مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۴ -۱

ساختن توابع *APN* جدید

مهدی علائیان[1*]، سید محمدکاظم حسینی‌پور[2]

۱- استاد، دانشگاه علم و صنعت ایران، ۲- مدرس دانشگاه علم و صنعت ایران

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۱)

چکیده

تابع F از $\mathbb{F}_{2^n}$ به خودش که n یک عدد صحیح مثبت است تقریباً ناخطی تام (APN) نامیده می‌شود، هرگاه برای هر $a \neq 0$ و هر b از $\mathbb{F}_{2^n}$ معادله $F(x+a)+F(x)=b$ حداکثر دو جواب در $\mathbb{F}_{2^n}$ داشته باشد. در این مقاله یک تابع APN جدید روی $\mathbb{F}_{2^n}$ که n یک عدد صحیح زوج است را معرفی می‌کنیم.

واژه‌های کلیدی: تقریباً خم، تقریباً ناخطی تام، یکنواختی تفاضل، جعبه‌های جانشینی

۱- مقدمه

در این مقاله n را همواره یک عدد صحیح مثبت در نظر می‌گیریم.

فرض کنیم $F:\mathbb{F}_2^n \to \mathbb{F}_2^n$. در این صورت F را می‌توان به‌طور یکتا به‌صورت:

$$F(x_1,x_2,\dots,x_n)=\sum_{i=1}^{n} c(u)\prod_{i=1}^{n} x_i^{u_i},$$

نمایش داد که در آن $c(u)\in\mathbb{F}_2^n$. این نمایش را فرم نرمال جبری F گویند. درجه جبری F که آن‌را با $d^0(F)$ نشان می‌دهیم عبارت است از درجه فرم نرمال جبری آن، یعنی:

$$d^0(F)=\sum_{x\in\mathbb{F}_2^n} u=(u_1,u_2,\dots u_n)\in\mathbb{F}_2^n, c(u)\neq 0\}.$$

تابع $F:\mathbb{F}_2^n \to \mathbb{F}_2^n$ را خطی[1]، آفین[2] یا کوادراتیک[3] گویند هرگاه به ترتیب دارای درجه جبری یک، حداکثر یک و حداکثر دو باشد. توجه داشته باشید که میدان $\mathbb{F}_{2^n}$ به عنوان فضای برداری با $\mathbb{F}_2^n$ یک‌ریخت است. لذا هر تابع از $\mathbb{F}_2^n$ به خودش را می‌توان به‌عنوان تابعی از $\mathbb{F}_{2^n}$ به $\mathbb{F}_{2^n}$ درنظر گرفت. هر تابع مانند F از $\mathbb{F}_{2^n}$ به خودش یک نمایش یکتا به‌صورت یک چندجمله‌ای[4] از درجه حداکثر 2^n-1 روی $\mathbb{F}_{2^n}$ مانند

$$F(x)=\sum_{i=1}^{2^n-1} c_i x^i,\ \ c_i\in\mathbb{F}_{2^n} \qquad (۱)$$

دارد. برای هر $0\le k\le n$ تعداد ضرایب ناصفر $k_s\in\{0,1\}$ در بسط دودویی $k=\sum_{i=1}^{n-1} k_s 2^s$ را -2 وزن k نامیده و آن‌را با $w_2(k)$ نشان می‌دهیم. درجه جبری F برابر است با بیشینه -2 وزن توان‌های i از چندجمله‌ای $F(x)$ به‌طوری‌که $c_i\neq 0$، یعنی $d^0(F)=max_{0\le i\le n-1, c_i\neq 0} w_2(i)$ [۱۱]. بنابراین، اگر F خطی باشد، آن‌گاه نمایش آن به فرم (۱) عبارت است از $F(x)=\sum_{i=1}^{n-1} c_i x^{2^i}$ و اگر آفین باشد نمایشی به‌صورت $F(x)=c+\sum_{i=1}^{n-1} c_i x^{2^i}$ دارد و درصورتی‌که کوادراتیک باشد می‌توان آن‌را به‌صورت:

$$F(x)=\ c+\sum_{i=1}^{n-1} c_i x^{2^i}+\sum_{0\le j<k<n} d_{kj} x^{2^k+2^j},$$

نوشت.

برای تابع $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ مجموعه جواب‌های معادله:

$$F(x+a)+F(x)=b \qquad (۲)$$

در $\mathbb{F}_{2^n}$ را که $a,b\in\mathbb{F}_{2^n}$ با $\delta_F(a,b)$ نشان می‌دهیم، یعنی:

$$\delta_F(a,b)=\{x\in\mathbb{F}_{2^n}: F(x+a)+F(x)=b\}.$$

تابع $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ را δ_F-یکنواخت تفاضلی گوییم هرگاه:

$$\delta_F=\max_{a\in\mathbb{F}_{2^n}^*, b\in\mathbb{F}_{2^n}} |\delta_F(a,b)|,$$

و اگر $\delta_F=2$، آن‌گاه F تقریباً ناخطی تام یا APN نامیده می‌شود. توجه داشته باشید که $\delta_F\ge 2$ زیرا a و 0 هر دو جواب‌های معادله *(2)* به ازای $b=F(0)+F(a)$ در $\mathbb{F}_{2^n}$ اند. به‌علاوه، δ_F همواره زوج است زیرا اگر x جواب معادله (۲) باشد،

* رایانامه نویسنده مسئول: alaeiyan@iust.ac.ir

1- Linear
2- Affine
3- Quadratic

آن‌گاه $x+a$ نیز جوابی از این معادله است.

برهان: برای اعداد صحیح و مثبت δ تابع F از $\mathbb{F}_{2^n}$ به خودش به‌طور تفاضلی δ-یکنواخت نامیده می‌شود هرگاه برای هر $a \neq 0$ و b از $\mathbb{F}_{2^n}$ معادله $F(x+a)=F(x)=b$ حداکثر δ جواب در $\mathbb{F}_{2^n}$ داشته باشد. توابع روی $\mathbb{F}_{2^n}$ که به‌عنوان $s-box$ در رمزهای بلوکی استفاده می‌شوند باید دارای یک‌نواختی تفاضلی پایینی باشند تا در برابر حملات تفاضلی امنیت بیش‌تری داشته باشند [۱]. از این جهت توابع 2-یکنواخت تفاضلی بهینه‌اند زیرا برای هر تابع روی $\mathbb{F}_{2^n}$ داریم: $\delta \geq 2$.

برای هر تابع $F: \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ قرار می‌دهیم:

$$\lambda_F(a+b) = \sum(-1)^{tr(bF(x)+ax)}, a, b \in \mathbb{F}_{2^n},$$

که $tr(x) = x + x^2 + \cdots + x^{2^{n-1}}$ تابع اثر از $\mathbb{F}_{2^n}$ به $\mathbb{F}_2$ است. مجموعه $\{\lambda_F(a,b) | a, b \in \mathbb{F}_{2^n}, b \neq 0\}$ طیف والش F نامیده می شود.

اگر طیف والش F مساوی $\left\{0, \pm 2^{\frac{n+1}{2}}\right\}$ باشد، آن‌گاه تابع تقریباً خم[1] (AB) نامیده می‌شود. بنابراین، توابع AB فقط برای n های فرد موجودند. این توابع بیشترین امنیت را در برابر حملات خطی دارند [۱۰] . هر تابع AB، APN نیز هست [۹] و برای nهای فرد هر تابع کوادراتیک APN است اگر و تنها اگر AB باشد [۸] . یک بررسی جامع از توابع APN و AB را می توان در [۷] یافت. اخیراً چند خانواده از توابع APN کوادراتیک ساخته شده است [۲-۵]. در [۶] یک روش برای ساختن توابع APN کوادراتیک با استفاده از یک تابع APN شناخته‌شده در قالب قضیه زیر ارائه شده است:

قضیه ۱-۱- فرض کنیم F یک تابع APN کوادراتیک از $\mathbb{F}_{2^n}$ به خودش و f یک تابع بولی کوادراتیک روی $\mathbb{F}_{2^n}$ باشد. همچنین فرض کنیم:

$$\varphi_F(x,a) = F(x+a) + F(x) + F(o) + F(a),$$
$$\varphi_f(x,a) = f(x+a) + f(x) + f(o) + f(a).$$

در این صورت، اگر برای هر $a \neq 0$ از $\mathbb{F}_{2^n}$ تابع بولی خطی l_a که در شرایط زیر صدق می‌کند

$$l_a(\varphi_F(x,a)) = \varphi_f(x,a). \qquad (1)$$

(۲) اگر برای $x \in \mathbb{F}_{2^n}$ داشته باشیم $\varphi_F(x,a) = 1$، آن‌گاه $l_a(1) = 0$، آن‌گاه $F(x)+f(x)$ تابعی APN است.

در بخش دوم این مقاله با استفاده از این قضیه و تابع APN کوادراتیک $F(x) = x^3$ یک تابع APN روی $\mathbb{F}_{2^n}$ که n عددی زوج است را می‌سازیم و در بخش سوم نتیجه‌گیری مختصری ارائه می‌گردد.

۲- ساختن توابع APN کوادراتیک جدید

گزاره ۲-۱- اگر $F: F_{2^n} \to F_{2^n}$ یک تابع کوادراتیک باشد و $a \in F_{2^n}^*$، آن‌گاه برای هر $b \in F_{2^n}$ داریم:

$$|\delta_F(a,b)| = |\delta_F(a, F(a)+F(0))|.$$

برهان: چون F کوادراتیک است، پس دارای نمایشی به صورت:

$$F(x) = c + \sum_{i=0}^{2^n-1} c_i x^{2^i} + \sum_{0 \leq i<k<n} d_{kj} x^{2^k+2^j},$$

است. تابع $G: \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ را با ضابطه:

$$G(x) = \sum_{0 \leq j<k<n} d_{jk}(x^{2^k}a^{2^j} + x^{2^j}a^{2^k}),$$

تعریف می کنیم. اگر $\mathbb{F}_{2^n}$ را به‌عنوان فضای برداری روی $\mathbb{F}_2$ در نظر بگیریم، آن‌گاه G یک تبدیل خطی است زیرا برای هر $x, y \in \mathbb{F}_{2^n}$،

$$G(x+y) = \sum_{0 \leq j<k<n} d_{jk}((x+y)^{2^j}a^{2^k} + (x+y)^{2^k}a^{2^j}),$$

$$= \sum_{0 \leq i<j<n} d_{jk}(x^{2^j}a^{2^k} + y^{2^j}a^{2^k} + x^{2^k}a^{2^j} + y^{2^k}a^{2^j}),$$

$$= \sum_{0 \leq j<k<n} d_{jk}(x^{2^j}a^{2^k} + x^{2^k}a^{2^j}) + \sum_{0 \leq j<k<n} d_{jk}(y^{2^j}a^{2^k} + y^{2^k}a^{2^j}),$$

$$= G(x) + G(y),$$

و $G(0) = 0$. حال فرض کنیم برای $a \in \mathbb{F}_{2^n}^*$ و $b \in \mathbb{F}_{2^n}$، x جوابی از معادله $F(x+a) = F(x) = b$ باشد. چون:

$$F(x+a) = c + \sum_{i=0}^{n-1}(x+a)^{2^i} + \sum_{0 \leq j<k<n} d_{jk}(x+a)^{2^j+2^k},$$
$$= c + \sum_{i=0}^{n-1} x^{2^i} + \sum_{i=0}^{n-1} a^{2^i} + \sum_{0 \leq j<k<n} d_{jk}[(x^{2^j} + a^{2^j})(x^{2^k} + a^{2^k})],$$
$$= c + \sum_{i=0}^{n-1} x^{2^i} + \sum_{i=0}^{n-1} a^{2^i} + \sum_{0 \leq j<k<n} d_{jk}x^{2^j+2^k} + \sum_{0 \leq j<k<n} d_{jk}a^{2^j+2^k} + \sum_{0 \leq j<k<n} d_{jk}(x^{2^j}a^{2^k} + x^{2^k}a^{2^j}),$$

$$= F(x) + F(0) + F(a) + G(x).$$

پس داریم:

$$G(x) + F(0) + F(a) = b$$

و در نتیجه:

$$G(x) = F(0) + F(a) + b.$$

بنابراین:

1- almost bent

$$\delta_F(a,b) = G^{-1}(F(0)+F(a)+b). \quad (۳)$$

از این‌رو:

$$\delta_F(a,F(0)+F(a)) = G^{-1}(0) = kerG.$$

از طرفی داریم:

$$|Ker\ G| = |G^{-1}(F(0)+F(a)+b)|.$$

لذا بنابر رابطه (۳):

$$|\delta_F(a,b)| = |\delta_F(a,F(0)+F(a))|.$$

نتیجه ۲-۲: فرض کنیم $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ تابعی کوادراتیک باشد. در این صورت، F تابعی APN است هرگاه برای هر $a\in\mathbb{F}_{2^n}$ معادله $F(x)+F(x+a)=F(0)+F(a)$ دو جواب در $\mathbb{F}_{2^n}$ داشته باشد.

فرض کنیم F تابعی کوادراتیک و APN از $\mathbb{F}_{2^n}$ به خودش باشد و $a\in\mathbb{F}_{2^n}^*$. هم‌چنین فرض کنیم:
$L=\{\varphi_F(x,a)|x\in\mathbb{F}_{2^n}\}.$

چون F کوادراتیک است دارای نمایشی به صورت:

$$F(x)=c+\sum_{i=0}^{2^n-1}c_ix^{2^i}+\sum_{0\le i<k<n}d_{kj}x^{2^k+2^j},$$

است که $c,a_i,d_{jk}\in\mathbb{F}_{2^n}$. تابع $G:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ را با ضابطه:

$$G(x)=\sum_{0\le j<k<n}d_{jk}(x^{2^k}a^{2^j}+x^{2^j}a^{2^k}),$$

تعریف می‌کنیم. همان‌طورکه در برهان گزاره ۲-۱ مشاهده کردید G خطی است و برای هر $x\in\mathbb{F}_{2^n}$ داریم:

$$F(x+a)=F(x)+F(0)+F(a)+G(x).$$

پس برای هر $x,y\in\mathbb{F}_{2^n}$:

$$\varphi_F(x+y,a)=F(x+y+a)+F(x+y)+F(a)+F(0),$$

$$=(F(x+y)+F(0)+F(a)+G(x+y))+F(x+y)+F(a)+F(0),$$

$$=G(x+y),$$

$$=G(x)+G(y).$$

از طرفی داریم:

$$\varphi_F(x,a)+\varphi_F(y,a)=F(x+a)+F(x)+F(a)+F(0)+F(y+a)+F(y)+F(a)+F(0),$$

$$=F(x+a)+F(x)+F(y+a)+F(y),$$

$$=(F(x)+F(0)+F(a)+G(x))+F(x)+(F(y)+F(0)+F(a)+G(y))+F(y),$$

$$=G(x)+G(y).$$

از این‌رو:

$$\varphi_F(x+y,a)=\varphi_F(x,a)+\varphi_F(y,a). \quad (۴)$$

لذا L زیرفضای $\mathbb{F}_{2^n}$ است. چون f نیز کوادراتیک است، داریم:

$$\varphi_f(x+y,a)=\varphi_f(x,a)+\varphi_f(y,a).$$

اینک تابع $l_a:L\to\mathbb{F}_{2^n}$ را با ضابطه:

$$l_a(\varphi_F(x,a))=\varphi_f(x,a)$$

تعریف می‌کنیم. این تابع خوش تعریف است زیرا اگر برای $x,y\in\mathbb{F}_{2^n}$ داشته باشیم $\varphi_F(x,a)=\varphi_F(y,a)$، آن‌گاه $\varphi_F(x,a)+\varphi_F(y,a)=0$ و در نتیجه بنابر رابطه (۴)، $\varphi_F(x+y,a)=0$. اما چون F تابعی APN است، از این تساوی نتیجه می‌شود که $x+y=0$ یا $x+y=a$. اگر $x+y=0$، آن‌گاه $x=y$ و در نتیجه $\varphi_f(x,a)=\varphi_f(y,a)$ و اگر $x+y=a$، آن‌گاه $y=x+a$ و لذا:

$$\varphi_f(y,a)=\varphi_f(x+a,a)=f(x+a+a)+f(x+a)+f(a)+f(0),$$

$$=f(x)+f(x+a)+f(a)+f(0),$$

$$=\varphi_f(x,a).$$

پس داریم $l_a(\varphi_F(x,a))=l_a(\varphi_F(y,a))$. لذا l_a خوش تعریف است. بعلاوه برای هر $x,y\in\mathbb{F}_{2^n}$:

$$l_a(\varphi_F(x,a)+\varphi_F(y,a))=l_a(\varphi_F(x+y,a)),$$

$$=\varphi_f(x+y,a),$$

$$=\varphi_f(x,a)+\varphi_f(y,a),$$

$$=l_a(\varphi_F(x,a))+l_a(\varphi_F(y,a)).$$

پس خطی است. علاوه بر این، l_a را می‌توان به یک تابع خطی از $\mathbb{F}_{2^n}$ به $\mathbb{F}_2$ توسعه داد. لذا همواره تابع $l_a:\mathbb{F}_{2^n}\to\mathbb{F}_2$ موجود است که شرط (۲) قضیه ۱-۱ را بر آورده می‌کند.

قضیه ۲-۳- فرض کنیم n یک عدد صحیح مثبت و زوج باشد. دراین صورت تابع $f(x)=tr(x^9+x^3)$ روی $\mathbb{F}_{2^n}$، APN است.

برهان: فرض کنیم $F(x)=x^3$ و $f(x)=tr(x^9+x^3)$. در این

صورت، F یک تابع APN کوتدراتیک و f یک تابع بولی کوتدراتیک خطی است و داریم $\varphi_F(x,a)=a^2x+ax^2$ و $\varphi_f(x,a)=tr(a^8x+ax^8+ax^2+a^2x)$. برای هر عضو ناصفر a از $\mathbb{F}_{2^n}$ تابع بولی خطی l_a را به صورت زیر در نظر می‌گیرم:

$$l_a(y)=tr(a^6y+a^3y^2+a^{-3}y^4+y)$$

از این‌رو:

$$l_a(\varphi_F(x,a))=tr(a^6(a^2x+ax^2)+a^3(a^4x^2+a^2x^4)+a^{-3}(a^8x^4+a^4x^8)+a^2x+ax^2$$
$$=tr(a^8x+ax^8+a^2x+ax^2)$$
$$=\varphi_f(x,a).$$

اینک فرض کنیم وجود داشته باشد $x\in\mathbb{F}_{2^n}$ به‌طوری‌که $\varphi_F(x,a)=1$. در این صورت:

$$l_a(1)=tr(a^6+a^3+a^{-3}+1)=tr(a^{-3}+1)$$
$$=tr(a^{-3})+tr(1).$$

چون n زوج است، $tr(1)=0$. از این‌رو:

$$l_a(1)=tr(a^{-3})$$
$$=tr(\frac{a^2x+ax^2}{a^{-3}})$$
$$=tr\left(\left(\frac{x}{a}\right)+\left(\frac{x}{a}\right)^2\right)=0.$$

لذا به موجب قضیه ۱-۱، $x^3+tr(x^9+x^3)$ تابعی APN است.

۳- نتیجه‌گیری

توابع APN بیشترین امنیت را در برابر حملات تفاضلی دارا هستند. چندین روش برای ساختن توابع APN ارائه شده است. یکی از این روش‌ها در قالب قضیه ۱-۱ در بخش اول این مقاله معرفی شد. در این مقاله با استفاده از این روش تابع APN کوادراتیک $x^3+tr(x^9+x^3)$ روی $\mathbb{F}_{2^n}$ که n عددی صحیح و زوج است ساخته شد.

۴- مراجع

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," J. Cryptology, vol. 4, no. 1, pp. 3-72, 1991.

[2] C. Bracken, E. Byrne, N. Markin, and G. McGuire, "New families of quadratic almost perfect nonlinear trinomials and multinomials," Finite Fields Appl., vol. 14, pp. 703–714, 2008.

[3] C. Bracken, E. Byrne, N. Markin, and G. McGuire, "A few more quadratic APN functions," preprint, 2008.Available at http:// www.arxiv.org/abs/0804.4799.

[4] L. Budaghyan and C. Carlet, "Classes of quadratic APN trinomials and hexanomials and related structures," IEEE Trans. Inform. Theory, vol. 54, no. 5, pp. 2354–2357, 2008.

[5] L. Budaghyan, C. Carlet, and G. Leander, "Two classes of quadratic APN binomials inequivalent to power functions," IEEE Trans. Inform. Theory, vol. 54, no. 9, pp. 4218–4229, 2008.

[6] L. Budaghyan, C. Carlet, and G. Leander, "Constructing new APN functions from known ones," Finite Fields and Their Applications, vol. 15, issue 2, pp. 150-159, 2009.

[7] C. Carlet, "Vectorial boolean functions for cryptography," chapter of the monography Boolean Methods and Models, Y. Crama, P. Hammer (Eds.), Cambridge Univ. Press, in press.

[8] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," Des. Codes Cryptogr., vol. 15, no. 2, pp. 125–156, 1998.

[9] F. Chabaud and S. Vaudenay, "Links between differential and linear cryptanalysis," in: Advances in Cryptology EUROCRYPT'94, in: Lecture Notes in Comput. Sci., vol. 950, Springer-Verlag, New York, pp. 356–365, 1995.

[10] M. Matsui, "Linear cryptanalysis method for DES cipher," in: Advances in Cryptology EUROCRYPT'93, in: Lecture Notes in Comput. Sci., Springer-Verlag, pp. 386–397, 1994.