ششمین کنفرانس بین المللی انجمن رمز ایران
۱۵ و ۱۶ مهر ماه ۱۳۸۸، دانشگاه اصفهان
انجمن رمز ایران
دانشگاه اصفهان

محاسبه دقیق توزیع وزن ورودی-خروجی برای ماتریس‌های MDS با ابعاد ۴×۴

حمید ملا[۱]، محمد دخیل‌علیان[۲]، سید مهدی سجادیه[۱] و رؤیا عرب لو دریچه[۱]

[۱] اصفهان، دانشگاه صنعتی اصفهان، دانشکده برق و کامپیوتر، آزمایشگاه تحقیقاتی رمزنگاری و امنیت سیستم‌ها
Cryptography & System Security Research Lab (CSSRL)
hamid_mala@ec.iut.ac.ir, sadjadieh@ec.iut.ac.ir, r_arab_loodariche@yahoo.com

[۲] اصفهان، دانشگاه صنعتی اصفهان، دانشکده برق و کامپیوتر
mdalian@ cc.iut.ac.ir

چکیده

ماتریس‌های MDS که نشأت‌گرفته از کدهای تصحیح خطای MDS هستند، دارای کاربردهای فراوانی در رمزهای قالبی، رمزهای دنباله‌ای و توابع درهمساز می‌باشند. ایجاد انتشار مناسب برای رمزهای قالبی همچون الگوریتم‌های رمز AES و KHAZAD از مهمترین مصادیق کاربرد این ماتریس‌ها در رمزنگاری می‌باشد. در این مقاله، توزیع وزن ورودی- خروجی و احتمالات گذار برای ماتریس‌های MDS با ابعاد ۴×۴ به صورت جبری و به طور دقیق محاسبه شده است. نتایج بدست آمده می‌تواند در حمله‌ی تفاضل ناممکن به الگوریتم‌هایی که در لایه انتشار خود از این ماتریس‌ها استفاده می‌کنند، مورد استفاده قرارگیرد.

واژه‌های کلیدی

انتشار، رمز قالبی، ماتریس MDS

۱- مقدمه

الگوریتم‌های رمز قالبی از مهمترین ابزارهای رمزنگاری هستند. در طراحی رمزهای قالبی دو معیار انتشار[۱] و درهم‌پیچیدگی[۲] از اهمیت بسیاری برخوردارند. برای ایجاد انتشار مناسب در ساختار رمزهای قالبی، تاکنون روشهای مختلفی مورد توجه قرارگرفته است. جابجایی بیتی یکی از ابتدایی‌ترین روشهاست که در رمزهایی همچون DES و SERPENT به کار رفته است [۱و۲]. در رمزهایی همچون ARIA و CAMELLIA برای ایجاد انتشار، از ماتریس‌های باینری استفاده شده است [۳و۴]. ماتریس‌های MDS[۳] در رمزهایی همچون KHAZAD ، Square و AES مورد استفاده قرار گرفته‌اند [۵و۶و۷]. ماتریسهای MDS در رمزهای دنباله‌ای و توابع درهمساز[۴] پیام نیز مورد استفاده قرار می‌گیرند.

حمله "تفاضل ناممکن"[۵] یکی از مشتقات حمله تفاضلی[۶] [۸] است که برای اولین بار در [۹] ارایه شده است. برخلاف حمله تفاضلی که بر مبنای یافتن تفاضل‌های با احتمال وقوع بالا استوار است، در حمله تفاضل ناممکن از تفاضل‌های با احتمال وقوع صفر برای حذف زیرکلیدهای نادرست استفاده می‌شود. این حمله یکی از قوی‌ترین حملات موجود به رمزهای قالبی است که برای تحلیل AES نیز مورد استفاده قرار گرفته است.

با برگزیده شدن الگوریتم Rijndael به عنوان استاندارد رمزگذاری پیشرفته (AES)، این الگوریتم کاربرد روزافزونی یافته است. به همین سبب همواره از سوی تحلیل‌گران، در معرض تحلیل‌های مختلف قرار می‌گیرد. برای ایجاد انتشار در الگوریتم

[1] Diffusion
[2] Confusion
[3] Maximum Distance Separable (MDS)
[4] Hash function
[5] Impossible Differential Attack
[6] Differential Attack

AES از یک ماتریس MDS ۴×۴ با عناصری از $GF(2^8)$ استفاده شده است. ورودی و خروجی این ماتریس بردارهای (کلمات) چهاربایتی می‌باشد. نحوه عملکرد این ماتریس نقش عمده‌ای در حمله تفاضل ناممکن به الگوریتم AES دارد. به عنوان مثال احتمال اینکه یک بردار با وزن همینگ ۲ در ورودی، به یک بردار با وزن همینگ ۳ در خروجی تبدیل شود می‌تواند در روند حمله تفاضل ناممکن به AES بسیار مهم باشد. اگرچه پیش از این در مراجع مختلف و از جمله [۱۰] فرض یکنواختی توزیع خروجی ماتریس MDS، مورد استفاده قرار گرفته است، در این مقاله توزیع وزن ورودی-خروجی برای ماتریس‌های MDS ۴×۴ به صورت یک قضیه بیان و به طور دقیق محاسبه و اثبات می‌شود. این توزیع نه تنها برای عملیات MixColumns در رمز AES بلکه برای تمام ماتریس‌های MDS ۴×۴ برقرار است.

در این مقاله، ابتدا در بخش ۲ ماتریس‌های MDS ۴×۴ و خواص آنها مرور می‌گردد. سپس در بخش ۳ یک قضیه اساسی در مورد توزیع وزن ورودی-خروجی برای این ماتریس‌ها بیان و اثبات می‌شود. بخش ۴ به خلاصه و نتیجه‌گیری اختصاص یافته است.

۲- مبانی ریاضی

ماتریس‌های MDS با ابعاد ۴×۴ و با عناصری از $GF(2^8)$ تا کنون در رمزهای قالبی متعددی همچون AES و Square مورد استفاده قرار گرفته‌اند [۶و۷]. ماتریس MDS به صورت زیر تعریف می‌شود.

تعریف ۱: ماتریس مربعی A را یک ماتریس MDS می‌نامیم هرگاه دترمینان هر زیرماتریس مربعی از آن، غیرصفر باشد [۶].

این ماتریس‌ها در واقع عملگرهای خطی بوده و وظیفه فراهم آوردن انتشار مناسب و بهینه را برای رمز قالبی بر عهده دارند. این عملیات در مورد رمز AES به عملیات MixColumns یا به اختصار MC موسوم شده است. اگر ورودی و خروجی این عملگر را کلمات ۳۲ بیتی x و y در نظر بگیریم، می‌توان عملیات را به صورت ضرب ماتریسی زیر نشان داد. توجه کنید که ضرب و جمع عناصر در $GF(2^8)$ انجام می‌گردد.

$$y = A.x \Leftrightarrow \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \quad (۱)$$

که در آن کلمات x و y هر کدام با ۴ بایت نشان داده شده‌اند. با توجه به خطی بودن عملیات، هر زوج کلمه ۳۲ بیتی با تفاضل Δx در ورودی منجر به یک زوج کلمه ۳۲ بیتی با تفاضل مشخص Δy به صورت زیر می‌شود:

$$\Delta y = A.\Delta x \quad (۲)$$

تعریف ۲: وزن همینگ[1] کلمه ۳۲ بیتی (۴ بایتی) x به صورت زیر تعریف می‌شود:

$$w(x) = \#\{x_i : x_i \neq 0\}\ ;\ x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}; x_i \in GF(2^8) \quad (۳)$$

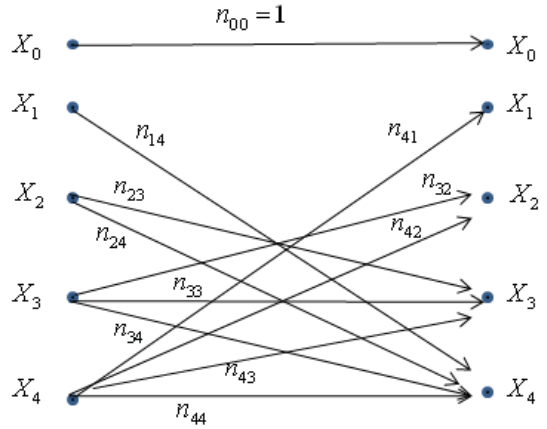
واضح است که $w(x)$ عددی بین ۰ تا ۴ خواهد بود. اکنون می‌توان تمام کلمات ۳۲ بیتی را با توجه به وزن همینگ آن‌ها به ۵ زیر مجموعه افراز کرد.

$$X_i = \{x : w(x) = i\}, i = 0,1,...,4 \quad (۴)$$

بنابراین واضح است که :

$$\{0,1\}^{32} = \bigcup_{i=0}^{4} X_i \quad (۵)$$

از طرفی می‌دانیم برای ماتریس MDS ۴×۴، عدد انشعاب[2] برابر با ۵ است؛ بنابراین چنانچه ورودی عملگر دارای وزن همینگ ۱ باشد، خروجی آن حتماً دارای وزن همینگ ۴ خواهد شد و اگر ورودی دارای وزن ۲ باشد، خروجی یکی از دو وزن ۳ یا ۴ را اتخاذ می‌نماید. شکل ۱، تمام حالت‌های ممکن که یک کلمه ۳۲ بیتی با وزن مشخص در اثر لایه انتشار (ماتریس MDS) به کلمه‌ی با وزن مشخص دیگری تبدیل می‌شود را نشان می‌دهد.



شکل ۱: حالات ممکن برای تبدیل کلمات با وزن i به کلمات با وزن j.

در این شکل منظور از n_{ij} تعداد کلمات ۳۲ بیتی با وزن i است که با عبور از ماتریس A به کلمات ۳۲ بیتی با وزن j تبدیل می‌شوند. به عبارت دیگر n_{ij} برابر است با:

$$n_{ij} \quad \#\{x \in X_i : A.x \in X_j\} \quad (۶)$$

با توجه به معکوس پذیر بودن ماتریس MDS واضح است که:

$$\forall\ 0 \le i, j \le 4 : n_{ij} = n_{ji} \quad (۷)$$

[1] Hamming Weight

[2] Branch Number

۳- توزیع وزن ورودی-خروجی ماتریس MDS

قضیه‌ی زیر مقدار n_{ij}ها را مشخص می‌سازد.

قضیه ۱: اگر $A_{۴\times۴}$ یک ماتریس MDS باشد، آنگاه توزیع وزنی ورودی-خروجی این ماتریس مطابق جدول ۱ می‌باشد که در آن:

$$n_{ij} = \#\{ x \ : w(x) = i \ , \ w(Ax) = j \ \} \qquad (۸)$$

اثبات: با توجه به خطی بودن ماتریس A، واضح است که وزنی تمام-صفر به خروجی تمام-صفر تبدیل می‌شود و n_{00}=1 است. تمام کلمات با وزن ۱، توسط ماتریس A به کلمات با وزن ۴ تبدیل می‌شوند؛ بنابراین n_{14}=4×(2^8-1) . محاسبه‌ی سایر n_{ij}ها به صورت زیر انجام می‌شود.

جدول ۱: تعداد حالات ممکن برای تبدیل کلمات با وزن *i* به کلمات با وزن *j*.

i, j	$n_{ij} = n_{ji}$
۰ و ۰	۱
۴ و ۱	۴×۲۵۵
۳ و ۲	۶×۴×۲۵۵
۴ و ۲	۶×۶۴۰۰۵
۳ و ۳	۴×۴×۶۴۰۰۵
۴ و ۳	۴×۱۶۳۲۳۸۲۵
۴ و ۴	۴۱۶۲۵۷۰۲۷۵

محاسبه n_{23} :

برای محاسبه n_{23} ، کلمه ورودی را به فرم $x=(x_1\ x_2\ 0\ 0)^T$ و کلمه خروجی را به فرم $y=(y_1\ y_2\ y_3\ 0)^T$ در نظر بگیرید که در آن x_iها و y_jها همگی غیر صفر می‌باشند. واضح است که تعداد کل کلمات ورودی به فرم $(x_1\ x_2\ 0\ 0)$ برابر با $(2^8\text{-}1)^2$ است. اما همه آن‌ها نمی‌توانند در رابطه‌ی:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ 0 \end{pmatrix} \qquad (۹)$$

صدق کنند؛ زیرا با توجه به سطر چهارم ماتریس داریم :

$$a_{41}x_1 + a_{42}x_2 = 0 \Rightarrow x_2 = -a_{42}^{-1}a_{41}x_1 \qquad (۱۰)$$

از طرف دیگر x_1 و x_2 باید سه نامعادله‌ی زیر را نیز که از رابطه‌ی (۹) به دست می‌آیند، برآورده سازند.

$$a_{11}x_1 + a_{12}x_2 = y_1 \neq 0 \qquad (۱۱)$$

$$a_{21}x_1 + a_{22}x_2 = y_2 \neq 0 \qquad (۱۲)$$

$$a_{31}x_1 + a_{32}x_2 = y_3 \neq 0 \qquad (۱۳)$$

به عنوان مثال برای اینکه (۱۰) و (۱۱) همزمان برقرار باشند، بایستی:

$$a_{11}x_1 + a_{12}(-a_{42}^{-1}a_{41}x_1) \neq 0$$
$$\Rightarrow a_{11} - a_{12}a_{42}^{-1}a_{41} \neq 0$$
$$\Rightarrow a_{11}a_{42} - a_{12}a_{41} \neq 0$$

این شرط خود بخود برقرار است: زیرا ماتریس A ، MDS است و دترمینان هر زیرماتریس مربعی از آن از جمله زیر ماتریسی که از حذف سطرهای ۲ و ۳ ستونهای ۴ و ۳ بدست می‌آید (این زیرماتریس با $A_{(2,3),(3,4)}$ نمایش داده می‌شود) غیر صفر است.

$$A_{(2,3),(3,4)} = \begin{pmatrix} a_{11} & a_{12} \\ a_{41} & a_{42} \end{pmatrix}$$
$$\det(A_{(2,3),\,(3,4)}) = a_{11}a_{42} - a_{12}a_{41} \neq 0$$

بطور مشابه، با برقرار بودن رابطه (۱۰) ، رابطه‌های (۱۲) و (۱۳) نیز به دلیل MDS بودن ماتریس A خودبخود برقرار می‌باشند؛ لذا تنها شرط روی x_2 و x_1 برای صدق در (۹) همان رابطه (۱۰) است. بنابراین تعداد ورودی‌های به فرم $(x_1\ x_2\ 0\ 0)^T$ برابر با (۱-۲^۸) می‌باشد. از طرف دیگر در حالت کلی $\binom{4}{2} = 6$ فرم مختلف برای کلمه‌ی ۴ بایتی ورودی وجود دارد که ۲ بایت آن صفر باشد و همچنین $\binom{4}{1} = 4$ فرم مختلف برای کلمه‌ی ۴ بایتی خروجی وجود دارد که فقط یک بایت آن صفر باشد؛ بنابراین n_{23} برابر می‌شود با:

$$n_{23} = \binom{4}{2}\binom{4}{1}(2^8 - 1) = 6120 = n_{32}$$

محاسبه n_{24} :

برای محاسبه n_{24} بایستی تعداد کلمات با وزن ۲ که توسط ماتریس A به کلمات با وزن ۴ تبدیل می‌شوند را شمارش کنیم. یک فرم از شش فرم ممکن برای کلمه‌ی ورودی با وزن ۲ را به صورت $x=(x_1\ x_2\ 0\ 0)^T$ در نظر بگیرید؛ بایستی رابطه‌ی زیر به ازای $y_i \neq 0$ برقرار باشد.

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} \qquad (۱۴)$$

رابطه‌ی (۱۴) را می‌توان به روابط زیر تبدیل نمود:

$$a_{11}x_1 + a_{12}x_2 = y_1 \neq 0 \Rightarrow x_2 \neq -a_{12}^{-1}a_{11}x_1 \qquad (۱۵)$$

$$a_{21}x_1 + a_{22}x_2 = y_2 \neq 0 \Rightarrow x_2 \neq -a_{22}^{-1}a_{21}x_1 \qquad (۱۶)$$

$$a_{31}x_1 + a_{32}x_2 = y_3 \neq 0 \Rightarrow x_2 \neq -a_{32}^{-1}a_{31}x_1 \qquad (۱۷)$$

$$a_{41}x_1 + a_{42}x_2 = y_4 \neq 0 \Rightarrow x_2 \neq -a_{42}^{-1}a_{41}x_1 \qquad (۱۸)$$

چهار مقدار ذکر شده در سمت راست چهار رابطه‌ی اخیر، از هم مجزا هستند؛ به عنوان مثال اگر سمت راست رابطه (۱۵) با سمت راست رابطه (۱۶) برابر باشد داریم:

$$-a_{12}^{-1}a_{11}x_1 = -a_{22}^{-1}a_{21}x_1$$
$$\Rightarrow a_{11}a_{22} - a_{21}a_{12} = 0 \Rightarrow \det(A_{(3,4),(4,3)}) = 0$$

که متناقض با MDS بودن ماتریس A می‌باشد. بنابراین x_2 علاوه بر صفر، نمی‌تواند چهار مقدار اخیر را اتخاذ نماید؛ اما x_1 تمام مقادیر غیرصفر را می‌تواند اتخاذ نماید. از طرفی ۶ فرم مختلف برای کلمه‌ی با وزن ۲ وجود دارد، پس n_{24} برابر می‌شود با:

$$n_{24} = \binom{4}{2}(2^8-1)(2^8-5)$$

توجه کنید که با توجه به شکل (۱) بایستی :

$$n_{23} + n_{24} = \#\{x : w(x) = 2\} = \binom{4}{2}(2^8-1)^2$$

البته n_{23} و n_{24} محاسبه شده نیز این رابطه را برآورده می‌سازند.

محاسبه n_{34} :

این بار بایستی رابطه‌ی (۱۹) به ازای i=1, 2, 3 , $x_i \neq 0$ و j=1, 2, 3, 4 , $y_j \neq 0$ برقرار باشد.

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ 0 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} \quad (۱۹)$$

با بسط این ضرب ماتریسی داریم:

$$a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = y_1 \neq 0$$
$$\Rightarrow x_3 \neq -a_{13}^{-1}(a_{11}x_1 + a_{12}x_2) \quad (۲۰)$$

$$a_{21}x_1 + a_{22}x_2 + a_{23}x_3 = y_2 \neq 0$$
$$\Rightarrow x_3 \neq -a_{23}^{-1}(a_{21}x_1 + a_{22}x_2) \quad (۲۱)$$

$$a_{31}x_1 + a_{32}x_2 + a_{33}x_3 = y_3 \neq 0$$
$$\Rightarrow x_3 \neq -a_{33}^{-1}(a_{31}x_1 + a_{32}x_2) \quad (۲۲)$$

$$a_{41}x_1 + a_{42}x_2 + a_{43}x_3 = y_4 \neq 0$$
$$\Rightarrow x_3 \neq -a_{43}^{-1}(a_{41}x_1 + a_{42}x_2) \quad (۲۳)$$

اکنون باید بررسی شود که آیا ۴ مقدار مندرج در سمت راست روابط(۲۰) تا (۲۳) می‌توانند با هم برابر باشند یا نه. به عنوان نمونه فرض کنید که سمت راست روابط (۲۰) و (۲۱) با هم مساوی باشند؛ در این‌صورت داریم:

$$-a_{13}^{-1}(a_{11}x_1 + a_{12}x_2) = -a_{23}^{-1}(a_{21}x_1 + a_{22}x_2)$$
$$\Rightarrow (a_{23}a_{11} - a_{13}a_{21})x_1 = (a_{13}a_{22} - a_{23}a_{12})x_2 \quad (۲۴)$$

در رابطه (۲۴) ضرائب x_2 و x_1 از جنس دترمینان زیرماتریس‌های ۲×۲ از ماتریس A بوده و بنابراین غیرصفرند. درنتیجه ممکن است که سمت راست روابط (۲۰) و (۲۱) با هم برابر باشد. حال بررسی می‌کنیم که آیا این دو مقدار مساوی می‌توانند با سمت راست رابطه (۲۲) نیز برابر باشند یا نه. فرض کنید سمت راست روابط (۲۰) و (۲۲) با هم برابر باشند، به طور مشابه با (۲۴) داریم :

$$(a_{33}a_{11} - a_{13}a_{31})x_1 = (a_{13}a_{32} - a_{33}a_{12})x_2 \quad (۲۵)$$

با جایگزین نمودن x_2 از رابطه (۲۵) در رابطه (۲۴) داریم:

$$(a_{13}a_{32} - a_{33}a_{12})(a_{13}a_{22} - a_{23}a_{12})^{-1}(a_{23}a_{11} - a_{13}a_{21})x_1 = (a_{23}a_{11} - a_{13}a_{31})x_1$$

پس از ساده نمودن عبارت فوق داریم :

$$a_{11}(a_{22}a_{33} - a_{32}a_{23}) - a_{12}(a_{33}a_{21} - a_{23}a_{31}) + a_{13}(a_{21}a_{32} - a_{31}a_{22}) = 0$$

عبارت سمت چپ تساوی فوق برابر با دترمینان زیرماتریسی است که از حذف سطر ۴ و ستون ۴ ماتریس A بدست آمده است؛ یعنی:

$$\det(A_{(4),(4)}) = 0$$

و این متناقض با MDS بودن ماتریس A می‌باشد، بنابراین امکان ندارد که بیش از ۲ عبارت از ۴ عبارت سمت راست روابط (۲۰) تا (۲۳) با هم برابر باشند.

همچنین به سادگی می‌توان نشان داد که امکان ندارد که در بین ۴ رابطه‌ی (۲۰) تا (۲۳)، دو جفت رابطه‌ی معادل یکدیگر باشند، مثلاً ممکن نیست که همزمان رابطه‌ی (۲۰) با (۲۱) و رابطه‌ی (۲۲) با (۲۳) معادل یکدیگر باشند. بعلاوه اگر هر یک از روابط (۲۰) تا (۲۳) با رابطه $x_3 \neq 0$ برابر نباشند، (۵-2^8) انتخاب برای x_3 وجود دارد. در این حالت بایستی روابط زیر برقرار باشند:

$$a_{11}x_1 + a_{12}x_2 \neq 0 \Rightarrow x_2 \neq -a_{12}^{-1}a_{11}x_1 \quad (۲۶)$$
$$a_{21}x_1 + a_{22}x_2 \neq 0 \Rightarrow x_2 \neq -a_{22}^{-1}a_{21}x_1 \quad (۲۷)$$
$$a_{31}x_1 + a_{32}x_2 \neq 0 \Rightarrow x_2 \neq -a_{32}^{-1}a_{31}x_1 \quad (۲۸)$$
$$a_{41}x_1 + a_{42}x_2 \neq 0 \Rightarrow x_2 \neq -a_{42}^{-1}a_{41}x_1 \quad (۲۹)$$

به سادگی می‌توان دو مورد زیر را در مورد چهار رابطه‌ی (۲۶) تا (۲۹) دید.

- این ۴ رابطه از همدیگر مستقل‌اند.
- اگر در بین روابط (۲۰) تا (۲۳) یک زوج رابطه معادل وجود داشته باشد آنگاه این چهار رابطه ، خودبخود برقرار می‌باشند.

بنابراین اگر روابط (۲۰) تا (۲۳) مستقل از هم و از رابطه‌ی $x_3 \neq 0$ مستقل باشند، (۵-2^8) مقدار ممکن برای x_3 وجود دارد. بعلاوه در این حالت x_2، ۱۱ مقدار زیر را نمی تواند اتخاذ کند:

- صفر

- $\binom{4}{2}=6$ مقدار حاصل از مساوی قرار دادن هر یک از ۶ زوج ممکن از روابط (۲۰) تا (۲۳)

- ۴ مقدار ممکن مذکور در روابط (۲۶) تا (۲۹)

لذا در این حالت $\binom{4}{3}(2^8-1)(2^8-11)(2^8-5)$ کلمه‌ی ورودی با وزن ۳ وجود دارد که در رابطه‌ی (۱۹) صدق می‌کند. از طرفی چنانچه روابط (۲۰) تا (۲۳) مستقل نباشند، ۲ تا از این ۴ رابطه با هم معادلند (و حالت دیگری هم وجود ندارد) و حتماً روابط (۲۶) تا (۲۹) نیز برقرار خواهند بود. در این حالت برای x_3، (2^8-4) حالت و برای x_2، $\binom{4}{2}=6$ حالت وجود دارد.

اگر روابط (۲۰) تا (۲۳) مستقل باشند اما یکی از آنها با رابطه $x_3\neq 0$ معادل باشد، در این حالت نیز برای x_3، (2^8-4) حالت و برای x_2، ۴ حالت وجود دارد.

جدول ۲، این سه حالت جدا از هم را مورد بررسی قرار می‌دهد.

جدول ۲: حالات ممکن در روند محاسبه‌ی n_{34} .

انتخابهای ممکن برای x_3	انتخابهای ممکن برای x_2	انتخابهای ممکن برای x_1	شرایط
2^8-5	2^8-11	$\binom{4}{3}(2^8-1)$	روابط (۲۰) تا (۲۳) مستقل از هم و مستقل از رابطه $x_3\neq 0$ ۴ رابطه مستقل (۲۶) تا (۲۹) هم باید برقرار باشند
2^8-4	4	$\binom{4}{3}(2^8-1)$	روابط (۲۰) تا (۲۳) مستقل اما یکی از آنها معادل رابطه $x_3\neq 0$ است. ۴ رابطه مستقل (۲۶) تا (۲۹) هم باید برقرار باشند
2^8-4	$\binom{4}{2}=6$	$\binom{4}{3}(2^8-1)$	روابط (۲۰) تا (۲۳) مستقل از هم نباشند و ۲تای آنها با هم معادل باشند (همگی مستقل از $x_3\neq 0$ می‌باشند).

بنابراین n_{34} مجموع تعداد حالت‌های سه سطر جدول ۲ می‌باشد.

$$n_{34}=\binom{4}{3}(2^8-1)(2^8-11)(2^8-5)+\binom{4}{3}(2^8-1)(4)(2^8-4)+\binom{4}{3}(2^8-1)\binom{4}{2}(2^8-4)=4(2^8-1)(2^{16}-6\times 2^8+15)$$

محاسبه n_{33} :

این بار بایستی رابطه (۳۰) به ازای $x_i\neq 0$ و $y_j\neq 0$ برقرار باشد.

$$\begin{pmatrix}a_{11}&a_{12}&a_{13}&a_{14}\\a_{21}&a_{22}&a_{23}&a_{24}\\a_{31}&a_{32}&a_{33}&a_{34}\\a_{41}&a_{42}&a_{43}&a_{44}\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\0\end{pmatrix}=\begin{pmatrix}y_1\\y_2\\y_3\\0\end{pmatrix} \qquad (۳۰)$$

با بسط ضرب ماتریسی فوق داریم:

$$a_{11}x_1+a_{12}x_2+a_{13}x_3=y_1\neq 0 \qquad (۳۱)$$

$$a_{21}x_1+a_{22}x_2+a_{23}x_3=y_2\neq 0 \qquad (۳۲)$$

$$a_{31}x_1+a_{32}x_2+a_{33}x_3=y_3\neq 0 \qquad (۳۳)$$

$$a_{41}x_1+a_{42}x_2+a_{43}x_3=0\Rightarrow x_3=-a_{43}^{-1}(a_{41}x_1+a_{42}x_2) \qquad (۳۴)$$

چون می‌خواهیم x_3 غیرصفر باشد، با توجه به (۳۴) بایستی:

$$a_{41}x_1+a_{42}x_2\neq 0\Rightarrow x_2\neq -a_{42}^{-1}a_{41}x_1 \qquad (۳۵)$$

با جایگذاری x_3 از رابطه (۳۴) در روابط (۳۱) و (۳۲) و (۳۳) داریم:

$$x_2\neq (a_{13}a_{41}-a_{11}a_{43})(a_{12}a_{43}-a_{13}a_{42})^{-1}x_1 \qquad (۳۶)$$

$$x_2\neq (a_{23}a_{41}-a_{21}a_{43})(a_{22}a_{43}-a_{23}a_{42})^{-1}x_1 \qquad (۳۷)$$

$$x_2\neq (a_{33}a_{41}-a_{31}a_{43})(a_{32}a_{43}-a_{33}a_{42})^{-1}x_1 \qquad (۳۸)$$

مقادیر سمت راست سه معادله اخیر، نمی‌توانند با هم برابر باشند؛ زیرا به عنوان مثال اگر مقادیر سمت راست روابط (۳۶) و (۳۷) با هم برابر قرار داده شوند؛ داریم:

$$(a_{13}a_{41}-a_{11}a_{43})(a_{12}a_{43}-a_{13}a_{42})^{-1}=(a_{23}a_{41}-a_{21}a_{43})(a_{22}a_{43}-a_{23}a_{42})^{-1}$$
$$\Rightarrow a_{41}(a_{12}a_{23}-a_{13}a_{22})-a_{42}(a_{11}a_{23}-a_{13}a_{21})-a_{43}(a_{11}a_{22}-a_{12}a_{21})=0$$
$$\det(A_{(3),(4)})=0$$

صفر بودن دترمینان زیرماتریس $A_{(3),(4)}$ متناقض با MDS بودن ماتریس A می‌باشد. از سوی دیگر مقدار سمت راست رابطه (۳۵) نیز نمی‌تواند با مقادیر روابط (۳۶) و (۳۷) و (۳۸) با هم برابر باشند زیرا به عنوان مثال اگر رابطه (۳۵) بخواهد با رابطه (۳۶) برابر شود داریم:

$$-a_{41}(a_{12}a_{43}-a_{13}a_{42})=a_{42}(a_{13}a_{41}-a_{11}a_{43})\Rightarrow a_{11}a_{42}=a_{12}a_{41}\Rightarrow \det(A_{(2,3),(3,4)})=0$$

بنابراین x_2 علاوه بر اینکه غیر صفر است، چهار مقدار ذکر شده در روابط (۳۵) تا (۳۸)را نیز نمی‌تواند اتخاذ نماید. x_3 نیز تنها مقدار مندرج در رابطه (۳۴) را به خود می‌گیرد، اما x_1 هر مقدار از ۱ تا ۱-2^8 را می‌گیرد؛ بنابراین n_{33} برابر با مقدار زیر است.

$$n_{33} = \binom{4}{3}^2 (2^8-1)(2^8-5)(1) = 16\times(2^8-1)(2^8-5)$$

اکنون با محاسبه n_{14}، n_{24} و n_{34} مقدار n_{44} به سادگی از رابطه‌ی $n_{14}+n_{24}+n_{34}+n_{44}=(2^8-1)^4$ بدست می‌آید.

با دراختیار داشتن n_{ij}ها به سادگی می‌توان احتمالات گذار را نیز محاسبه نمود. اگر احتمال تبدیل شدن برداری با وزن همینگ $i=1,2,3,4$ به برداری با وزن همینگ $j=1,2,3,4$ در اثر عبور از یک ماتریس MDS با ابعاد ۴×۴ را با p_{ij} نمایش دهیم، مقادیر p_{ij} از رابطه‌ی (۳۹) محاسبه و در جدول ۳ نشان داده شده است.

$$p_{ij} = \frac{n_{ij}}{\binom{4}{i}\binom{4}{j}.255^i} \qquad (۳۹)$$

در این جدول فرض شده است که مکان بایتهای صفر و بایتهای غیرصفر، هم در ورودی و هم در خروجی معلوم می‌باشد. لازم به ذکر است که موارد ذکر نشده در جدول دارای احتمال صفر می‌باشند.

جدول ۳: احتمالات گذار

(i,j)	p_{ij}	(i,j)	p_{ij}
$(0,0)$	1	$(3,4)$	0.9845
$(1,4)$	1	$(4,1)$	$1/255^3$
$(2,3)$	$1/255$	$(4,2)$	$251/255^3$
$(2,4)$	$251/255$	$(4,3)$	0.0039
$(3,2)$	$1/255^2$	$(4,4)$	0.9845
$(3,3)$	$251/255^2$		

۴- نتیجه‌گیری

در این مقاله توزیع وزنی ورودی-خروجی برای ماتریس‌های MDS با ابعاد ۴×۴ به طور دقیق بدست آمد. ورودی و خروجی ماتریس MDS به صورت بردارهای چهاربایتی در نظرگرفته شد. تعداد بردارهای ورودی با وزن همینگ i $(0\le i\le 4)$ که به بردارهای با وزن همینگ j $(0\le j\le 4)$ در خروجی، تبدیل می‌شوند به طور دقیق محاسبه شد. در روش بدست آوردن این توزیع، صرفاً از تعریف ماتریس MDS استفاده شده است، بنابراین نتیجه حاصل نه تنها برای عملیات MixColumns در AES، بلکه برای تمام ماتریس‌های MDS با همین ابعاد، صحیح می‌باشد. تعمیم این روش برای ماتریسهای با ابعاد ۸*۸ و بزرگتر می‌تواند در کارهای آتی مورد توجه قرارگیرد.

مراجع

[1] Data Encryption Standard. Federal Information Processing Standard (FIPS) 46, National Bureau of Standards, 1977.

[2] R. Anderson, E. Biham, L. Knudsen, "Serpent: A Proposal for the Advanced Encryption Standard." In: First Advanced Encryption Standard (AES) conference. (1998)

[3] D. Kwon, J. Kim, S. Park, S. Hak Sung and etc. "New Block Cipher: ARIA," In: J.I. Lim and D.H. Lee (Eds.), ICISC 2003, LNCS 2971, pp. 432-445, 2004.

[4] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai and etc. " Camellia: a 128-bit block cipher suitable for multiple platforms-design and analysis," In: Stinson, D.R., Tavares, S. (eds.) SAC 2000. LNCS, vol. 2012, pp. 39–56. Springer, Heidelberg (2001)

[5] P. Barreto and V. Rijmen, "The Khazad Legacy-Level Block Cipher," In First Open NESSIE Workshop, KU-Leuven, 2000. Submission to NESSIE.

[6] J. Daemen, L. Knudsen, and V. Rijmen, "The Block Cipher Square," FSE97, volume 1267 of Lectures Notes in Computer Science, pp 149–165. Springer, 1997.

[7] J. Daemen and V. Rijmen, "AES Proposal: Rijndael," In AES Round 1 Technical Evaluation CD-1: Documentation. NIST, 1998.

[8] E. Biham, A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Journal of Cryptology, Vol 3, pp.3-72, (1991)

[9] E. Biham, A. Biryukov and A. Shamir, "Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials," Advances in Cryptology-EUROCRYPT'99, LNCS 2595, pp.12-23, Springer-Verlag (1999)

[10] B. Bahrak, and M.R. Aref, "Impossible differential attack on seven-round AES-128," IET Inf. Secur., 2008, vol. 2, No. 2, pp. 28-32.