هشتمین کنفرانس بین‌المللی انجمن رمز ایران
دانشگاه فردوسی مشهد - ۲۳ و ۲۴ شهریور ۱۳۹۰

ویژگی‌های رمزنگاری عملگر جمع پیمانه‌ای، به هنگ توانی از ۲

سید مجتبی دهنوی[۱]، اکبر محمودی ریشکانی[۲]، حمید رضا میمنی[۳]

[۱] دانشگاه تربیت معلم، تهران
dehnavism@tmu.ac.ir

[۲] دانشگاه شهید بهشتی، تهران
am_rishakani@yahoo.com

[۳] دانشگاه تربیت دبیر شهید رجایی، تهران
maimani@ipm.ir

چکیده

در این مقاله، به بررسی جمع پیمانه‌ای به پیمانه‌ی توانی از ۲ می‌پردازیم؛ در ابتدا، توزیع بیت‌های نقلی را به دست می‌آوریم و پس از آن، توزیع توأم و چندگانه‌ی بردار بیت‌های نقلی را محاسبه می‌کنیم. ما، دو سنج در اندازه‌گیری فاصله‌ی توابع دودویی برداری، تعریف می‌کنیم و بر اساس آن، تقریب جمع پیمانه‌ای با XOR بیتی را مورد بررسی قرار می‌دهیم. بررسی پارامترهای خطی و تفاضلی توابع دودویی برداری، اهمیت بالایی در رمزنگاری دارد؛ به همین منظور، ما پارامترهای خطی وتفاضلی این عملگر را نیز به عنوان یک تابع دودویی برداری بررسی می‌کنیم. در پایان، درجه‌ی جبری بیت نقلی و تعداد جملات در ANF تابع دودویی معرف بیت نقلی را به دست می‌آوریم.

کلمات کلیدی

جمع پیمانه‌ی به پیمانه‌ی توانی از ۲، توابع مؤلفه‌ای، بیت‌های نقلی، درجه‌ی جبری، پارامترهای خطی وتفاضلی

۱- مقدمه

یکی از عملگرهایی که تاکنون کاربردهای بسیاری را در رمزنگاری متقارن داشته، جمع پیمانه‌ای به پیمانه‌ی 2^n است که در اینجا n عددی صحیح و مثبت و معمولاً برابر اندازه‌ی پردازنده‌های نوعی - یعنی ۸، ۱۶، ۳۲ و یا ۶۴ - می‌باشد. به عنوان مثال، این عملگر در رمزهای دنباله‌ای Bluetooth [2] و RC4 [6] و نیز در رمزهای قالبی RC6 [5]، Towfish [7] و Mars [4] به کار رفته است.

ما در این مقاله، ابتدا به بررسی توزیع بیت نقلی[۱] جمع پیمانه‌ای به پیمانه‌ی توانی از ۲ می‌پردازیم و علاوه بر به دست آوردن توزیع بیت‌های نقلی، توزیع توأم و چندگانه‌ی بردار بیت‌های نقلی را نیز به دست می‌آوریم. همچنین، تقریب جمع پیمانه‌ای با XOR بیتی را مورد بررسی قرار می‌دهیم و پس از تعریف دو سنج در تعیین فاصله‌ی دو تابع دودویی برداری، فاصله‌ی جمع پیمانه‌ای با XOR بیتی را محاسبه می‌کنیم. پس از آن، ویژگی‌های خطی و تفاضلی این عملگر را بررسی می‌کنیم و پس از اثبات یک قضیه، پارامترهای خطی توابع دودویی مؤلفه‌ای[۲] این عملگر را، که به کمک برنامه‌نویسی به دست آورده‌ایم، ارائه می‌کنیم. در پایان، به بررسی خواص جبری بیت نقلی می‌پردازیم و درجه‌ی جبری و تعداد جملات در ANF[۳] تابع دودویی معرف بیت نقلی را به دست می‌آوریم.

در بخش ۲ به بیان تعاریف و اصطلاحات می‌پردازیم. بخش ۳ به بررسی توزیع بیت‌های نقلی و توزیع‌های توأم و چندگانه‌ی آنها می‌پردازد. در بخش ۴ ویژگی‌های خطی و تفاضلی جمع پیمانه‌ای را مورد بررسی قرار می‌دهیم. بخش ۵ به خواص جبری بیت نقلی اختصاص دارد و در پایان در بخش ۶ به نتیجه‌گیری می‌پردازیم.

۲- تعاریف و اصطلاحات

در این مقاله، تعداد عناصر مجموعه‌ی متناهی A را با $|A|$ نشان می‌دهیم. برای تابع $f:A\to B$، نقش معکوس یک عنصر $b\in B$ را به صورت $\{a\in A|\ f(a)=b\}$ تعریف کرده، با $f^{-1}(b)$ نشان می‌دهیم. وزن همینگ یک عدد طبیعی یا بردار x را با $w(x)$ و فاصله‌ی همینگ دو عدد یا بردار x و y را با $d(x,y)$ نشان می‌دهیم. عملگر AND را نیز با "$\wedge$" نمایش می‌دهیم.

فرض کنیم F_2 میدان متناهی با دو عضو باشد؛ دراین صورت، هر عضو ${F_2}^n$ (حاصل ضرب دکارتی n نسخه از F_2) را می‌توان به صورت یک بردار در نظر گرفت. با توجه به تعریف ${F_2}^n$، یک تناظر یک‌به‌یک بین ${F_2}^n$ و Z_{2^n}، حلقه‌ی اعداد صحیح به پیمانه‌ی 2^n، برقرار است که به صورت ذیل تعریف می‌شود:

$$\varphi:{F_2}^n\to Z_{2^n}$$
$$x=(x_{n-1},\dots,x_0)\mapsto\varphi(x)=\sum_{i=0}^{n-1}x_i\,2^i$$

حال، ترتیب جزیی $\prec$ را روی ${F_2}^n$ به صورت زیر تعریف می‌کنیم:

$$x\prec a\ \Leftrightarrow\ x_i\le a_i,\ 0\le i<n$$

با نمادگذاری فوق اگر

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

آنگاه x^u را به صورت ${x_0}^{u_0}\dots{x_{n-1}}^{u_{n-1}}$ تعریف می‌کنیم.

هر تابع f به صورت $f:{F_2}^n\to F_2$ را یک تابع دودویی می‌نامیم. فرض کنید f تابعی دودویی باشد؛ f را می‌توان به شکلی یکتا که آن را شکل نرمال جبری یا ANF می‌نامیم، نمایش داد. در واقع، داریم:

$$f(x)=\bigoplus_{u\in Z_{2^n}}h_u x^u,\quad h_u\in F_2$$

که ضرایب h_u به صورت زیر تعیین می‌شوند:

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

درجه جبری تابع f، که با $\deg(f)$ نمایش داده می‌شود، برابر با تعداد متغیرها در طولانی‌ترین جمله‌ی شکل نرمال جبری است؛ به طور معادل، $\deg(f)$ بیشترین مقدار $w(u)$، در میان $h_u\neq 0$ ها تعریف می‌شود.

هر تابع $f:{F_2}^m\to{F_2}^n$، با $n>1$ را تابع دودویی برداری یا S-box می‌نامیم. چنین تابعی را می‌توان به وسیله‌ی بردار $(f_{n-1},f_1,\dots,f_0)$ از توابع بیان کرد: هر f_i، $0\le i<n$، یک تابع دودویی $f_i:{F_2}^m\to F_2$ است که به آن تابع مؤلفه‌ای i-ام می‌گوییم.

برای یک نگاشت دودویی $f:{F_2}^m\to F_2$، توابع دودویی f_a را به صورت ذیل تعریف می‌کنیم:

$$f_a(x)=\begin{cases}0 & f(x)=a.x\\ 1 & f(x)\neq a.x\end{cases}$$

که در تعریف فوق، "$.$" به معنای ضرب داخلی است و $a\in F_2^m$؛ به عبارت دیگر، داریم:

$$a.x=(a_{m-1},\dots,a_0).(x_{m-1},\dots,x_0)=\bigoplus_{i=0}^{m-1}a_i x_i$$

و c_f را به صورت

$$\max_{\substack{a\in F_2^m\\ a\neq 0}}\left(4\left(\frac{|f^{-1}(0)|-2^{m-1}}{2^m}\right)^2\right)$$

تعریف می‌کنیم. همچنین، توابع دودویی f^a را به صورت ذیل تعریف می‌کنیم:

$$f^a(x)=\begin{cases}0 & f(x)=f(x\oplus a)\\ 1 & f(x)\neq f(x\oplus a)\end{cases}$$

و d_f را به صورت

$$\max_{\substack{a\in F_2^m\\ a\neq 0}}\frac{|\{x|\ f^a(x)=0\}|}{2^m}$$

تعریف می‌کنیم.

c_f و d_f، در واقع، همان پارامترهای خطی و تفاضلی S-box f $m\times 1$ می‌باشند.

برای دو تابع دودویی برداری $f,g:F_2^m\to F_2^n$ احتمال تساوی $P_{f,g}$ را به صورت

$$P_{f,g}=\frac{|\{x\in F_2^m\mid f(x)=g(x)\}|}{2^m}$$

تعریف می‌کنیم و امید تعداد بیت‌های مساوی $E_{f,g}$ را به صورت

$$E_{f,g}=\frac{\sum_{x\in F_2^m}d(f(x),g(x))}{2^m}$$

$$= \frac{\sum_{i=0}^{n-1} |\{x \in F_2^m \mid f_i(x) = g_i(x)\}|}{2^m}$$

تعریف می‌کنیم که در بالا، f_i و g_i ها، $0 \le i < n$، توابع مؤلفه‌ای توابع f و g می‌باشند.

۳- توزیع بیت‌های نقلی

می‌دانیم که اگر جمع پیمانه‌ای را به صورت تابع دودویی برداری $f : F_2^{2n} \to F_2^n$ با $f(x,y) = z$ یا $z = x + y \mod 2^n$ در نظر بگیریم، داریم:

$$\begin{aligned} z_0 &= x_0 \oplus y_0 \oplus c_0, \quad c_0 = 0 \\ z_i &= x_i \oplus y_i \oplus c_i, \quad c_i = x_{i-1}y_{i-1} \oplus c_{i-1}(x_{i-1} \oplus y_{i-1}) \end{aligned} \qquad (1)$$

که در اینجا، داریم:

$$x = (x_{n-1},\ldots,x_0),\ y = (y_{n-1},\ldots,y_0),\ z = (z_{n-1},\ldots,z_0).$$

قضیه ۳-۱: اگر $x = (x_{n-1},\ldots,x_0)$ و $y = (y_{n-1},\ldots,y_0)$، آنگاه داریم:

$$x + y = (x \oplus y) + 2(x \wedge y) \bmod 2^n \qquad (2)$$

اثبات: فرض کنیم $z = (z_{n-1},\ldots,z_0)$ با $z = x + y \bmod 2^n$ و نیز فرض کنیم که $a = x \oplus y$ با $a = (a_{n-1},\ldots,a_0)$ و $b = 2(x \wedge y)$ با $b = (b_{n-1},\ldots,b_0)$ و $c = a + b \mod 2^n$ با $c = (c_{n-1},\ldots,c_0)$، آنگاه داریم $z_i = x_i \oplus y_i \oplus d_i$، $0 \le i < n$، با $d_0 = 0$ و

$$d_i = x_{i-1}y_{i-1} \oplus d_{i-1}(x_{i-1} \oplus y_{i-1}) \quad 0 < i < n$$

همچنین، داریم $b_0 = 0$ و $b_i = x_{i-1}y_{i-1}$، $0 < i < n$، و $a_i = x_i \oplus y_i$، $0 \le i < n$، و نیز داریم $c_i = a_i \oplus b_i \oplus e_i$، $0 \le i < n$، با $e_0 = 0$ و

$$e_i = a_{i-1}b_{i-1} \oplus e_{i-1}(a_{i-1} \oplus b_{i-1}) \quad 0 < i < n$$

ابتدا ثابت می‌کنیم

$$e_i = d_i \oplus x_{i-1}y_{i-1} \quad 0 < i < n$$

از استقرا روی i استفاده می‌کنیم؛ به ازای $i = 1$ داریم:

$$\begin{aligned} d_1 &= x_0y_0 \oplus d_0(x_0 \oplus y_0) = x_0y_0 \\ e_1 &= a_0b_0 \oplus e_0(a_0 \oplus b_0) = a_0b_0 = 0 \end{aligned}$$

و لذا داریم $e_1 = d_1 \oplus x_0y_0$؛ حال، اگر حکم به ازای $i-1$ صحیح باشد، آنگاه، داریم:

$$\begin{aligned} e_i \oplus x_{i-1}y_{i-1} &= a_{i-1}b_{i-1} \oplus e_{i-1}(a_{i-1} \oplus b_{i-1}) \oplus x_{i-1}y_{i-1} \\ &= (x_{i-1} \oplus y_{i-1})x_{i-2}y_{i-2} \oplus \\ &\quad (d_{i-1} \oplus x_{i-2}y_{i-2})(x_{i-1} \oplus y_{i-1} \oplus x_{i-2}y_{i-2}) \oplus x_{i-1}y_{i-1} \\ &= (x_{i-1} \oplus y_{i-1})x_{i-2}y_{i-2} \oplus d_{i-1}(x_{i-1} \oplus y_{i-1}) \oplus d_{i-1}x_{i-2}y_{i-2} \\ &\quad \oplus x_{i-2}y_{i-2}(x_{i-1} \oplus y_{i-1}) \oplus x_{i-2}y_{i-2} \oplus x_{i-1}y_{i-1} \\ &= (x_{i-1}y_{i-1} \oplus d_{i-1}(x_{i-1} \oplus y_{i-1})) \oplus d_{i-1}x_{i-2}y_{i-2} \oplus x_{i-2}y_{i-2} \\ &= d_i \oplus d_{i-1}x_{i-2}y_{i-2} \oplus x_{i-2}y_{i-2} = d_i \end{aligned}$$

تساوی اخیر، از ضرب دو طرف تساوی

$$d_{i-1} = x_{i-2}y_{i-2} \oplus d_{i-2}(x_{i-2} \oplus y_{i-2})$$

در $x_{i-2}y_{i-2}$ به دست می‌آید:

$$\begin{aligned} d_{i-1}x_{i-2}y_{i-2} &= x_{i-2}y_{i-2} \oplus d_{i-2}x_{i-2}y_{i-2} \oplus d_{i-2}x_{i-2}y_{i-2} \\ &= x_{i-2}y_{i-2} \end{aligned}$$

حال، می‌توان ثابت کرد که $c = z$؛ داریم:

$$\begin{aligned} c_0 &= a_0 \oplus b_0 \oplus e_0 = a_0 \oplus b_0 = x_0 \oplus y_0 \\ &= x_0 \oplus y_0 \oplus d_0 = z_0 \end{aligned}$$

و برای $i > 0$ نیز داریم:

$$\begin{aligned} c_i &= a_i \oplus b_i \oplus e_i \\ &= (x_i \oplus y_i) \oplus x_{i-1}y_{i-1} \oplus d_i \oplus x_{i-1}y_{i-1} \\ &= x_i \oplus y_i \oplus d_i = z_i \end{aligned}$$

با توجه به قضیه 3-1، می‌توان احتمال تساوی تابع جمع پیمانه‌ای به پیمانه‌ی 2^n با XOR بیتی، یا به تعبیر دیگر، تقریب جمع پیمانه‌ای با XOR بیتی را به دست آورد؛ در واقع، در تساوی (2)، کافی است که $2(x \wedge y) = 0$ برقرار باشد؛ با یک استدلال ترکیبیاتی ساده می‌توان دید که اگر تابع f معرف جمع پیمانه‌ای به پیمانه‌ی 2^n و تابع g معرف تابع XOR بیتی باشد، داریم:

$$P_{f,g} = \left(\frac{3}{4}\right)^{n-1}$$

قضیه ۳-۲: اگر $x = (x_{n-1},\ldots,x_0)$ و $y = (y_{n-1},\ldots,y_0)$ و $z = x + y \bmod 2^n$ با $z = (z_{n-1},\ldots,z_0)$؛ در این صورت، به ازای $0 \le i < n$ داریم:

$$P(c_i = 0) = \frac{1}{2} + \frac{1}{2^{i+1}}$$

که در اینجا با توجه به (1) داریم: $z_i = x_i \oplus y_i \oplus c_i$.

اثبات: قضیه را به استقرا روی i ثابت می‌کنیم؛ داریم:

$$P(c_0 = 0) = 1 = \frac{1}{2} + \frac{1}{2^1}$$

حال، اگر حکم به ازای $i-1$ صحیح باشد، داریم:

$$P(c_i = 0) = P(x_{i-1}y_{i-1} \oplus c_{i-1}(x_{i-1} \oplus y_{i-1}) = 0)$$

$$= P(c_{i-1} = 0)P(x_{i-1}y_{i-1} = 0) +$$
$$P(c_{i-1} = 1)P(x_{i-1} \oplus y_{i-1} \oplus x_{i-1}y_{i-1} = 0)$$

$$= \frac{3}{4}(\frac{1}{2} + \frac{1}{2^i}) + \frac{1}{4}(\frac{1}{2} - \frac{1}{2^i})$$

$$= \frac{1}{2} + \frac{1}{2^{i+1}}$$

با استفاده از قضیه‌ی فوق، امید تعداد بیت‌های مساوی تابع جمع پیمانه‌ای به پیمانه‌ی 2^n و تابع XOR بیتی برابر است با

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

قضیه ۳-۳: برای تعاریف جمع مذکور در قضیه‌ی ۳-۲، به ازای هر $(a_{n-1},\ldots,a_0) \in F_2^n$، داریم:

$$P(c_{n-1} = a_{n-1},\ldots,c_0 = a_0) = \begin{cases} (\frac{3}{4})^{n-1}3^{-w(b)} & a_0 = 0 \\ 0 & a_0 \neq 0 \end{cases}$$

که در اینجا c_i ها، $0 \le i < n$، بیت‌های نقلی جمع هستند و بردار b، برابر است با

$$b = (b_{n-1},\ldots,b_0)$$
$$= (a_{n-1} \oplus a_{n-2},\ldots,a_1 \oplus a_0,0)$$

اثبات: برای حالت $a_0 = 1$، چون بیت نقلی نخست همواره برابر صفر است، برابری واضح می‌باشد؛ در غیر این صورت، به سادگی تحقیق می‌شود که

$$P(c_i = 0 \mid c_{i-1} = 0) = P(c_i = 1 \mid c_{i-1} = 1) = \frac{3}{4}$$

و

$$P(c_i = 1 \mid c_{i-1} = 0) = P(c_i = 0 \mid c_{i-1} = 1) = \frac{1}{4}$$

رابطه‌ی ذیل نیز با توجه به (1) به سادگی بـه دست می‌آید؛ در واقع، رابطه‌ی (1)، به روشنی خاصیت مارکوف را برای دنباله یا فرایند تصادفی $\{c_i\}$ ثابت می‌کند. به تعبیر دیگر، داریم:

$$P(c_i = a_i \mid c_{i-1} = a_{i-1},\ldots,c_0 = a_0)$$
$$= P(c_i = a_i \mid c_{i-1} = a_{i-1})$$

لذا، داریم:

$$P(c_{n-1} = a_{n-1},\ldots,c_0 = 0)$$

$$= P(c_0 = 0) \times P(c_1 = a_1 \mid c_0 = 0)$$
$$\times \ldots \times P(c_{n-1} = a_{n-1} \mid c_{n-2} = a_{n-2})$$

$$= (\frac{3}{4})^{d_1} \times (\frac{1}{4})^{d_2} = \frac{3^{d_1}}{4^{d_1+d_2}}$$

که در اینجا

$$d_1 = |\{j \mid 0 \le j < n-1, a_j = a_{j+1}\}|$$

$$d_2 = |\{j \mid 0 \le j < n-1, a_j \neq a_{j+1}\}|$$

روشن است کـه $d_1 = n - w(b) - 1$ و $d_1 + d_2 = n - 1$ و ایـن اثبـات قضیه را تکمیل می‌کند.

شایان ذکر است که احتمال تساوی تابع جمع پیمانه‌ای به پیمانه‌ی توانی از ۲ با تابع XOR بیتی را به کمک قضیه‌ی ۳-۳ نیز می‌توان به دست آورد.

قضیه ۳-۴: به ازای $i \ge 2$ و $1 \le j < i$ و بیت‌های دلخواه a و b، داریم:

$$P(c_i = a \mid c_{i-j} = b) = \frac{1}{2} + \frac{(-1)^{a+b}}{2^{j+1}}$$

اثبات: حالت $i = 2$ با همه‌ی $1 \le j < i$ها یا $j = 1$ را در اثبات قضیه‌ی ۳-۳ بیان کردیم. حال فرض کنیم قضیه به ازای i و همه‌ی $1 \le j < i$ها صحیح باشد، ثابت می‌کنیم به ازای $i+1$ و هر $1 \le j < i+1$ نیز صحیح است؛ داریم:

$$P(c_{i+1} = a \mid c_{i+1-j} = b) = \frac{P(c_{i+1} = a, c_{i+1-j} = b)}{P(c_{i+1-j} = b)}$$

$$= \frac{P(c_{i+1} = a, c_i = 0, c_{i+1-j} = b)}{P(c_{i+1-j} = b)}$$

$$+ \frac{P(c_{i+1} = a, c_i = 1, c_{i+1-j} = b)}{P(c_{i+1-j} = b)}$$

$$= \frac{P(c_{i+1-j}=b)P(c_i=0\mid c_{i+1-j}=b)P(c_{i+1}=a\mid c_i=0,c_{i+1-j}=b)}{P(c_{i+1-j}=b)}$$

$$+ \frac{P(c_{i+1-j}=b)P(c_i=1\mid c_{i+1-j}=b)P(c_{i+1}=a\mid c_i=1,c_{i+1-j}=b)}{P(c_{i+1-j}=b)}$$

$$= P(c_i=0\mid c_{i+1-j}=b)P(c_{i+1}=a\mid c_i=0)$$

$$+ P(c_i=1\mid c_{i+1-j}=b)P(c_{i+1}=a\mid c_i=1)$$

$$= (\frac{1}{2}+\frac{(-1)^b}{2^j})(\frac{1}{2}+\frac{(-1)^a}{2^2})$$

$$+ (\frac{1}{2}+\frac{(-1)^{b+1}}{2^j})(\frac{1}{2}+\frac{(-1)^{a+1}}{2^2})$$

$$= \frac{1}{2}+\frac{(-1)^{a+b}}{2^{j+1}}$$

قضیه ۳-۵: به ازای هر $2\le r\le n$ و هر $a\in F_2^r$ با

$$a=(a_{r-1},\ldots,a_0)$$

و هر $(j_{r-1},\ldots,j_0)$ با $0<j_0<j_1<\ldots<j_{r-1}<n$، داریم:

$$P(c_{j_{r-1}}=a_{r-1},\ldots,c_{j_0}=a_0)=\prod_{k=0}^{r-1}(\frac{1}{2}+\frac{(-1)^{a_k+a_{k-1}}}{2^{j_k-j_{k-1}+1}})$$

که در اینجا داریم $j_{-1}=a_{-1}=0$.

اثبات: مشابه قضیه‌ی قبل و با استفاده از (1) یا خاصیت مارکوف $\{c_i\}$، داریم:

$$P(c_{j_{r-1}}=a_{r-1},\ldots,c_{j_0}=a_0)$$

$$= P(c_{j_0}=a_0)\prod_{k=1}^{r-1}P(c_{j_k}=a_k\mid c_{j_{k-1}}=a_{k-1},\ldots,c_{j_0}=a_0)$$

$$= P(c_{j_0}=a_0)\prod_{k=1}^{r-1}P(c_{j_k}=a_k\mid c_{j_{k-1}}=a_{k-1})$$

$$= \prod_{k=0}^{r-1}(\frac{1}{2}+\frac{(-1)^{a_k+a_{k-1}}}{2^{j_k-j_{k-1}+1}})$$

روشن است که قضیه‌ی ۳-۴، تعمیمی از قضیه‌ی ۳-۳ نیز می‌باشد.

۴- ویژگی‌های خطی و تفاضلی

در بررسی یک نگاشت از منظر رمزنگاری، پارامترهای خطی و تفاضلی از اهمیت زیادی برخوردارند؛ به همین دلیل، ما قضیه‌ای درباره‌ی پارامترهای خطی و تفاضلی اثبات می‌کنیم و پس از آن، پارامترهای خطی و تفاضلی جمع پیمانه‌ای به پیمانه‌ی 2^n را که به کمک برنامه‌نویسی، برای $1\le n\le 8$، به دست آورده‌ایم، ارائه می‌دهیم.

قضیه ۴-۱: اگر جمع پیمانه‌ای به پیمانه‌ی 2^n را به صورت $f:F_2^{2n}\to F_2^n$ در نظر بگیریم و پارامترهای خطی و تفاضلی تابع مؤلفه‌ای i-ام، $0\le i<n$، را با c_i^n و d_i^n نشان دهیم، داریم:

$$\begin{aligned} c_i^n &= c_i^m,\ 0\le i<n,\ m>n \\ d_i^n &= 1,\quad 0\le i<n \end{aligned} \qquad (3)$$

اثبات: رابطه‌ی اول (3)، به این دلیل صحیح است که بیت i-ام خروجی جمع، به بیت‌های 0- ام تا i- ام ورودی‌ها بستگی دارد؛ در واقع، در محاسبه‌ی c_i^m، همان محاسبات c_i^n، به تعداد 2^{m-n} بار تکرار می‌شود؛ یا به تعبیر دیگر، یک عامل 2^{m-n} در صورت و مخرج کسر مربوط به محاسبه‌ی c_i^m ضرب می‌شود.

در محاسبه‌ی d_i^n، $0\le i<n$، کافی است قرار دهیم:

$$a=(1,\overbrace{0,\ldots,0}^{n-1},1,\overbrace{0,\ldots,0}^{n-1})$$

به سادگی می‌توان دید که به ازای هر $x\in F_2^{2n}$، داریم:

$$f_i(x\oplus a)=f_i(x)$$

و این اثبات را کامل می‌کند.

ما c_{n-1}^n را به ازای $n=0,1,\ldots,7$ به ترتیب برای جمع پیمانه‌ای به پیمانه‌های 2^1 تا 2^8 محاسبه کرده‌ایم؛ در ذیل عدد سمت راست برابر c_0^1 است:

۰.۰۰۰۰۰۶, 0.00024, 0.00098, 0.00391, 0.01563, 0.625, 0.25

۵- ویژگی‌های جبری

در این بخش، با استفاده از مراجع [1] و [3]، به بیان ویژگی‌های جبری بیت نقلی می‌پردازیم.

قضیه ۵-۱: درجه‌ی جبری تابع دودویی معرف بیت نقلی i - ام جمع یا c_i، $i > 0$، برابر است با $i+1$؛ همچنین، تعداد جملات تابع مذکور برابر است با $2^i - 1$.

اثبات: [1].

۶- نتیجه‌گیری

در این مقاله ، ما به بررسی جمع پیمانه‌ای به پیمانه‌ی توانی از ۲ پرداختیم. در ابتدا، به بررسی توزیع بیت‌های نقلی جمع پرداختیم و پس از به دست آوردن توزیع مذکور، توزیع توأم و چندگانه‌ی بردار بیت‌های نقلی را نیز به دست آوردیم. سپس، به بررسی خواص خطی و تفاضلی جمع پیمانه‌ای به پیمانه‌ی توانی از ۲ پرداختیم و ثابت کردیم که این عملگر، به هیچ وجه ویژگی‌های تفاضلی خوبی ندارد ولی از دیدگاه خطی، همبستگی بیت‌های پرارزش جمع پیمانه‌ای با ورودی‌ها، تا حدودی پایین است. در پایان، به بررسی ویژگی‌های جبری بیت نقلی پرداختیم و بـر اساس قضیـه‌ای از [1]، درجه‌ی توابع دودویی معرف بیت‌های نقلی و تعداد جملات در توابع مذکور را ارائه دادیم.

مراجع

[1] رحیمی‌پور علیرضا، دهنوی سید مجتبی، "درجه جبری توابع مؤلفه‌ای جمع پیمانه‌ای به پیمانه 2^t با r عملوند"، **ششمین کنفرانس بین المللی انجمن رمز ایران، صفحه‌های ۱-۵، دانشگاه اصفهان، ۱۳۸۸ .**

[2] Bluetooth SIG, "Specification of the Bluetooth System", Version 1.1, 1 Febraury 22, 2001, available at http://www.bluetooth.com.

[3] A. Braeken, I. Semaef, "The ANF of Composition of Addition and Multiplication mod 2^n with a Boolean Function", FSE'05, LNCS 2887, pp. 290-306, Springer-Verlag, 2005.

[4] 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.

[5] J. Jonsson and B. S. Kaliski, Jr, "RC6 block cipher", Primitive submitted to NESSIE by RSA, Sept. 2000.

[۶] R.L.Rivest, "The RC4 encryption algorithm," RSA Data Security, Inc.,Mar.,1992.

[۷] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, "Twofish: A 128-Bit Block Cipher", 1998,
Available via http://www.counterpane.com/twofish.html.

زیرنویس‌ها

۱ **Carry Bit**

۲ **Component Boolean Functions**

۳ ***Algebraic Normal Form***