نشریه علوم دانشگاه خوارزمی
جلد ۱۲، شماره ۱
تاریخ چاپ زمستان ۱۳۹۱

ویژگی‌های رمزنگاری عملگر ضرب پیمانه‌ای به پیمانهٔ توانی از ۲

*سید مجتبی دهنوی: دانشگاه خوارزمی، دانشکدهٔ ریاضی
اکبر محمودی ریشکانی: دانشگاه شهید بهشتی، دانشکدهٔ ریاضی و علوم کامپیوتر
محمدرضا میرزائی شمس‌آباد: دانشگاه شهید باهنر کرمان، دانشکدهٔ ریاضی و کامپیوتر
عین‌اله پاشا: دانشگاه خوارزمی، دانشکدهٔ ریاضی

چکیده

عملگر ضرب پیمانه‌ای به پیمانهٔ توانی از ۲، یکی از عمل‌گرهای مورد استفاده در رمزنگاری، خصوصاً رمزنگاری متقارن، است. در این مقاله، به بررسی خواص آماری و جبری این عملگر از منظر رمزنگاری می‌پردازیم. در ابتدا توزیع خروجی عملگر ضرب پیمانه‌ای به پیمانهٔ توانی از ۲ را، به‌عنوان یک تابع دودویی برداری، محاسبه می‌کنیم و پس از آن توزیع توابع مؤلفه‌ای آن را به‌دست می‌آوریم. در ادامه، با معرفی یک سنج در اندازه‌گیری میزان ناترازی نگاشت‌ها، به بررسی ناترازی این عملگر و توابع مؤلفه‌ای آن می‌پردازیم. در پایان، درجهٔ جبری توابع مؤلفه‌ای عملگر ضرب پیمانه‌ای به پیمانهٔ توانی از ۲ را بررسی می‌کنیم و یک کران پایین برای درجه‌های مذکور ارائه می‌دهیم.

مقدمه

یکی از عمل‌گرهایی که تاکنون کاربردهای مختلفی در رمزنگاری داشته‌اند، ضرب پیمانه‌ای به پیمانهٔ توانی از ۲ است. به‌عنوان مثال، این عملگر در رمز قالبی مارس[۱] [۱]، یکی از پنج نامزد نهایی پروژهٔ AES و نیز رمز دنباله‌ای سوسمانوک[۲] [۲]، یکی از رمزهای فاز نهایی پروژهٔ ای‌کریپت[۳]، استفاده شده است. به‌همین دلیل، بررسی ویژگی‌های جبری و آماری این عملگر از اهمیت شایانی در طراحی و تحلیل رمزها برخوردار است. در این مقاله، ما ضرب پیمانه‌ای به پیمانهٔ توانی از ۲ را به‌عنوان یک تابع دودویی برداری در نظر می‌گیریم. در بررسی نگاشت‌های دودویی برداری، یکی از مهم‌ترین مواردی که باید بررسی شود، عبارت است از ویژگی‌های آماری خروجی نگاشت: به‌همین منظور، ما توزیع خروجی این عملگر و توابع مؤلفه‌ای آن را به دست می‌آوریم. نکتهٔ درخور توجه آن است که این عملگر بر خلاف عملگر جمع پیمانه‌ای به پیمانهٔ توانی از ۲، تراز نیست؛ از همین رو، ما یک سنج برای اندازه‌گیری مقدار ناترازی نگاشت‌ها تعریف می‌کنیم و به کمک آن، میزان ناترازی عملگر ضرب پیمانه‌ای و توابع مؤلفه‌ای آن را به‌دست می‌آوریم.

واژه‌های کلیدی: ضرب پیمانه‌ای به هنگ توانی از ۲، توابع دودویی، توابع مؤلفه‌ای، درجهٔ جبری، ناترازی
دریافت ۹۰/۱۱/۱۱ پذیرش ۹۱/۸/۳۰
*نویسنده مسئول dehnavism@tmu.ac.ir

۱. Mars ۲. Sosemanuk ۳. Ecrypt

[Downloaded from jsci.khu.ac.ir on 2024-10-12]

یکی از معیارهای دیگر در بررسی توابع دودویی برداری، درجهٔ جبری توابع مؤلفه‌ای است؛ از همین رو، ما با استفاده از نتایج تحقیقات پیشین در زمینهٔ تحلیل جبری این عمل‌گر [۳]، درجات جبری توابع مؤلفه‌ای عمل‌گر ضرب پیمانه‌ای به پیمانهٔ توانی از ۲ را، به‌عنوان یک تابع دودویی برداری بررسی می‌کنیم و برای درجهٔ توابع مؤلفه‌ای، یک کران پایین ارائه می‌دهیم.

در بخش ۲، به بیان تعاریف و اصطلاحات می‌پردازیم. بخش ۳ به محاسبهٔ توزیع خروجی ضرب پیمانه‌ای به پیمانهٔ توانی از ۲ به‌عنوان یک تابع دودویی برداری اختصاص دارد. در بخش ۴، توزیع توابع مؤلفه‌ای این عمل‌گر را به‌دست می‌آوریم. بخش ۵ به ناترازی این عمل‌گر و توابع مؤلفه‌ای آن می‌پردازد. در بخش ۶، به بررسی خواص جبری این عمل‌گر می‌پردازیم و بالاخره در بخش ۷ به نتیجه‌گیری و ارائهٔ راهکار برای تحقیقات آینده می‌پردازیم.

تعاریف و اصطلاحات

در این مقاله، تعداد عناصر مجموعهٔ متناهی A را با $|A|$، قدر مطلق عدد صحیح (حقیقی) a را نیز با $|a|$ و متمم مجموعهٔ A را با $\bar{A}$ نمایش می‌دهیم. بزرگ‌ترین مقسوم‌علیه مشترک دو عدد صحیح a و b را با (a,b) نمایش می‌دهیم. برای تابع $f: A \to B$، نقش معکوس عنصر $b \in B$ را با $f^{-1}(b)$ نمایش داده و به‌صورت $\{a \in A | f(a) = b\}$ تعریف می‌کنیم؛ همچنین، برای هر $X \subseteq B$، نقش معکوس X را با $f^{-1}(X)$ نمایش داده و به‌صورت $\{a \in A \mid f(a) \in X\}$ تعریف می‌کنیم. بزرگ‌ترین توان 2 در تجزیهٔ عدد طبیعی a با $p(a)$ و وزن همینگ یک عدد طبیعی یا بردار x با $w(x)$ نشان داده می‌شود.

فرض کنیم $\mathbb{F}_2$ میدان متناهی با دو عنصر باشد؛ در این صورت هر عنصر ${\mathbb{F}_2}^m$ (حاصل ضرب دکارتی m نسخه از $\mathbb{F}_2$) را می‌توان به‌صورت یک بردار m تایی در نظر گرفت. اگر $\mathbb{Z}_{2^m}$ را حلقهٔ اعداد صحیح به پیمانهٔ 2^m در نظر بگیریم، آن‌گاه یک تناظر یک به یک بین ${\mathbb{F}_2}^m$ و $\mathbb{Z}_{2^m}$ به‌صورت ذیل برقرار است:

$$\varphi: {\mathbb{F}_2}^m \to \mathbb{Z}_{2^m}$$
$$x = (x_{m-1}, \dots, x_0) \longmapsto \varphi(x) = \sum_{i=0}^{m-1} x_i 2^i.$$

حال، ترتیب جزئی $\prec$ را روی ${\mathbb{F}_2}^m$ بدین‌صورت تعریف می‌کنیم:

$$x \prec a \Leftrightarrow x_i \le a_i, \qquad 0 \le i < m;$$

با نمادگذاری فوق اگر

$$x = (x_{m-1}, \dots, x_0), \qquad u = (u_{m-1}, \dots, u_0),$$

آن‌گاه x^u را به‌صورت $x^u = {x_0}^{u_0} \dots {x_{m-1}}^{u_{m-1}}$ تعریف می‌کنیم.

هر تابع f به‌صورت $f: {\mathbb{F}_2}^m \to \mathbb{F}_2$ را یک تابع دودویی می‌نامیم. فرض کنیم f تابعی دودویی باشد؛ در این

[Downloaded from jsci.khu.ac.ir on 2024-10-12]

صورت f را می‌توان به شکلی یکتا که آن را شکل نرمال جبری[۱] f می‌نامیم، نمایش داد [۴]. در واقع داریم:

$$f(x) = \bigoplus_{u \in Z_{2^m}} h_u x^u, \qquad h_u \in \mathbb{F}_2 \tag{1}$$

که ضرایب h_u بدین‌صورت تعیین می‌شوند:

$$h_u = \bigoplus_{x \prec u} f(x).$$

درجهٔ جبری تابع f که با $d(f)$ نمایش داده می‌شود، برابر است با تعداد متغیرها در طولانی‌ترین جملهٔ شکل نرمال جبری، یا به‌طور معادل، برابر است با بزرگ‌ترین مقدار $w(u)$، در میان جملات با $h_u \neq 0$.

هر تابع $f: \mathbb{F}_2{}^n \to \mathbb{F}_2{}^m$، با شرط $m > 1$ را تابع دودویی برداری می‌نامیم. چنین تابعی را می‌توان به‌صورت مرسوم برداری $(f_{m-1}, \dots, f_0)$ از توابع دودویی بیان کرد که هر f_i، $0 \leq i < m$، یک تابع دودویی $f_i: \mathbb{F}_2{}^n \to \mathbb{F}_2$ است. این تابع را تابع مؤلفه‌ای[۲] i- ام می‌نامیم. تابع f_{m-1} را *بالاترین تابع مؤلفه‌ای* می‌نامیم. همچنین، اگر $x \in \mathbb{F}_2{}^n$، آن‌گاه بیت i - ام x را با x_i نشان می‌دهیم. توجه داریم که هر تابع دودویی برداری $f: \mathbb{F}_2{}^n \to \mathbb{F}_2{}^m$، $\binom{m}{2}$ تابع دودویی برداری

$$f_{i,j}: \mathbb{F}_2{}^n \to \mathbb{F}_2{}^2, \qquad i < j$$
$$f_{i,j}(x) = \big(f_i(x), f_j(x)\big), \qquad x \in \mathbb{F}_2{}^n$$

را معین می‌کند: این توابع دودویی برداری را توابع مؤلفه‌ای توأم f می‌نامیم. در اینجا نیز تابع $f_{m-2,m-1}$ را *بالاترین تابع مؤلفه‌ای توأم* می‌نامیم.

اگر متغیر تصادفی X را روی فضای $\mathbb{F}_2{}^n$ با توزیع یکنواخت در نظر بگیریم، یعنی داشته باشیم:

$$P(X = x) = \frac{1}{2^n}, \qquad x \in \mathbb{F}_2{}^n,$$

آن‌گاه هر تابع دودویی $f: \mathbb{F}_2{}^n \to \mathbb{F}_2{}^m$، یک توزیع روی همدامنهٔ f، یعنی $\mathbb{F}_2{}^m$، تعیین می‌کند؛ به‌عبارت دیگر متغیر تصادفی $Y = f(X)$ را با توزیع ذیل خواهیم داشت:

$$P(Y = y) = \frac{|f^{-1}(y)|}{2^n}, \qquad y \in \mathbb{F}_2{}^m.$$

فرض کنیم m، n و d اعدادی طبیعی با شرط $n = dm$ باشند. تابع $f: A \to B$، با شرط $|A| = n$ و $|B| = m$ را تراز می‌نامیم اگر و تنها اگر

$$\forall b \in B,\ |f^{-1}(b)| = d.$$

توزیع ضرب پیمانه‌ای به‌عنوان یک تابع دودویی برداری

در این بخش، به توزیع خروجی‌های عملگر ضرب پیمانه‌ای، به‌عنوان یک تابع دودویی برداری، می‌پردازیم.

۱. Algebraic Normal Form=ANF ۲. Component Boolean Function

[Downloaded from jsci.khu.ac.ir on 2024-10-12]

قضیه ۱-۳. اگر ضرب پیمانه‌ای به هنگ 2^m را به‌عنوان تابع $f: \mathbb{F}_2{}^{2m} \to \mathbb{F}_2{}^m$ با تعریف $f(x,y) = xy \ mod \ 2^m$ در نظر بگیریم، آن‌گاه برای هر $c \in \mathbb{F}_2{}^m$ داریم:

$$|f^{-1}(c)| = (p(c)+1)2^{m-1}$$

که در این‌جا، $p(0)$ را برابر $m+1$ در نظر می‌گیریم.

اثبات. به ازای هر $c \in \mathbb{F}_2{}^m$، $|f^{-1}(c)|$ برابراست با تعداد جواب‌های معادلهٔ $c = xy \ mod \ 2^m$ که در این‌جا c معلوم و (x,y) مجهول است. ابتدا فرض کنیم $c \neq 0$؛ در این صورت این دو حالت پیش می‌آید:

حالت اول: $p(c) = 0$؛ در این صورت c عددی فرد است و در نتیجه هیچ‌کدام از x و y نمی‌توانند زوج باشند.

اکنون به ازای هر انتخاب y، چون $(y, 2^m) = 1$، یک x یکتا وجود دارد که در معادلهٔ فوق صدق می‌کند:

بنا بر این در این حالت تعداد جواب‌های معادلهٔ فوق برابر است با تعداد عناصر فرد $\mathbb{F}_2{}^m$، یعنی

$$2^{m-1}=(0+1)2^{m-1}$$

حالت دوم: $p(c) = i > 0$؛ در این صورت $c = 2^i q$ که در این‌جا q عددی فرد است. فرض کنیم زوج‌های

$$(h_r, k_r), \quad 1 \le r \le 2^{m-1},$$

2^{m-1} جواب معادلهٔ $q = hk \ mod \ 2^m$ باشند؛ ادعا می‌کنیم زوج‌های

$$(h_{r,j}, k_{r,j}), \quad 1 \le r \le 2^{m-1}, \ 1 \le j \le i,$$

با فرض

$$h_{r,j} = 2^j(h_r \ mod \ 2^{m-j}) = 2^j\left(h_r - 2^{m-j}\left\lfloor\frac{h_r}{2^{m-j}}\right\rfloor\right)$$

و

$$k_{r,j} = 2^{i-j}(k_r \ mod \ 2^{m-i+j}) = 2^{i-j}\left(k_r - 2^{m-i+j}\left\lfloor\frac{k_r}{2^{m-i+j}}\right\rfloor\right)$$

جواب‌های متمایز معادلهٔ $c = xy \ mod \ 2^m$ هستند. داریم:

$$h_{r,j}k_{r,j} = 2^j\left(h_r - 2^{m-j}\left\lfloor\frac{h_r}{2^{m-j}}\right\rfloor\right)2^{i-j}\left(k_r - 2^{m-i+j}\left\lfloor\frac{k_r}{2^{m-i+j}}\right\rfloor\right)$$

$$= 2^i h_r k_r - 2^{m-j+i}k_r\left\lfloor\frac{h_r}{2^{m-j}}\right\rfloor - 2^{m+j}h_r\left\lfloor\frac{k_r}{2^{m-i+j}}\right\rfloor + 2^{2m}\left\lfloor\frac{h_r}{2^{m-j}}\right\rfloor\left\lfloor\frac{k_r}{2^{m-i+j}}\right\rfloor$$

$$= 2^i q \ mod \ 2^m$$

بنا بر این معادلهٔ $c = xy \ mod \ 2^m$ حداقل دارای $(i+1)2^{m-1}$ جواب است. بالعکس، واضح است که هر جوابی از معادلهٔ $c = xy \ mod \ 2^m$ به‌شکل جواب‌های ارائه شده است. بنا بر این تعداد جواب‌های معادلهٔ $c = xy \ mod \ 2^m$ دقیقاً برابر $(i+1)2^{m-1}$ است.

اکنون کافی است مقدار $|f^{-1}(0)|$ را محاسبه کنیم. برای این منظور می‌توان مجموع تعداد جواب‌های پیشین را از 2^{2m} کسر کرد اما ما این محاسبه را مستقیم انجام می‌دهیم. معادلهٔ $xy = 0 \ mod \ 2^m$ را در نظر می‌گیریم. این دو حالت را داریم:

حالت اول: حداقل یک از دو مؤلفهٔ (x,y) صفر باشد. در این صورت جواب‌های $(i,0)$ و $(0,i)$ را به ازای

[Downloaded from jsci.khu.ac.ir on 2024-10-12]

$0 < i < 2^m$ به انضمام جواب $(0,0)$ داریم که تعداد آن‌ها برابر است با $1 + 2(2^m - 1) = 2^{m+1} - 1$.

حالت دوم: هیچ‌کدام از دو مؤلفهٔ (x, y) صفر نباشند؛ فرض کنیم $x = 2^t h$ و $y = 2^s k$ که در اینجا h و k اعدادی فرد هستند. واضح است که $s + t \geq m$. ابتدا توجه می‌کنیم که $x = 2^t h < 2^m$ و لذا $h < 2^{m-t}$ و چون h عددی فرد است، پس 2^{m-t-1} انتخاب برای h و لذا برای x داریم. به‌ترتیب مشابه، 2^{m-s-1} انتخاب برای k و لذا برای y داریم: بنا بر این تعداد جواب‌های بدون مؤلفهٔ صفر برابر است با مجموع جواب‌های به شکل

$$2^{m-t-1} \times 2^{m-s-1} = 2^{2m-2-(t+s)}.$$

با شرط $s + t \geq m$ بنا بر این باید مجموع ذیل را محاسبه کنیم:

$$\sum_{\substack{t+s\geq m \\ 0\leq t,s<m}} 2^{2m-2-(t+s)};$$

با تغییر متغیر $t + s = k$، برای هر $k = m, \dots, 2m-2$، $2m - k - 1$ انتخاب وجود دارد. با توجه به این مطلب داریم:

$$\begin{aligned}\sum_{\substack{t+s\geq m \\ 0\leq t,s<m}} 2^{2m-2-(t+s)} &= 2^{2m-2} \sum_{\substack{t+s\geq m \\ 0\leq t,s<m}} 2^{-(t+s)} \\ &= 2^{2m-2} \sum_{k=m}^{2m-2} (2m-k-1)2^{-k} = 2^{m-1} \sum_{k=1}^{m-1} (m-k)2^{-k} \\ &= 2^{m-1} \sum_{k=1}^{m-1} k2^{-m+k} = \frac{1}{2} \sum_{k=1}^{m-1} k2^k = m2^{m-1} - 2^m + 1\end{aligned}$$

روابط ذیل را می‌توان به‌وسیلهٔ روش‌های ترکیبیاتی یا استقرا به‌سادگی اثبات کرد:

$$\sum_{i=0}^{m-1} i2^{-i} = \frac{2^m - m - 1}{2^{m-1}} \tag{2}$$

$$\sum_{i=1}^{m-1} i2^i = 2(m2^{m-1} - 2^m + 1) \tag{3}$$

با توجه به مطالب فوق، داریم:

$$|f^{-1}(0)| = 2^{m+1} - 1 + m2^{m-1} - 2^m + 1 = 2^{m-1}(m+2)$$

لازم به ذکر است اگر در قضیهٔ ۱-۳، $z = f(x, y)$، آن‌گاه با نمادگذاری بخش ۲ داریم:

$$P(z = c) = \frac{p(c) + 1}{2^{m+1}}. \tag{4}$$

توزیع توابع مؤلفه‌ای ضرب پیمانه‌ای به‌عنوان یک تابع دودویی برداری

در این بخش، توزیع دوگانهٔ توابع مؤلفه‌ای عمل‌گر ضرب پیمانه‌ای به پیمانهٔ توانی از ۲ را به‌کمک توزیع برداری این عمل‌گر به‌دست می‌آوریم؛ همچنین، توزیع توابع مؤلفه‌ای این عمل‌گر را محاسبه می‌کنیم.

[Downloaded from jsci.khu.ac.ir on 2024-10-12]

با توجه به رابطهٔ (۴)، داریم:

$$P(z=c)=P(z_{m-1}=c_{m-1},\dots,z_0=c_0)=\frac{p(c)+1}{2^{m+1}} \tag{5}$$

که در این‌جا با توجه به نمادگذاری بخش ۲ داریم $c=(c_{m-1},\dots,c_0)$ و $z=(z_{m-1},\dots,z_0)$. بنا بر این، رابطهٔ (۵) توزیع m- گانهٔ بیت‌های خروجی ضرب پیمانه‌ای را به‌عنوان تابع دودویی برداری $f:\mathbb{F}_2{}^{2m}\to\mathbb{F}_2{}^{m}$ به‌دست می‌دهد. لم ذیل که برگرفته از مفهوم توزیع‌های حاشیه‌ای است، در اثبات قضایای آتی به‌طور وسیع استفاده می‌شود.

لم ۱-۴. فرض کنیم $x,y\in\mathbb{F}_2{}^{m}$ و $z=xy\ \ mod\ \ 2^m$؛ در این صورت برای هر $1\le r\le m$، هر $a\in\mathbb{F}_2{}^{r}$ با $a=(a_{r-1},\dots,a_0)$ و هر $(j_{r-1},\dots,j_0)$ با فرض $0\le j_0<\cdots<j_{r-1}<m$، داریم:

$$P\left(z_{j_{r-1}}=a_{r-1},\dots,z_{j_0}=a_0\right)=\sum_{\substack{0\le c<2^m\\ c_{j_k}=a_k\\ 0\le k<r}}P(z=c)$$

قضیه ۲-۴. فرض کنیم $x,y\in\mathbb{F}_2{}^{m}$ و $z=xy\ \ mod\ \ 2^m$؛ در این صورت برای هر $a,b\in\mathbb{F}_2$ و هر $0\le i<j<m$، داریم:

$$P\left(z_i=a,z_j=b\right)=\frac{1}{4}+\frac{(-1)^a}{2^{i+3}}+(1-a)\frac{(-1)^b}{2^{j+2}}$$

اثبات. ابتدا قرار می‌دهیم $a=b=0$. طبق رابطهٔ (4)، داریم:

$$\begin{aligned}
P\left(z_i=0,z_j=0\right)&=\sum_{\substack{c_i=0,c_j=0\\0\le c<2^m}}P(z=c)=\sum_{\substack{c_i=0,c_j=0\\0\le c<2^m}}\frac{p(c)+1}{2^{m+1}}\\
&=\sum_{p(c)=m+1}\frac{p(c)+1}{2^{m+1}}+\sum_{0\le p(c)<i}\frac{p(c)+1}{2^{m+1}}\\
&\quad+\sum_{i<p(c)<j}\frac{p(c)+1}{2^{m+1}}+\sum_{j<p(c)<m}\frac{p(c)+1}{2^{m+1}}\\
&=\frac{m+2}{2^{m+1}}+\sum_{0\le k<i}\frac{(k+1)}{2^{m+1}}2^{m-(k+3)}\\
&\quad+\sum_{i<k<j}\frac{(k+1)}{2^{m+1}}2^{m-(k+2)}+\sum_{j<k<m}\frac{(k+1)}{2^{m+1}}2^{m-(k+1)} \qquad (6)\\
&=\frac{m+2}{2^{m+1}}+\left(\frac{1}{4}-\frac{i+2}{2^{i+3}}\right)+\left(\frac{i+3}{2^{i+3}}-\frac{j+2}{2^{j+2}}\right)+\left(\frac{j+3}{2^{j+2}}-\frac{m+2}{2^{m+1}}\right) \qquad (7)\\
&=\frac{1}{4}+\frac{1}{2^{i+3}}+\frac{1}{2^{j+2}}
\end{aligned}$$

توجه کنید که تساوی (۶) از این حقیقت به‌دست آمده است که برای $0\le k<i$، به تعداد $2^{m-(k+3)}$ تا c، با شرط $p(c)=k$ و $c_i=c_j=0$ وجود دارد؛ به‌ازای $i<k<j$، به‌تعداد $2^{m-(k+2)}$ تا c، با شرط $p(c)=k$

[Downloaded from jsci.khu.ac.ir on 2024-10-12]

و $c_i = c_j = 0$ داریم و برای $j < k < n$ نیز، به‌تعداد $2^{m-(k+1)}$ تا c، با شرط $p(c) = k$ و $c_i = c_j = 0$ وجود دارد. همچنین، تساوی (۷) از رابطهٔ (۲) به‌دست آمده است.

حال اگر $a = 1$، آن‌گاه داریم:

$$\begin{aligned}
P(z_i = 1, z_j = b) &= \sum_{\substack{c_i=1, c_j=b \\ 0\le c<2^m}} P(z = c) = \sum_{\substack{c_i=1, c_j=b \\ 0\le c<2^m}} \frac{p(c)+1}{2^{m+1}} \\
&= \sum_{p(c)=i} \frac{p(c)+1}{2^{m+1}} + \sum_{0\le p(c)<i} \frac{p(c)+1}{2^{m+1}} \\
&= \frac{(i+1)}{2^{m+1}} 2^{m-(i+2)} + \sum_{0\le k<i} \frac{(k+1)}{2^{m+1}} 2^{m-(k+3)} \qquad (8) \\
&= \frac{1}{4} - \frac{1}{2^{i+3}} \qquad (9)
\end{aligned}$$

رابطهٔ (۸) مشابه رابطهٔ (۶) به‌دست می‌آید. تساوی (۹) نیز با استفاده از رابطهٔ (۲) به‌دست آمده است. سرانجام، اگر $a = 0, b = 1$، آن‌گاه داریم:

$$\begin{aligned}
P(z_i = 0, z_j = 1) &= \sum_{\substack{c_i=1, c_j=0 \\ 0\le c<2^m}} P(z = c) = \sum_{\substack{c_i=0, c_j=1 \\ 0\le c<2^m}} \frac{p(c)+1}{2^{m+1}} \\
&= \sum_{p(c)=j} \frac{p(c)+1}{2^{m+1}} + \sum_{0\le p(c)<i} \frac{p(c)+1}{2^{m+1}} + \sum_{i<p(c)<j} \frac{p(c)+1}{2^{m+1}} \\
&= \frac{(j+1)}{2^{m+1}} 2^{m-(j+1)} + \sum_{0\le k<i} \frac{(k+1)}{2^{m+1}} 2^{m-(k+3)} + \sum_{i<k<j} \frac{(k+1)}{2^{m+1}} 2^{m-(k+2)} \qquad (10) \\
&= \frac{1}{4} + \frac{1}{2^{i+3}} - \frac{1}{2^{j+2}}
\end{aligned}$$

تساوی (۱۰) مشابه دو حالت قبلی محاسبه می‌شود.

حال به بررسی توابع مؤلفه‌ای ضرب پیمانه‌ای می‌پردازیم و توزیع این توابع مؤلفه‌ای را محاسبه می‌کنیم.

قضیه ۳-۴. فرض کنیم $x, y \in \mathbb{F}_2{}^m$ و $z = xy \mod 2^m$؛ در این صورت برای هر $a \in \mathbb{F}_2$ و $0 \le i < m$، داریم:

$$P(z_i = a) = \frac{1}{2} + \frac{(-1)^a}{2^{i+2}}$$

اثبات. با توجه به قضیهٔ ۲-۴، اگر $0 \le i < m-1$، آن‌گاه داریم:

$$\begin{aligned}
P(z_i = a) &= P(z_i = a, z_{m-1} = 0) + P(z_i = a, z_{m-1} = 1) \\
&= \left(\frac{1}{4} + \frac{(-1)^a}{2^{i+3}} + (1-a)\frac{(-1)^0}{2^{m+1}}\right) + \left(\frac{1}{4} + \frac{(-1)^a}{2^{i+3}} + (1-a)\frac{(-1)^1}{2^{m+1}}\right) = \frac{1}{2} + \frac{(-1)^a}{2^{i+2}}
\end{aligned}$$

برای $i = m-1$ نیز داریم:

$$P(z_{m-1} = a) = P(z_0 = 0, z_{m-1} = a) + P(z_0 = 1, z_{m-1} = a)$$

[Downloaded from jsci.khu.ac.ir on 2024-10-12]

$$= \left(\frac{1}{4} + \frac{(-1)^0}{2^3} + (1-0)\frac{(-1)^a}{2^{m+1}}\right) + \left(\frac{1}{4} + \frac{(-1)^1}{2^3} + (1-1)\frac{(-1)^a}{2^{m+1}}\right)$$
$$= \frac{1}{2} + \frac{(-1)^a}{2^{m+1}}$$

ناترازی ضرب پیمانه‌ای و توابع مؤلفه‌ای آن

در طراحی و تحلیل توابع دودویی برداری، یکی از مهم‌ترین موارد، بررسی تراز بودن توابع است. به وضوح، ضرب پیمانه‌ای به پیمانهٔ توانی از ۲ تابعی تراز نیست: تا کنون به بررسی میزان ناترازی نگاشت‌ها و ارائهٔ معیارهایی برای محاسبهٔ میزان ناترازی نگاشت‌ها پرداخته نشده است. در این بخش، ما به ارائهٔ یک سنج یا معیار برای اندازه‌گیری ناترازی نگاشت‌ها می‌پردازیم و به‌کمک آن، ناترازی ضرب پیمانه‌ای و توابع مؤلفه‌ای آن را به‌دست می‌آوریم.

تعریف ۱-۵ [۵]. فرض کنیم P_1 و P_2، دو توزیع روی یک فضای نمونه‌ای متناهی $\mathcal{X}$ باشند. در این صورت فاصلهٔ آن‌ها، $D(P_1, P_2)$، بدین‌صورت تعریف می‌شود:

$$D(P_1, P_2) = \sum_{x \in \mathcal{X}} |P_1(x) - P_2(x)|$$

حال برای تابع $f: A \to B$، با فرض $|A| = n$، $|B| = m$ و $n = dm$، توزیع P_1 را روی B، بدین‌صورت در نظر می‌گیریم:

$$\forall b \in B, \quad P_1(b) = \frac{|f^{-1}(b)|}{n} \tag{11}$$

و توزیع P_2 را روی B، توزیع یک‌نواخت در نظر می‌گیریم. یعنی

$$\forall b \in B, \quad P_2(b) = \frac{d}{n} \tag{12}$$

بر این اساس، تعریف ذیل را انجام می‌دهیم.

تعریف ۲-۵. ناترازی D_f را برای تابع $f: A \to B$، با شرط $|A| = n$، $|B| = m$ و $n = dm$، با استفاده از تعریف ۱-۵ و روابط (۱۱) و (۱۲)، به‌صورت ذیل تعریف می‌کنیم:

$$D_f = \frac{2(m-1)}{m} D(P_1, P_2) = \frac{\sum_{b \in B} \left| |f^{-1}(b)| - d \right|}{2(m-1)d}.$$

لم ۳-۵. برای هر تابع $f: A \to B$، با شرط $|A| = n$، $|B| = m$ و $n = dm$، داریم:

$$0 \le D_f \le 1$$

اثبات. واضح است که برای هر تابع تراز f داریم $D_f = 0$؛ از طرفی طبق تعریف ۲-۵ روشن است که برای هر تابع f، $0 \le D_f$. لذا کافی است نشان دهیم که برای هر تابع f، $D_f \le 1$. برای این منظور فرض می‌کنیم $C = \{b \in B \mid |f^{-1}(b)| \ge d\}$؛ در این صورت داریم:

$$D_f = \frac{1}{2(m-1)d} \left(\sum_{b \in C} (|f^{-1}(b)| - d) + \sum_{b \in \bar{C}} (d - |f^{-1}(b)|) \right)$$

[Downloaded from jsci.khu.ac.ir on 2024-10-12]

$$= \frac{1}{2(m-1)d}\left(|\bar{C}|d - |C|d + \sum_{b\in C}|f^{-1}(b)| - \sum_{b\in \bar{C}}|f^{-1}(b)|\right)$$

$$= \frac{1}{2(m-1)d}\left((m-|C|)d - |C|d + |f^{-1}(C)| - |f^{-1}(\bar{C})| \right)$$

$$= \frac{|f^{-1}(C)| - |C|d}{(m-1)d} \qquad (13)$$

از آن‌جا که $|C| = 0$ به تناقض منجر می‌شود، داریم $|C| \geq 1$؛ از سوی دیگر $|f^{-1}(c)| \leq n$. از این رو

$$D_f = \frac{|f^{-1}(C)| - |C|d}{(m-1)d} \leq \frac{n-d}{(m-1)d} = 1.$$

نیز توجه داریم که برای هر تابع ثابت f داریم:

$$D_f = \frac{(m-1)d + (n-d)}{2(m-1)d} = \frac{(m-1)d + (md-d)}{2(m-1)d} = \frac{2(m-1)d}{2(m-1)d} = 1. \qquad \blacksquare$$

اکنون میزان ناترازی ضرب پیمانه‌ای را به‌دست می‌آوریم.

قضیه ۴-۵. اگر ضرب پیمانه‌ای به هنگ 2^m را به عنوان تابع $f: \mathbb{F}_2{}^{2m} \to \mathbb{F}_2{}^{m}$ با تعریف $f(x,y) = xy \mod 2^m$ در نظر بگیریم، آن‌گاه داریم:

$$D_f = \frac{2^{m-2}}{2^m - 1}.$$

اثبات. با توجه به تعریف D_f، اثبات قضیه ۱-۳ و روابط (۲) و (۳) داریم:

$$D_f = \frac{\sum_{b\in\mathbb{F}_2^m}\left||f^{-1}(b)| - 2^m\right|}{2(2^m-1)2^m}$$

$$= \frac{m2^{m-1} + 2^{2m-2} + \sum_{i=1}^{m-1}(2^{m-i-1})(i-1)2^{m-1}}{2^{m+1}(2^m-1)}$$

$$= \frac{m2^{m-1} + 2^{2m-2} + 2^{2m-2}(\sum_{i=1}^{m-1} i2^{-i} - \sum_{i=1}^{m-1} 2^{-i})}{2^{m+1}(2^m-1)}$$

$$= \frac{m + 2^{m-1} + 2^{m-1}(\sum_{i=0}^{m-1} i2^{-i} - \sum_{i=1}^{m-1} 2^{-i})}{4(2^m-1)}$$

$$= \frac{m + 2^{m-1} + 2^{m-1}(\frac{2^m - m - 1}{2^{m-1}} - \frac{2^{m-1}-1}{2^{m-1}})}{4(2^m-1)}$$

$$= \frac{m + 2^{m-1} + 2^m - m - 1 - 2^{m-1} + 1}{4(2^m-1)} = \frac{2^{m-2}}{2^m-1}$$

توجه داریم قضیهٔ ۴-۵ بیان می‌دارد که میزان ناترازی مجانبی توابع ضرب پیمانه‌ای به‌عنوان یک تابع دودویی برداری برابر است با ۰/۲۵. در ادامه، به بررسی ناترازی توابع مؤلفه‌ای می‌پردازیم و ثابت می‌کنیم ناترازی مجانبی بالاترین توابع مؤلفه‌ای، بسیار کم‌تر از ناترازی این تابع به‌عنوان یک تابع دودویی برداری است.

قضیه ۵-۵. اگر ضرب پیمانه‌ای به پیمانهٔ 2^m را به‌عنوان تابع $f: \mathbb{F}_2{}^{2m} \to \mathbb{F}_2{}^{m}$ با توابع مؤلفه‌ای $(f_{m-1}, \dots, f_0)$ در نظر بگیریم، آن‌گاه ناترازی تابع توأم دودویی $f_{i,j}$ ، $i < j$، برابر است با

[Downloaded from jsci.khu.ac.ir on 2024-10-12]

$$D_{f_{i,j}} = \frac{1}{3 \times 2^i}.$$

اثبات. داریم:

$$D_{f_{i,j}} = \frac{\left|\left|f_{i,j}^{-1}(0,0)\right| - 2^{2m-2}\right| + \left|\left|f_{i,j}^{-1}(0,1)\right| - 2^{2m-2}\right| + \left|\left|f_{i,j}^{-1}(1,0)\right| - 2^{2m-2}\right| + \left|\left|f_{i,j}^{-1}(1,1)\right| - 2^{2m-2}\right|}{2(2^2-1)2^{2m-2}}$$

$$= \frac{(2^{2m-i-3} + 2^{2m-j-2}) + (2^{2m-i-3} - 2^{2m-j-2}) + (2^{2m-i-3}) + (2^{2m-i-3})}{3 \times 2^{2m-1}}$$

$$= \frac{4 \times 2^{2m-i-3}}{3 \times 2^{2m-1}} = \frac{1}{3 \times 2^i}$$

نتیجه ۶-۵. ناترازی مجانبی بالاترین تابع مؤلفه‌ای توأم عمل‌گر ضرب پیمانه‌ای، برابر صفر است.

قضیه ۷-۵. اگر ضرب پیمانه‌ای به پیمانهٔ 2^m را به‌عنوان تابع $f: \mathbb{F}_2{}^{2m} \to \mathbb{F}_2{}^m$ با توابع مؤلفه‌ای $(f_{m-1}, \dots, f_0)$ در نظر بگیریم، آن‌گاه ناترازی تابع دودویی مؤلفه‌ای i- ام برابر است با

$$D_{f_i} = \frac{1}{2^{i+1}}.$$

اثبات. داریم:

$$D_{f_i} = \frac{\left|\left|f_i^{-1}(0)\right| - 2^{2m-1}\right| + \left|\left|f_i^{-1}(1)\right| - 2^{2m-1}\right|}{2(2-1)2^{2m-1}} = \frac{(2^{2m-i-2}) + (2^{2m-i-2})}{2^{2m}} = \frac{1}{2^{i+1}}$$

نتیجه ۸-۵. ناترازی مجانبی بالاترین تابع مؤلفه‌ای عمل‌گر ضرب پیمانه‌ای به پیمانهٔ توانی از ۲، برابر صفر است.

درجهٔ جبری توابع مؤلفه‌ای ضرب پیمانه‌ای

در طراحی و تحلیل رمزهای متقارن، اطلاع از درجهٔ جبری توابع دودویی اهمیت زیادی دارد [۶]. در این بخش ما ابتدا قضیه‌ای را در زمینهٔ درجهٔ جبری توابع مؤلفه‌ای ضرب پیمانه‌ای، بدون اثبات، می‌آوریم: برای مشاهدهٔ اثبات این قضیه می‌توانید به [۳] مراجعه کنید. سپس به‌کمک این قضیه، کرانی پایین برای درجهٔ توابع مؤلفه‌ای ضرب پیمانه‌ای ارائه می‌دهیم.

قضیه ۱-۶. فرض کنیم $u \epsilon \mathbb{Z}_{2^m}$ و $f: \mathbb{F}_2{}^m \to \mathbb{F}_2$ با تعریف $f(x) = x^u$ یک تابع دودویی باشد؛ در این صورت، ANF تابع دودویی $f(xy)$ (ضرب به هنگ 2^m محاسبه می‌شود) به‌صورت ذیل خواهد بود:

$$f(xy) = \bigoplus_{\substack{\sum_{i=0}^{m-1} k_i 2^i = u \\ k_i \geq 0, 0 \leq i \leq m}} x^{a(k_{m-1},\dots,k_0)} y^{b(k_{m-1},\dots,k_0)} \tag{14}$$

که در اینجا $k_i = (k_{i,m-1}, \dots, k_{i,0})$، $0 \leq i < m$ و

$$a(k_{m-1}, \dots, k_0) = \sum_{i=0}^{m-1} a_i(k_{m-1}, \dots, k_0)\, 2^i, \qquad b(k_{m-1}, \dots, k_0) = \sum_{i=0}^{m-1} b_i(k_{m-1}, \dots, k_0)\, 2^i$$

[Downloaded from jsci.khu.ac.ir on 2024-10-12]

$$a_i(k_{m-1},\dots,k_0)=\begin{cases}0 & (k_{m-1,i},\dots,k_{0,i})=(0,\dots,0)\\ 1 & (k_{m-1,i},\dots,k_{0,i})\neq(0,\dots,0)\end{cases},\qquad b_i(k_{m-1},\dots,k_0)=\begin{cases}0 & k_i=0\\ 1 & k_i\neq 0\end{cases}.$$

مثال ۲-۶. عناصر $\mathbb{Z}_8$ را به‌صورت بردارهای $x=(x_2,x_1,x_0)$ و $y=(y_2,y_1,y_0)$ در نظر می‌گیریم و قرار می‌دهیم $g(x,y)=f(xy)$ که در اینجا $g=(g_2,g_1,g_0)$ و

$$f(z)=z^4 \quad\equiv\quad f(z_2,z_1,z_0)=(z_2,z_1,z_0)^{(1,0,0)}=z_2$$

و ضرب، به پیمانهٔ ۸ انجام می‌شود. در این صورت g_2، معرف بالاترین تابع مؤلفه‌ای ضرب پیمانه‌ای به هنگ ۸ می‌باشد. از آنجا که چهار مجموعه جواب

$$(k_2,k_1,k_0)=(1,0,0)\ ،(k_2,k_1,k_0)=(0,2,0)\ ،(k_2,k_1,k_0)=(0,1,2)\ ،(k_2,k_1,k_0)=(0,0,4)$$

تمام مجموعه جواب‌های معادلهٔ (۱۴) است، ANF بالاترین تابع مؤلفه‌ای ضرب پیمانه‌ای به هنگ ۸ به‌صورت ذیل است:

$$g_2(y_2,y_1,y_0,x_2,x_1,x_0)=x^4y^1\oplus x^3y^3\oplus x^2y^2\oplus x^1y^4$$
$$=x_2y_0\oplus x_0x_1y_0y_1\oplus x_1y_1\oplus x_0y_2$$

و داریم $d(g_2)=4$.

به‌وسیلهٔ قضیه ۱-۶، می‌توان درجهٔ توابع دودویی مؤلفه‌ای ضرب پیمانه‌ای به پیمانهٔ 2^m را بررسی کرد؛ اگر به ازای $q=2^0,2^1,\dots,2^{m-1}$، قرار دهیم $f(x)=x^q$، آن‌گاه درجهٔ توابع $f(xy)$ همان درجهٔ توابع مؤلفه‌ای ضرب پیمانه‌ای به پیمانهٔ 2^m خواهد بود.

قضیه ۳-۶. اگر ضرب پیمانه‌ای به پیمانهٔ 2^m را به‌عنوان تابع $f:\mathbb{F}_2{}^{2m}\to\mathbb{F}_2{}^{m}$ با توابع مؤلفه‌ای $(f_{m-1},\dots,f_0)$ در نظر بگیریم، آن‌گاه داریم:

$$d(f_i)\geq i+1. \tag{15}$$

اثبات. به سادگی می‌توان تحقیق کرد که درجهٔ دو تابع مؤلفه‌ای اول برابر ۲ است که در نامساوی (۱۵) صادق است. در ادامهٔ اثبات i را بزرگ‌تر از ۱ در نظر می‌گیریم. برای اثبات نامساوی (۱۵) کافی است یک جواب برای معادلهٔ $\sum_{r=0}^{m-1}k_r2^r=2^i$ به دست آوریم و سپس ثابت کنیم که جملهٔ متناظر با این جواب در ANF تابع مؤلفه‌ای i- ام، با جملهٔ دیگری که در رابطهٔ (۱۴) صدق کند، ساده نمی‌شود. جواب

$$(k_{m-1},\dots,k_i,k_{i-1},\dots,k_1,k_0)=(0,\dots,0,1,\dots,1,2)$$

را در نظر می‌گیریم. به سادگی می‌توان تحقیق کرد که درجهٔ جبری جملهٔ متناظر با جواب ارائه شده برابر است با $i+1$. این جواب منحصر به فرد است، یعنی جواب دیگری وجود ندارد که جملهٔ متناظر با آن، جملهٔ متناظر با جواب ارائه شده را خنثی نماید: در واقع، اگر هر جواب متفاوت دیگری را در نظر بگیریم، آن‌گاه

$$\sum_{r=0}^{m-1}k_r2^r>2^i$$

که تناقض است؛ بنا بر این درجه تابع مؤلفه‌ای i- ام، حداقل برابر است با $i+1$.

[Downloaded from jsci.khu.ac.ir on 2024-10-12]

نتیجه‌گیری

در این مقاله، به بررسی خواص آماری و جبری عمل‌گر ضرب پیمانه‌ای به پیمانهٔ توانی از ۲ پرداختیم. در ابتدا توزیع خروجی عمل‌گر ضرب پیمانه‌ای به پیمانهٔ توانی از ۲ را، به‌عنوان یک تابع دودویی برداری، محاسبه کردیم و پس از آن، توزیع توابع مؤلفه‌ای آن را به‌دست آوردیم. پس از آن، با معرفی یک سنج در اندازه‌گیری میزان ناترازی نگاشت‌ها، به بررسی ناترازی این عمل‌گر و توابع مؤلفه‌ای آن پرداختیم و در پایان، درجهٔ جبری توابع مؤلفه‌ای عمل‌گر ضرب پیمانه‌ای به پیمانهٔ توانی از ۲ را بررسی کردیم و یک کران پایین برای درجات مذکور ارائه دادیم.

ثابت کردیم ناترازی مجانبی عمل‌گر ضرب پیمانه‌ای به پیمانهٔ توانی از ۲، به‌عنوان یک تابع دودویی برداری، برابر ۰/۲۵ است اما ناترازی مجانبی بالاترین تابع مؤلفه‌ای و بالاترین تابع مؤلفه‌ای توأم این عمل‌گر برابر صفر است؛ بنا بر این می‌توان گفت که گرچه عمل‌گر ضرب پیمانه‌ای به هنگ توانی از دو به‌عنوان یک تابع دودویی برداری، ناتراز است، در مقابل، بالاترین تابع مؤلفه‌ای و بالاترین تابع مؤلفه‌ای توأم آن تقریباً تراز هستند.

با استفاده از کران ارائه شده در این مقاله، می‌توان گفت که بالاترین تابع خروجی ضرب پیمانه‌ای به پیمانهٔ توانی از ۲ از درجهٔ جبری نسبتاً بالایی برخوردار است. در ادامـهٔ تحقیقات این مقاله می‌توان به بررسی توزیع چندگانهٔ توابع مؤلفه‌ای خروجی عمل‌گر ضرب پیمانه‌ای به پیمانهٔ توانی از ۲ و ناترازی آن‌ها و نیز محاسبهٔ دقیق درجهٔ جبری توابع مؤلفه‌ای آن پرداخت.

منابع

1. C. Burwick, D. Coppersmith, E. D'Avignon, R. Gennaro, S. Halevi, C. Jutla, S.M. Matyas Jr., L. O'Connor, M. Peyravian, D. Safford and N. Zunic, "MARS: a candidate cipher for AES", Presented in the 1st AES conference, CA, USA, August (1998).
2. C. Berbain, O. Billet, A. Canteaut, N. Courtois, B. Debraize, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin, and H. Sibert, "Sosemanuk, a Fast Software-Oriented Stream Cipher", In New Stream Cipher Designs-The eSTREAM Finalists, LNCS 4986 (2008) 98-118, Springer-Verlag .
3. A. Braeken, I. Semaef, "The ANF of Composition of Addition and Multiplication mod 2^n with a Boolean Function", FSE'05, LNCS 3557 (2005) 112-125, Springer-Verlag.
4. Claude Carlet, "Boolean functions for Cryptography and Error Correcting Codes", available via http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.107.2986&rep=rep1&type=pdf
5. T. M. Cover and J. A. Thomas, "Elements of Information Theory", Second Edition, John Wiley & Sons (2006).
6. N. Courtois, "Algebraic attacks on combiners with memory and several outputs", In: Park, C., Chee, S. (eds.) Information Security and Cryptology -ICISC (2004).

[Downloaded from jsci.khu.ac.ir on 2024-10-12]