB4B, 0xB59, 0xBC9, 0xC1F, 0xC57, 0xC73,
0xC97, 0xC9B, 0xCD3, 0xCD5, 0xD1D, 0xD27, 0xD93,
0xE27, 0xE2B, 0xE4B, 0xEA3, 0xF0B, 0x9F7, 0xB6F,
0xBBD, 0xBDD, 0xCBF, 0xCF7, 0xD6F, 0xDBD, 0xDD7,
0xDE7, 0xDF5, 0xE5F, 0xE7D, 0xECF, 0xF37, 0xF5D,
0xF6D, 0xF97, 0xFA7, 0xFB5, 0xFFB, 0x1201, 0x120D,
0x1225, 0x1245, 0x1431, 0x1449, 0x1849, 0x1883, 0x1C05,
0x1D01, 0x1077, 0x111F, 0x11B3, 0x12B9, 0x131D, 0x13A3,
0x1467, 0x14E5, 0x154D, 0x1655, 0x18B9, 0x18CB, 0x18F1,
0x1999, 0x19C9, 0x1A2B, 0x1A63, 0x1B0D, 0x1B45, 0x1C27,
0x1C4D, 0x1CA5, 0x1D43, 0x1D83, 0x1F81, 0x13D7, 0x13DD,
0x166F, 0x1775, 0x18FB, 0x196F, 0x19E7, 0x1A5F, 0x1B2F,
0x1BD3, 0x1CEB, 0x1D3D, 0x1EB9, 0x1F39, 0x20C9, 0x2451,
0x2941, 0x209F, 0x2197, 0x21E3, 0x2563, 0x2571, 0x283D,
0x2993, 0x2C4D, 0x2CC5, 0x2D45, 0x2E91, 0x2F05, 0x31C9,
0x350D, 0x3705, 0x384B, 0x3A07, 0x3A51, 0x3C83, 0x25D7,

ادامه لیست چندجمله‌های تحویل‌ناپذیر داده شده در ضمیمه ج

0x263F, 0x273B, 0x276B, 0x2ADB, 0x2BAD, 0x2D67, 0x2E5B,
0x2EB9, 0x2F65, 0x34F9, 0x363B, 0x378B, 0x37E1, 0x3B53,
0x3C3B, 0x3D4D, 0x3D69, 0x3DB1, 0x3E69, 0x3F43, 0x3F45,
0x2EFD, 0x2FDD, 0x2FED, 0x3BF3, 0x3F37, 0x4021, 0x4941,
0x5007, 0x5301, 0x405F, 0x41F1, 0x44D5, 0x45C9, 0x491D,
0x4A93, 0x4CD1, 0x505D, 0x5265, 0x5271, 0x58B1, 0x5A25,
0x5AC1, 0x5E81, 0x609D, 0x6389, 0x681D, 0x7903, 0x45F3,
0x47D3, 0x4BB9, 0x572D, 0x5E47, 0x6697, 0x693D, 0x6BA5,
0x6D69, 0x6DC3, 0x715D, 0x719B, 0x722F, 0x754B, 0x761D,
0x7653, 0x7655, 0x7695, 0x76A3, 0x786D, 0x7A35, 0x7E61,
0x53BF, 0x597F, 0x74FD, 0x79D7, 0x7B5D, 0x8431, 0x84A1,
0x9061, 0x9809, 0xA481, 0xAC01, 0x8371, 0x84B5, 0x9075,
0x94E1, 0x9919, 0xA06B, 0xA329, 0xA495, 0xB0E1, 0xCC85,
0xD0A3, 0x8DE9, 0x96D3, 0x9A6D, 0xA5A7, 0xAB39, 0xAD1B,
0xB3A9, 0xB6D1, 0xC6E3, 0xCCA7, 0xD663, 0xE46B, 0xED15,
0xF30B, 0xF561, 0xF683, 0x9EED, 0xAC7F, 0xB1DF, 0xB3DD,
0xB5BB, 0xBB4F, 0xCF2F, 0xD66F, 0xDFA5, 0xEDB3, 0xF7DB,
0x18105, 0x101C7, 0x13911, 0x144A3, 0x1133D, 0x130F5,
0x15E0B, 0x15E25, 0x16297, 0x17487, 0x18EA9, 0x1C25D,
0x1C969, 0x1D24D, 0x1E42B, 0x10FE7, 0x177A5, 0x1AE5D,
0x1AE9B, 0x1B38F, 0x1FAB1, 0x1BF6B, 0x1BFAD, 0x1E777,
0x1F56F, 0x1FDD3, 0x2C041, 0x24195, 0x25191, 0x28435,
0x28515, 0x217A9, 0x23BC1, 0x26999, 0x26CA9, 0x26D61,
0x28CCD, 0x29873, 0x29D29, 0x31987, 0x31B85, 0x3C255,
0x29FA9, 0x2BEC9, 0x2D8F5, 0x3558F, 0x37D85, 0x38FA3,
0x39FA1, 0x3B9C3, 0x3EEC1, 0x3F4C9, 0x27EBD, 0x2DDD7,
0x48301, 0x421ED, 0x45B49, 0x5B443, 0x65545, 0x65781,
0x68CD1, 0x72B21, 0x46F47, 0x47B93, 0x5135F, 0x58ED9,
0x62BD3, 0x660BF, 0x7B169, 0x4F37D, 0x54FF3, 0x5F74B,
0x69F3B, 0x6DBE5, 0x7695F, 0x7E07F, 0xA462D, 0xFE009,
0xA69A7, 0xAA6C7, 0xC9A97, 0xE283F, 0xE6A4D, 0xFF103,
0x9F6D9, 0xF4773, 0xF9C4F, 0xFA6D5, 0xFB751, 0xFF0B3,
0xFFD3F, 0x105C05, 0x10507D, 0x1052AB, 0x10EA43, 0x17120B,
0x12AE39, 0x151E69, 0x1CE683, 0x1FB043, 0x12AFCB, 0x1CE83F,
0x340021, 0x26C125, 0x280DC3, 0x243F83, 0x2B1279, 0x2FA071,
0x2FAA11, 0x30387D, 0x3226E5, 0x3815E3, 0x3C2663, 0x3AC57F,
0x3F427F, 0x27FEED, 0x400C95, 0x450911, 0x405D45, 0x423195,
0x4988C5, 0x43A933, 0x706555, 0x57314F, 0x64DF91, 0x6B44AF,
0x71CB6F, 0x75AF2D, 0x7A567D, 0x7ED6C9, 0x7F7833, 0x81503D,
0x920BA1, 0xA0B191, 0xD4500B, 0x90570F, 0x921FA1, 0x925D83,
0xA24F15, 0x81F1F3, 0xD464F9, 0xF13C8D, 0xF951D1,
0x1C09423, 0x10BC10F, 0x11147D1, 0x118499B,
0x15138C5, 0x1A6058D, 0x14BA2EF, 0x1C7F193,
0x1D741BD, 0x240BC21, 0x31C2C91, 0x3A8CB49,
0x30CD3CF, 0x399B917, 0x2FF22CF, 0x3D1E87F,
0x52485C5, 0x543B111, 0x464EAC5, 0x550A9D5,
0x422A6FF, 0x4603DBF, 0x524FF91, 0xBB07017,
0x101B02C1, 0x15CFAB23, 0x3C077C4F, 0x3FDF6D43,
0x440408E5, 0x40458B45, 0x401B3BC1, 0x40299DC5,
0x417E2371, 0xFC73341F, 0x105580585, 0x105CA9185.