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

درجه‌ی جبری توابع مؤلفه‌ای جمع پیمانه‌ای به پیمانه‌ی 2^t با r عملوند

علیرضا رحیمی‌پور، سید مجتبی دهنوی

گروه صنایع امنیت فاوا - صا ایران

Alireza_rahimipour@mathdep.iust.ac.ir

Dehnavi.sm @gmail.com

چکیده

جمع پیمانه‌ای به پیمانه‌ی 2^t، یکی از عملگرهای پرکاربرد در رمزنگاری متقارن است؛ به همین جهت، بررسی خواص این عملگر نقش مهمی در طراحی و تحلیل رمزهای متقارن ایفا می‌کند. از آنجا که تحلیل جبری این عملگر برای دو عملوند قبلاً انجام شده است، در این مقاله با استفاده از نتایج پژوهش‌های پیشین، به بررسی جبری جمع پیمانه‌ای به پیمانه‌ی 2^t با $r \geq 2$ عملوند پرداخته، درجات توابع بولی مؤلفه‌ای این عملگر را، به عنوان یک نگاشت بولی، به دست می‌آوریم. همچنین، ضمن انجام تحلیلی نظری در چند حالت خاص، الگوریتمی کارامد جهت محاسبه‌ی درجات توابع بولی مؤلفه‌ای عملگر مذکور در حالت کلی ارائه می‌کنیم. در نهایت به کمک این الگوریتم، درجه‌ی توابع مؤلفه‌ای مورد بحث را برای سه تا هشت عملوند به دست می‌آوریم.

واژه‌های کلیدی

جمع پیمانه‌ای به پیمانه‌ی 2^t، تابع بولی، ANF، درجه‌ی جبری.

۱- مقدمه

یکی از عملگرهایی که تاکنون بیشترین کاربرد را در رمزنگاری متقارن داشته، جمع پیمانه‌ای به پیمانه‌ی 2^t می‌باشد که در آن t عددی صحیح و مثبت است و معمولاً برابر اندازه‌ی پردازنده‌های نوعی - یعنی ۸، ۱۶، ۳۲ و یا ۶۴ - می‌باشد. به عنوان مثال، این عملگر در رمزهای دنباله‌ای Bluetooth [1] و RC4 [2]، نیز در رمزهای قالبی خانواده‌ی SAFER [3]، IDEA [4]، RC6 [5]، Towfish [6] و Mars [7] به کار رفته است. در [8] به ویژگی‌های جبری جمع پیمانه‌ای به پیمانه‌ی 2^t با دو عملوند پرداخته شده و ANF توابع بولی مؤلفه‌ای این عملگر به طور صریح به دست آمده است. به دست آوردن ANF این توابع مؤلفه‌ای در حالت کلی بسیار مشکل است و حتی یافتن رابطه‌ای صریح برای درجات این توابع نیز کار سختی است. اما برای بسیاری از کاربردها در طراحی و ارزیابی رمزهای متقارن، دانستن درجه‌ی جبری توابع مؤلفه‌ای، اهمیت شایانی دارد. در این مقاله برای اولین بار، درجه‌ی توابع بولی مؤلفه‌ای را برای جمع پیمانه‌ای به پیمانه‌ی 2^t با $r \geq 2$ عملوند به دست آورده‌ایم.

در بخش ۲ به تعاریف و قضایای مقدماتی می‌پردازیم. بخش ۳ به اثبات قضایایی که درجه‌ی توابع بولی مؤلفه‌ای را در حالت 2^n عملوند صریحاً به دست می‌آورند، اختصاص دارد. در بخش ۴ به ارائه‌ی الگوریتمی کارامد برای محاسبه‌ی درجات مذکور در حالت کلی می‌پردازیم و در پایان، در بخش ۵ به نتیجه‌گیری و ارائه‌ی راهکار برای پژوهش‌های آینده می‌پردازیم.

۲- تعاریف و قضایای مقدماتی

فرض کنیم Z_2 میدان متناهی با دو عضو (حلقه‌ی اعداد صحیح به پیمانه‌ی ۲) باشد؛ در این صورت، هر عضو ${Z_2}^t$ (حاصل-ضرب دکارتی t نسخه از Z_2) را می‌توان به صورت یک بردار در نظر گرفت که ما آن را با $\bar{x}$ نشان می‌دهیم. با توجه به تعریف ${Z_2}^t$، یک تناظر یک به یک بین ${Z_2}^t$ و Z_{2^t}، حلقه اعداد صحیح به پیمانه‌ی 2^t، بر قرار است که به صورت ذیل تعریف می-شود:

$$\varphi : {Z_2}^t \to Z_{2^t}$$
$$\bar{x} = (x_{t-1},...,x_0) \mapsto x = \sum_{i=0}^{t-1} x_i 2^i \qquad (۱)$$

در نمایش بالا، x_i را مؤلفه‌ی $(i+1)$ - ام x می‌نامیم.

حال، ترتیب جزیی $\preceq$ را روی ${Z_2}^t$ به صورت زیر تعریف می‌کنیم:

$$\bar{x} \preceq \bar{a} \iff x_i \le a_i \quad 0 \le i \le t-1 \qquad (۲)$$

در نمایش بالا، اگر

$$\bar{x} = (x_{t-1},...,x_0) \quad و \quad \bar{u} = (u_{t-1},...,u_0) \qquad (۳)$$

آنگاه $\bar{x}^u$ به صورت ${x_0}^{u_0}...{x_{t-1}}^{u_{t-1}}$ تعریف می‌شود.

هر تابع f به صورت $f : {Z_2}^t \to Z_2$ را یک تابع بولی[1] می‌نامند. فرض کنید f تابعی بولی باشد: f را می‌توان به شکلی یکتا که آن را صورت نرمال جبری (ANF) می‌نامیم، نشان داد. در واقع:

$$f(\bar{x}) = \bigoplus_{u \in Z_{2^t}} h_u \bar{x}^u, \quad h_u \in Z_2 \qquad (۴)$$

که در آن ضرایب h_u به صورت زیر تعیین می‌شوند:

$$h_u = h(\bar{u}) = \bigoplus_{\bar{x} \preceq \bar{u}} f(\bar{x}) \qquad (۵)$$

درجه‌ی جبری[2] تابع f، که با $\deg(f)$ نشان داده می‌شود، برابر با تعداد متغیرها در طولانی‌ترین جمله‌ی ANF این تابع است؛ به طور معادل، $\deg(f)$ بیشترین وزن همینگ[3] $\bar{u}$، $wt(\bar{u})$، برای هر $h_u \neq 0$ تعریف می‌شود.

هر تابع $f : {Z_2}^t \to {Z_2}^m$، با $m > 1$، یک تابع بولی برداری[4] نامیده می‌شود. این تابع را می‌توان به وسیله‌ی بردار $(f_1, f_2, ... f_m)$ بیان کرد که هر f_i، $1 \le i \le m$، یک تابع بولی $f_i : {Z_2}^t \to Z_2$ است که به آن تابع مؤلفه‌ای[5] می‌گوییم.

می‌توان ثابت کرد که معادل بولی جمع در Z_{2^t} برای دو بردار $\bar{x} = (x_{t-1},...,x_0)$ و $\bar{y} = (y_{t-1},...,y_0)$، به صورت ذیل است:

$$r_0 = x_0 \oplus y_0 \oplus c_0, \quad c_0 = 0 \qquad (۶)$$
$$r_i = x_i \oplus y_i \oplus c_i, \quad c_i = x_{i-1}y_{i-1} \oplus x_{i-1}c_{i-1} \oplus y_{i-1}c_{i-1} \quad i \ge 1$$

قضیه ۲-۱: فرض کنیم ANF تابع بولی $f : {Z_2}^t \to Z_2$ با ضابطه‌ی $\bar{x} \mapsto f(\bar{x})$، یک تک‌جمله‌ای $\bar{x}^u$، $u \in Z_{2^t}$، باشد؛ در این صورت، ANF تابع $f(\bar{x} + \bar{y})$ به صورت زیر است:

$$f(\bar{x} + \bar{y}) = \bigoplus_{c=0}^{u} \bar{x}^{(u-c)} \bar{y}^c \qquad (۷)$$

که در اینجا، تفاضل $u - c$ در Z_{2^t} محاسبه می‌شود.

برهان: [8] .

قضیه۲-۲: اگر $y_1, y_2, ..., y_r \in Z_2^t$ و تابع f به شکلِ تعریف شده در قضیه‌ی ۲-۱ باشد، آنگاه ANF تابع $f(\bar{y}_1 + \bar{y}_2 + ... + \bar{y}_r)$ به صورت ذیل است:

$$f(\bar{y}_1 + \bar{y}_2 + ... + \bar{y}_r) = \bigoplus_{\substack{k_0,...k_{r-1} \ge 0 \\ k_0 + .. + k_{r-1} = u}} y_1^{k_0} ... y_r^{k_{r-1}} \qquad (۸)$$

برهان: برای اثبات، $r-1$ بار از قضیه‌ی ۲-۱ استفاده می‌کنیم. ابتدا، تغییر متغیر $\bar{y}_2 + ... + \bar{y}_r = \bar{x}_1$ را در نظر می‌گیریم و قضیه‌ی ۲-۱ را به کار می‌بریم:

$$f(\bar{y}_1 + \bar{y}_2 + ... + \bar{y}_r) = f(\bar{y}_1 + \bar{x}_1) = \bigoplus_{c_1=0}^{u} \bar{y}_1^{u-c_1} \bar{x}_1^{c_1} \qquad (۹)$$

حال، با توجه به رابطه‌ی صریح $\bar{x}_1$، داریم:

$$\bar{x}_1^{c_1} = (\bar{y}_2 + ... + \bar{y}_r)^{c_1} \qquad (۱۰)$$

و این، یعنی تابعی مانند f_1 با ANF $\bar{x}^{c_1}$؛ اکنون، قرار می‌دهیم $\bar{y}_3 + ... + \bar{y}_r = \bar{x}_2$ و دوباره از قضیه‌ی ۲-۱ استفاده می‌کنیم؛ داریم:

$$\bar{x}_1^{c_1} = f_1(\bar{x}_1) = f_1(\bar{y}_2 + \bar{x}_2) = \bigoplus_{c_2=0}^{c_1} \bar{y}_2^{c_1-c_2} \bar{x}_2^{c_2} \qquad (۱۱)$$

حال، رابطه‌ی (۱۱) را در رابطه (۹) جایگذاری می‌کنیم؛ داریم:

$$(۱۲)$$
$$f(\bar{y}_1 + \bar{y}_2 + ... + \bar{y}_r) = \bigoplus_{c_1=0}^{u} \bar{y}_1^{u-c_1} \bar{x}_1^{c_1}$$
$$= \bigoplus_{c_1=0}^{u} \bar{y}_1^{u-c_1} \left(\bigoplus_{c_2=0}^{c_1} \bar{y}_2^{c_1-c_2} \bar{x}_2^{c_2} \right)$$

[1] Boolean Function
[2] Algebraic Degree
[3] Hamming Weight
[4] Vector Boolean Function = S-Box
[5] Component Function

با ادامه‌ی روند بالا و به کارگیری مکرر قضیه‌ی ۲-۱، به رابطه‌ی ذیل می‌رسیم:

(۱۳)

$$f(\bar{y}_1+\bar{y}_2+...+\bar{y}_r)=$$
$$\bigoplus_{c_1=0}^{u}\bar{y}_1^{u-c_1}\left(\bigoplus_{c_2=0}^{c_1}\bar{y}_2^{c_1-c_2}\left(\bigoplus_{c_3=0}^{c_2}\bar{y}_3^{c_2-c_3}\left(...\left(\bigoplus_{c_{r-1}=0}^{c_r}\bar{y}_{r-1}^{c_{r-2}-c_{r-1}}\bar{y}_r^{c_{r-1}}\right)\right)\right)\right)$$

که رابطه‌ی (۱۳)، با تغییر متغیر به رابطه‌ی (۸) تبدیل می‌شود و لذا قضیه ثابت می‌گردد.

به کمک قضیه‌ی ۲-۲، درجه‌ی توابع بولی مؤلفه‌ای جمع پیمانه‌ای به پیمانه‌ی 2^t را می‌توان به صورت زیر به دست آورد:

اولاً، اگر در تابع $f(x)=\bar{x}^q$ قرار دهیم $q=2^0,2^1,...,2^{t-1}$، که t برابر اندازه‌ی پردازنده‌ی مورد نظر است، آنگاه با به دست آوردن درجه‌ی توابع مذکور، در واقع درجه‌ی توابع مؤلفه‌ای نگاشت بولی متناظر جمع پیمانه‌ای به پیمانه‌ی 2^t با r عملگر را می‌توان مشخص کرد.

ثانیاً، با توجه به رابطه‌ی (۸)، درمی‌یابیم که همه‌ی جملات در مجموع سمت راستِ این رابطه متمایزند و لذا، اگر در بین مجموعه‌ی همه‌ی $\{k_0,k_1,...,k_{t-1}\}$ ها، جوابی را بیابیم که در آن $\sum_{i=0}^{t-1}wt(k_i)$ بیشینه باشد، در واقع این مقدار با درجه‌ی توابع مؤلفه‌ای، متناظر می‌باشد.

۳- قضایای اصلی

فرض کنید n، u و t اعدادی صحیح و نامنفی باشند؛ معادله‌ی زیر را در نظر می‌گیریم:

$$X_1+X_2+...+X_{2^n}=2^u \pmod{2^t} \qquad (۱۴)$$

که در آن X_i ها، $1\le i\le 2^n$، اعدادی صحیح در Z_{2^t} هستند و $0\le u<t$. معادله‌ی (۱۴) دارای $\binom{2^u+2^n-1}{2^n}$ جواب صحیح نامنفی است. این مقدار برابر است با تعداد جمله‌ها در ANF $(u+1)$- امین تابع مولفه‌ای برای $0\le u<t$؛ در نتیجه، گزاره‌های زیر حاصل می‌شوند:

گزاره ۳-۱: تعداد جمله‌ها در ANF $(u+1)$- امین تابع مؤلفه‌ای جمع پیمانه‌ای به پیمانه‌ی 2^t با $r=2^n$ عملوند برابر است با $\binom{2^u+2^n-1}{2^n}$.

گزاره ۳-۲: تعداد متغیرها در ANF u- امین تابع مؤلفه‌ای جمع پیمانه‌ای به پیمانه 2^t با $r=2^n$ عملوند برابر است با ru.

اینک X_i را با نگاشت طبیعی اعداد صحیح، به بردارهای $\overline{X_i}$ تبدیل می‌کنیم. حال با توجه به قضیه‌ی ۲-۲ و رابطه‌ی (۸)، به دنبال جواب‌هایی برای معادله‌ی (۱۴) با مجموع وزن همینگ بیشینه هستیم. این جواب‌ها را جواب‌های می‌نامیم.

قضیه۳-۳ : با نمادهای بالا، در معادله‌ی (۱۴) و برای $n<u$، وزن همینگ جواب‌هایی که بهینه هستند، برابر است با:

$$\sum_{i=1}^{2^n}wt(X_i)=2^n(u-n)+2^{2n-u} \qquad n\ge u-n \qquad (۱۵)$$

(۱۶)

$$\sum_{i=1}^{2^n}wt(X_i)=(2^n-1)(u-n)+n+1 \qquad n<u-n$$

و اگر $n\ge u$، آنگاه وزن بیشینه برابر 2^n است.

برهان: برهان در دو بخش ارائه می‌گردد:

۱) $n<u$: این بخش خود به دو حالت تقسیم می‌شود: حالت اول برای $n\ge u-n$ و حالت دوم برای $n<u-n$. در ابتدا برای هر حالت جوابی را ارائه می‌کنیم و سپس نشان می‌دهیم که جواب ارائه شده بهینه می‌باشد.

جواب ارایه شده برای حالت اول برابر است با

$$X_1=X_2=...=X_{2^j}=2^{u-n+1}+2^{u-n}-1 \qquad (۱۷)$$
$$X_{2^j+1}=...=X_{2^n}=2^{u-n}-1$$

که در رابطه‌ی بالا داریم $u=2n-j$، $0\le j\le n-1$.

همچنین جواب ارائه شده برای حالت دوم برابر است با

$$X_1=X_2=...=X_{2^n-1}=2^{u-n}-1$$
$$X_{2^n}=2^n+2^{u-n}-1 \qquad (۱۸)$$

وزن جواب‌های ارائه شده برای حالت‌های اول و دوم برابر روابط (۱۵) و (۱۶) است؛ همچنین جواب‌های ارائه شده در رابطه‌ی (۱۴) صدق می‌کنند.

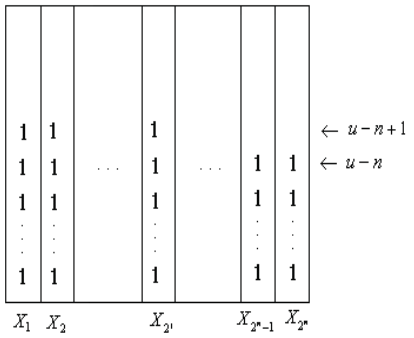
در ادامه، برای هر حالت یک جدول به نام جدول A در نظر می‌گیریم. جدول A دارای 2^n ستون می‌باشد. هر ستون از A متناظر با یک بردار $\overline{X_i}$ در $Z_2{}^t$ است. ستون‌های A از پایین به بالا با اندیس ۱ تا t شماره‌گذاری می‌شوند. هر درایه در A با $1\le i\le t, 1\le j\le 2^n$، $A(i,j)$ نمایش داده می‌شود.

$A(*,j)$ و $A(i,*)$ بـه ترتیب نمـایـانگر ستون j - ام و سطر i - ام A هستند؛ همچنین، تعداد 1های جدول A را با $one(A)$ نشان می‌دهیم.

در جدول A اگر داشته باشیم $A(i,j)=1$، آنگاه ارزش درایه‌ی $A(i,j)$ را برابر 2^{i-1} در نظر می‌گیریم؛ در غیر این صورت، ارزش آن برابر صفر است. با این توضیح، $sum(A)$ را مجموع ارزش‌های درایه‌های جدول A تعریف می‌کنیم.

حال، به دو حالتِ این بخش از برهان می‌پردازیم:

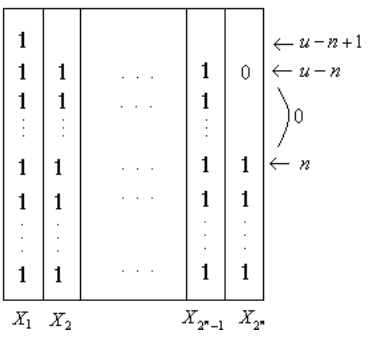
حـالـت اول، $n \geq u-n$: فـرض کنیـم $u=2n-j$، $0 \leq j \leq n-1$. جدول A برای جواب ارائه شده، به صورت شکل ۱ می‌باشد.



شکل ۱

با توجه به اینکه برای $1 \leq i \leq n-u+1$، تمامی درایه‌های 1 جدول A دارای کمترین ارزش می‌باشند، جواب ارائه شده بهینه است.

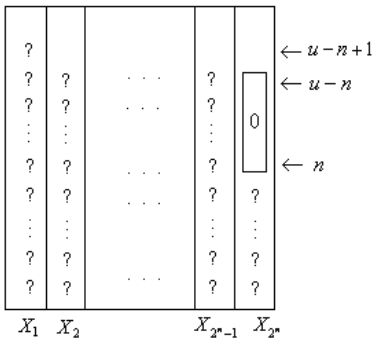
حالت دوم $n<u-n$: در این حالت جدول A برای جواب ارائه شده به صورت شکل ۲ است.



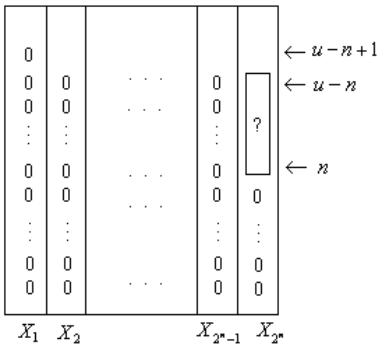
شکل ۲

فرض کنیم مجموعه جواب $\{Y_1, Y_2, ..., Y_{2^n-1}, Y_{2^n}\}$ با جدول B وجود داشته باشد که $one(B) > one(A)$.

جدول B^* را به صورتی تعریف می‌کنیم که در هر سطر، برای هر درایه‌ی غیر صفر $A(i,*)$، درایه‌ی متناظر آن در جدول B برابر صفر باشد. به همین ترتیب، جدول A^* را نیـز می‌سازیم. برای این دو جواب، جدول‌های A^* و B^* به ترتیب در شکل‌های ۳ و ۴ نمایش داده شده‌اند.



شکل ۳



شکل ۴

فـرض کنیـم k درایه‌ی 1 در جدول A^* در مکـان‌هـای $A^*(s_i+1,t_i)$، $1 \leq i \leq k$، مـوجـود بـاشـد. همچنین m درایـه‌ی 1 در مکـان‌هـای $B^*(l_j+1,2^n)$، $1 \leq j \leq m$ و $n<l_j<u-n$، در جدول B^* موجود باشد. برای این دو جدول داریم:

$$\begin{aligned} sum(A^*) &= 2^{s_1}+2^{s_2}+...+2^{s_k} \\ &= 2^{l_1}+2^{l_2}+...+2^{l_m} = sum(B^*) \end{aligned} \qquad (۱۹)$$

با توجـه بـه اینکـه تمامی درایـه‌های 1 در جدول B^* دارای ارزش‌هـای متمـایزی هستنـد (درایه‌های 1 تنها در $B^*(i,2^n)$ برای $n<i \leq u-n+1$ وجود دارند.) پس از ساده کردن طرفین رابطه‌ی (۱۹) و حذف مقادیر مساوی، با استفاده از فرض، داریم:

$$one(B^*) > one(A^*) \text{ و } sum(A^*) = sum(B^*) \qquad (۲۰)$$

توجـه داشتـه باشید کـه هیـچ یک از 2^{s_i} و 2^{l_j}ها، پس از ساده-سازی، برابر نیستند؛ در نتیجه، دو طرف رابطـه‌ی (۱۹) دارای

مؤلفه‌هـای متمایزی می‌باشند. بدون کاستن از کلیت مسأله فرض کنیم s_1 کوچکترین توان باشـد؛ آنگاه رابطـه‌ی (۱۳) بـه صورت زیر تغییر می‌کند:

$$1+2^{s_2-s_1}+\ldots+2^{s_k-s_1}=2^{l_1-s_1}+2^{l_2-s_1}+\ldots+2^{l_m-s_1} \quad (۲۱)$$

که یک تناقض است؛ پس جواب ارائه شده بهینه می‌باشد.

۲) $n \geq u$: در این بخش دو جواب ارائه می‌کنیم. برای $n=u$ جواب ارائه شده برابر است با:

$$X_1=X_2=\ldots=X_{2^n}=1 \quad (۲۲)$$

و برای $n>u$ برابر است با :

$$X_1=X_2=\ldots=X_{2^n}=1 \text{ و } X_{2^n+1}=\ldots=X_{2^u}=0 \quad (۲۳)$$

چون تمام درایه‌های 1 در این دو جواب در کمترین ارزش هستند، جواب‌های ارائه شده بهینه می‌باشند.

۴- الگوریتم یافتن جواب‌هایی با بیشترین وزن

در این بخش روشی کارامد برای حل مسأله‌ی یافتن درجه‌ی جبری توابع مؤلفه‌ای در حالت کلی، ارائه می‌کنیم. در پیوست، جدولی برای درجه جبری توابع مؤلفـه‌ای جمع پیمانه‌ای به پیمانه‌ی 2^{32} برای دو تا هشت عملوند ذکر شده است.

با توجه به فرض‌ها و نمادهای بخش ۳، در جدول A از جایگاه $A(1,1)$ شروع می‌کنیم و به ترتیب جایگاه‌های $A(1,2)$ و $A(1,3)$ و ... را برابر یک می‌کنیم. این روند را آنقدر ادامه می‌دهیم تا با افزایش یک 1، داشته باشیم $sum(A) \geq 2^u$. درایه‌های باقی مانده را صفر می‌کنیم. اگر $sum(A) > 2^u$، به طور معکوس، از سطر ماقبل پایانی شروع می‌کنیم و در هر سطر تـا جایی 1ها را حذف می‌کنیم که مجموع برابر 2^u شود. در غیر این صورت، به سطر پایین‌تر می‌رویم و همین روند را تکرار می‌کنیم تا مجموع برابر 2^u گردد.

جدول این جواب به شکلی است که در هر سطر (به جز سطر انتهایی) حداکثر یک درایه‌ی 0 وجود دارد؛ زیرا در غیر این صورت، می‌توان هر دو درایه‌ی 0 در یک سطر را با یک درایه‌ی 1 از سطر بالاتر جایگزین کرد.

حال نشان می‌دهیم که جواب به دست آمده یک جواب بهینه است: فرض کنیم جواب دیگری با وزن همینگ بیشتری موجود باشد. به این جواب جدول B را نسبت می‌دهیم و همانند بخش قبل، جدول‌های A^* و B^* را تشکیل می‌دهیم. فرض کنیم m درایه‌ی 1 در جایگاه‌هـای $A^*(k_i+1,s_i)$، به ازای $1 \leq i \leq m$ و n درایه‌ی 1 در جایگاه‌های $B^*(l_j+1,t_j)$، به ازای $1 \leq j \leq n$ موجود باشد. همانند رابطه‌ی (۱۹) داریم:

$$2^{l_1}+2^{l_2}+\ldots+2^{l_n}=2^{k_1}+2^{k_2}+\ldots+2^{k_m} \quad (۲۴)$$

حال اگر فرض کنیم l_1 کوچکترین توان باشد، خواهیم داشت:

$$1+2^{l_2-l_1}+\ldots+2^{l_n-l_1}=2^{k_1-l_1}+\ldots+2^{k_m-l_1} \quad (۲۵)$$

که یک تناقض است.

۵- نتیجه

در این مقاله، به بررسی خواص جبری جمع پیمانه‌ای به پیمانه‌ی 2^t پرداختیم. در واقع، بهترین تفسیر جبری یک عملگر، ANF توابع مؤلفه‌های آن است. یافتن درجه‌ی جبری توابع مؤلفه‌ای در مرتبه‌ی بعد قرار دارد ولی از اهمیت بسیار بالایی برخوردار است. ما این درجات را در چند حالت صریحاً به دست آوردیم و در حالت کلی نیز، الگوریتمی ارائه دادیم که در همه‌ی حالات کاربردی، به شکلی کارامد درجات جبری مؤلفه‌ها را به دست می‌آورد.

مراجع

[1] Bluetoth SIG, "Specification of the Bluetooth System", Verson 1.1, 1 Febrary 22, 2001, available at http://www.bluetooth.com.

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

[3] J. L. Massey, "SAFER K-64: A byte-oriented block-ciphering algorithm," in FastSoftware Encryption, FSE'93 (R. J. Anderson, ed.), vol. 809 of Lecture Notes inComputer Science, pp. 1–17, Springer-Verlag, 1994.

[4] X. Lai and J. Massey. "A proposal for a new block encryption standard". In I. Damg_ard, editor, Advances in Cryptology , Eurocrypt'90: Workshop on the Theory and Application of Cryptographic Techniques, Aarhus, Denmark, May 1990. Proceedings, volume 473 of LectureNotes in Computer Science, pages 389-404. Springer-Verlag, 1991.

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

[6] 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.

[7] 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.

[8] A. Braeken, I. Semaef, "The ANF of Composition of Addition and Multiplication mod 2^n with a Boolean Function", FSE'05, LNCS 3557, pp. 112-125, Springer-Verlag, 2005.

پیوست

درجات توابع مؤلفه‌ای برای جمع پیمانه‌ای به پیمانه‌ی 2^{32} برای سه تا هشت عملوند

	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵
۲	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶
۳	۱	۲	۳	۵	۷	۹	۱۱	۱۳	۱۵	۱۷	۱۹	۲۱	۲۳	۲۵	۲۷	۲۹
۴	۱	۲	۴	۶	۹	۱۲	۱۵	۱۸	۲۱	۲۴	۲۷	۳۰	۳۳	۳۶	۳۹	۴۲
۵	۱	۲	۴	۶	۹	۱۳	۱۷	۲۱	۲۵	۲۹	۳۳	۳۷	۴۱	۴۵	۴۹	۵۳
۶	۱	۲	۴	۷	۱۱	۱۵	۲۰	۲۵	۳۰	۳۵	۴۰	۴۵	۵۰	۵۵	۶۰	۶۵
۷	۱	۲	۴	۷	۱۱	۱۶	۲۲	۲۸	۳۴	۴۰	۴۶	۵۲	۵۸	۶۴	۷۰	۷۶
۸	۱	۲	۴	۸	۱۲	۱۸	۲۵	۳۲	۳۹	۴۶	۵۳	۶۰	۶۷	۷۴	۸۱	۸۸

	۱۶	۱۷	۱۸	۱۹	۲۰	۲۱	۲۲	۲۳	۲۴	۲۵	۲۶	۲۷	۲۸	۲۹	۳۰	۳۱
۲	۱۷	۱۸	۱۹	۲۰	۲۱	۲۲	۲۳	۲۴	۲۵	۲۶	۲۷	۲۸	۲۹	۳۰	۳۱	۳۲
۳	۳۱	۳۳	۳۵	۳۷	۳۹	۴۱	۴۳	۴۵	۴۷	۴۹	۵۱	۵۳	۵۵	۵۷	۵۹	۶۱
۴	۴۵	۴۸	۵۱	۵۴	۵۷	۶۰	۶۳	۶۶	۶۹	۷۲	۷۵	۷۸	۸۱	۸۴	۸۷	۹۰
۵	۵۷	۶۱	۶۵	۶۹	۷۳	۷۷	۸۱	۸۵	۸۹	۹۳	۹۷	۱۰۱	۱۰۵	۱۰۹	۱۱۳	۱۱۷
۶	۷۰	۷۵	۸۰	۸۵	۹۰	۹۵	۱۰۰	۱۰۵	۱۱۰	۱۱۵	۱۲۰	۱۲۵	۱۳۰	۱۳۵	۱۴۰	۱۴۵
۷	۸۲	۸۸	۹۴	۱۰۰	۱۰۶	۱۱۲	۱۱۸	۱۲۴	۱۳۰	۱۳۶	۱۴۲	۱۴۸	۱۵۴	۱۶۰	۱۶۶	۱۷۲
۸	۹۵	۱۰۲	۱۰۹	۱۱۶	۱۲۳	۱۳۰	۱۳۷	۱۴۴	۱۵۱	۱۵۸	۱۶۵	۱۷۲	۱۷۹	۱۸۶	۱۹۳	۲۰۰