



## ویژگی های جبری جمع پیمانه ای به پیمانه ی $2^t$

سید مجتبی دهنوی<sup>۱</sup>، علیرضا رحیمی پور<sup>۲</sup>

دانشگاه تربیت معلم<sup>۱</sup>

Dehnavism@tmu.ac.ir

<sup>۲</sup> Alirezarahimipour@yahoo.com

### چکیده

جمع پیمانه ای به پیمانه ی  $2^t$ ، یکی از عملگرهای پر کاربرد در رمزنگاری متقارن است و بررسی خواص این عملگر، نقش مهمی در طراحی و تحلیل رمزها ایفا می کند. از آنجا که تحلیل جبری این عملگر برای  $r=2$  عملوند، در مقاله ای به تألیف مؤلفان همین مقاله، در ششمین کنفرانس رمز ایران انجام شده است، در این مقاله با استفاده از نتایج پژوهش های پیشین، به بررسی جبری جمع پیمانه ای به پیمانه ی  $2^t$  پرداخته، درجات توابع بولی مؤلفه ای این عملگر را (به عنوان یک نگاشت بولی) در حالت کلی، به دست می آوریم. همچنین به عنوان یک کاربرد، درجه ی توابع مؤلفه ای مذکور را برای یکی از پرکاربردترین حالات، یعنی تبدیل های PHT به کار رفته در رمزهای قالبی و دنباله ای به دست می آوریم.

### واژه های کلیدی

جمع پیمانه ای به پیمانه ی  $2^t$ ، توابع بولی، فرم نرمال جبری، درجه ی جبری.

### ۱- مقدمه

پیمانه ی  $2^t$  با  $r$  عملوند، در حالتی که  $r$  توانی از ۲ است را به دست آورده ایم. در این مقاله، درجه ی جبری توابع مؤلفه ای را برای جمع پیمانه ای به پیمانه ی  $2^t$ ، در حالت کلی، به دست می آوریم. یکی از کاربردهای مهم جمع پیمانه ای به پیمانه ی  $2^t$ ، عبارت است از تبدیلات PHT<sup>۲</sup> که در برخی رمزهای قالبی و دنباله ای استفاده شده است. ما، درجات توابع بولی مؤلفه ای این تبدیلات را نیز - که از یک منظر - تعمیمی از عملگر جمع پیمانه ای است، به عنوان کاربردی از نتایج حاصله، محاسبه می کنیم. در بخش ۲ به تعاریف و قضایای مقدماتی می پردازیم. بخش ۳ به مرور و بیان نتایج به دست آمده در [1] اختصاص دارد. بخش ۴ شامل قضایا و نتایج اصلی می باشد. در بخش ۵، کاربردی از نتایج به دست آمده روی تبدیلات PHT<sup>۲</sup> ارائه می گردد و در پایان در بخش ۶، به نتیجه گیری می پردازیم.

یکی از عملگرهایی که تاکنون بیشترین کاربرد را در رمزنگاری متقارن داشته، جمع پیمانه ای به پیمانه ی  $2^t$  می باشد که در آن،  $t$  عددی صحیح و مثبت و معمولاً برابر اندازه ی پردازنده های نوعی - یعنی ۸، ۱۶، ۳۲ و یا ۶۴ - است. به عنوان مثال، این عملگر در رمزهای بلوکی [2] Twofish و [3] RC6 و رمز دنباله ای [4] RC4 - به کار رفته است. در [5]، ویژگی های جبری جمع پیمانه ای به پیمانه ی  $2^t$  با دو عملوند مورد بررسی قرار گرفته و ANF<sup>۱</sup> توابع بولی مؤلفه ای آن، به طور صریح به دست آمده است. برای بسیاری از کاربردها در طراحی و ارزیابی رمزهای متقارن، دانستن درجه ی جبری توابع مؤلفه ای، اهمیت شایانی دارد. در [1]، روابطی صریح برای درجه ی جبری توابع بولی مؤلفه ای جمع پیمانه ای به

<sup>۲</sup> Pseudo-Hadamard Transform

<sup>۱</sup> Algebraic Normal Form

هر تابع  $f: F_2^t \rightarrow F_2^m$  با  $m > 1$ ، تابع بولی برداری<sup>۴</sup> یا یک نگاشت بولی نامیده می‌شود. این تابع را می‌توان به وسیله‌ی بردار  $(f_1, f_2, \dots, f_m)$  بیان کرد که هر  $f_i$ ،  $1 \leq i \leq m$ ، یک تابع بولی  $f_i: F_2^t \rightarrow F_2$  است: به این توابع، تابع‌های مؤلفه‌ای<sup>۵</sup> می‌گوییم. می‌توان ثابت کرد که معادل بولی جمع  $\bar{x}$  و  $\bar{y}$  در  $Z_{2^t}$ ، یعنی  $\bar{f} = \bar{x} + \bar{y} \pmod{2^t}$ ، به عنوان یک نگاشت بولی، به صورت ذیل است:

$$\begin{aligned} r_0 &= x_0 \oplus y_0 \oplus c_0, \quad c_0 = 0 \\ r_i &= x_i \oplus y_i \oplus c_i, \quad c_i = x_{i-1}y_{i-1} \oplus x_{i-1}c_{i-1} \oplus y_{i-1}c_{i-1} \end{aligned} \quad (6)$$

**قضیه ۱-۲:** فرض کنیم ANF تابع بولی  $f: F_2^t \rightarrow F_2$  یک تک‌جمله‌ای  $\bar{x}^u$  با  $u \in Z_{2^t}$  باشد؛ در این صورت، ANF تابع  $f(\bar{x} + \bar{y})$  به صورت زیر است:

$$f(\bar{x} + \bar{y}) = \bigoplus_{c=0}^u \bar{x}^{(u-c)} \bar{y}^c \quad (7)$$

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

**برهان:** [5].

**قضیه ۲-۲:** اگر تابع  $f$  به شکل تعریف شده در قضیه‌ی ۱-۲ باشد، آنگاه ANF تابع  $f(\bar{y}_1 + \bar{y}_2 + \dots + \bar{y}_r)$ ، به صورت ذیل است:

$$f(\bar{y}_1 + \bar{y}_2 + \dots + \bar{y}_r) = \bigoplus_{\substack{k_1, \dots, k_r \geq 0 \\ k_1 + \dots + k_r = u}} \bar{y}_1^{k_1} \dots \bar{y}_r^{k_r} \quad (8)$$

**برهان:** [1,5].

به کمک قضیه‌ی ۲-۲، درجه‌ی توابع بولی مؤلفه‌ای جمع پیمانه‌ای به پیمانه‌ی  $2^t$  را می‌توان به این روش به دست آورد: اولاً، اگر به ازای  $q = 2^0, 2^1, \dots, 2^{t-1}$  که در اینجا  $t$  برابر اندازه‌ی پردازنده است، قرار دهیم  $f(\bar{x}) = \bar{x}^q$ ، در این صورت، با به دست آوردن درجه‌ی توابع مذکور، در واقع درجه‌ی توابع مؤلفه‌ای نگاشت بولی متناظر جمع پیمانه‌ای به پیمانه‌ی  $2^t$ ، با  $r$  عملوند را به دست آورده‌ایم. ثانیاً، با توجه به رابطه‌ی (8)، درمی‌یابیم که همه‌ی جملات در مجموع سمت راست این رابطه متمایزند و لذا، اگر در بین مجموعه‌ی همه‌ی  $\{k_1, k_1, \dots, k_r\}$  ها، جوابی را بیابیم که در آن  $\sum_{i=1}^r wt(k_i)$  بیشینه باشد، در واقع، درجه‌ی تابع مؤلفه‌ای متناظر را یافته‌ایم.

## ۲- تعاریف و قضایای مقدماتی!

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

$$\begin{aligned} \varphi: F_2^t &\rightarrow Z_{2^t} \\ \bar{x} = (x_{t-1}, \dots, x_0) &\mapsto \varphi(\bar{x}) = \sum_{i=0}^{t-1} x_i 2^i \end{aligned} \quad (1)$$

در نمایش بالا،  $x_i$  را مؤلفه‌ی مکان  $(i+1) - \text{ام}$  یا  $\bar{x}$  می‌نامیم.

حال، ترتیب جزئی  $\leq$  را روی  $F_2^t$  به صورت زیر تعریف می‌کنیم:

$$\bar{x} \leq \bar{a} \Leftrightarrow x_i \leq a_i, \quad 0 \leq i < t \quad (2)$$

در نمایش بالا اگر

$$\bar{x} = (x_{t-1}, \dots, x_0) \text{ و } u = \sum_{i=0}^{t-1} u_i 2^i \equiv (u_{t-1}, \dots, u_0) \quad (3)$$

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

هر تابع  $f: F_2^t \rightarrow F_2$  را یک تابع بولی<sup>۱</sup> می‌نامند: فرض کنید  $f(x)$  تابعی بولی باشد؛  $f$  را می‌توان به شکلی یکتا که آن را فرم نرمال جبری (ANF) می‌نامیم، نشان داد. در واقع، داریم:

$$f(\bar{x}) = \bigoplus_{u \in Z_{2^t}} h_u \bar{x}^u, \quad h_u \in F_2 \quad (4)$$

که در آن ضرایب  $h_u$  به صورت زیر تعیین می‌شوند:

$$h_u = h(\bar{u}) = \bigoplus_{\bar{x} \leq \bar{u}} f(\bar{x}) \quad (5)$$

درجه‌ی جبری<sup>۲</sup> تابع  $f$ ، برابر با تعداد متغیرها در طولانی‌ترین جمله‌ی ANF یا به طور معادل، بیشترین وزن همینگ<sup>۳</sup>  $\bar{u}$ ،  $wt(\bar{u})$ ، در میان جملات با  $h_u \neq 0$ ، تعریف می‌شود.

<sup>1</sup> Boolean Function

<sup>2</sup> Algebraic Degree

<sup>3</sup> Hamming Weight

<sup>4</sup> Vectorial Boolean Function = S-Box

<sup>5</sup> Component Function

### ۳- حالت $r = 2^n$ !

$$j = 2^{u-r} + [n2^{-r}] - n + 1 \quad (15)$$

فرض کنیم  $n, u$  و  $t$  سه عدد صحیح نامنفی باشند. رابطه‌ی (9) را در نظر بگیرید:

$$X_1 + X_2 + \dots + X_{2^n} = 2^u \quad (9)$$

که در آن  $X_i$  ها،  $1 \leq i \leq 2^n$ ، عضو  $Z_2$  هستند و  $0 \leq u < t$ . قضیه‌ی ذیل را داریم:

**قضیه ۳-۱:** برای  $n < u$ ، وزن همینگ جواب‌های با وزن همینگ بیشینه برابر است با

$$\sum_{i=1}^{2^n} wt(X_i) = 2^n(u-n) + 2^{2^n-u} \quad n \geq u-n, \quad (10)$$

$$\sum_{i=1}^{2^n} wt(X_i) = (2^n-1)(u-n) + n + 1 \quad n < u-n; \quad (11)$$

و اگر  $n \geq u$ ، وزن همینگ بیشینه برابر است با  $2^n$ .

**برهان:** [1].

### ۴- حالت کلی

در این بخش با استفاده از الگوریتم بیان و اثبات شده در [1]، وزن همینگ جواب بهینه‌ی معادله‌ی  $X_1 + X_2 + \dots + X_n = 2^u$  در حالت کلی برای  $n$  جمعوند به دست می‌آوریم؛ این جواب، در واقع برابر درجه‌ی جبری توابع مؤلفه‌ای جمع پیمانه‌ای به پیمانه‌ی  $2^t$  در حالت کلی است.

$$f(\bar{y}_1 + \bar{y}_2 + \dots + \bar{y}_n) = \bigoplus_{\substack{k_1, \dots, k_n \geq 0 \\ k_1 + \dots + k_n = 2^t}} \bar{y}_1^{k_1} \dots \bar{y}_n^{k_n}. \quad (12)$$

در اینجا، ANF تابع بولی  $f: F_2^m \rightarrow F_2$ ، یک تک‌جمله‌ای  $\bar{x}^{2^u}$  با  $2^u = 2^0, 2^1, \dots, 2^{t-1}$  می‌باشد.

در معادله‌ی  $X_1 + X_2 + \dots + X_n = 2^u$ ، اگر  $n > 2^u$ ، آنگاه تعدادی از  $X_i$  ها حتماً صفر هستند و معادله، تبدیل به معادله‌ای با شرط  $n \leq 2^u$  می‌شود؛ بنابراین در ادامه، همواره شرط  $n \leq 2^u$  را فرض می‌گیریم.

**قضیه ۴-۱:** وزن جواب بهینه یا جواب با وزن بیشینه معادله‌ی

$$X_1 + X_2 + \dots + X_n = 2^u$$

$$nr + j - wt(X^*) \quad (13)$$

که در اینجا،

$$r = \left\lceil \log_2 \left( \frac{2^u + n}{n} \right) \right\rceil \quad (14)$$

**برهان:** در ابتدا، الگوریتم ارائه شده در [1] را مرور می‌کنیم: در جدولی مشابه جدول شکل ۱، از سطر پایین و سمت چپ شروع می‌کنیم و به ترتیب، جایگاه‌های بعدی را در سطر اول برابر '1' قرار می‌دهیم و در صورت نیاز به سطر بالاتر می‌رویم. این روند را آنقدر ادامه می‌دهیم تا با افزایش یک '1'، مجموع ارزش‌های جدول بیشتر از یا مساوی با  $2^u$  شود. روشن است که بقیه‌ی درایه‌های جدول برابر '0' است؛ حال، اگر مجموع ارزش‌های جدول به طور اکید از  $2^u$  بیشتر باشد، به طور معکوس، از سطر ماقبل پایانی شروع می‌کنیم و در صورت امکان پس از '0' کردن یک درایه، به سطر پایین‌تر می‌رویم؛ این روند را تا جایی ادامه می‌دهیم که مجموع برابر  $2^u$  شود.

انکون، با استفاده از مفاهیم مطرح‌شده‌ی فوق و با توجه به الگوریتم مذکور در [1]، برای یافتن جواب بهینه، باید جدولی به صورت شکل ۱ را تشکیل داد: در این جدول، با افزودن یک '1' به سطر  $r+1$  و ستون  $j$  - ام، مجموع ارزش‌های جدول، از مقدار  $2^u$  بیشتر شده است.

چون ارزش هر '1' در سطر  $i$  - ام برابر  $2^{i-1}$  است، مقدار  $r$  از رابطه زیر به دست می‌آید:

$$n(2^r - 1) \leq 2^u < n(2^{r+1} - 1) \quad (17)$$

که با ساده کردن رابطه‌ی بالا، داریم:

$$r = \left\lceil \log_2 \left( \frac{2^u + n}{n} \right) \right\rceil = \left\lceil \log_2(2^u + n) - \log_2(n) \right\rceil \quad (18)$$

$$= u + \left\lceil \log_2 \left( 1 + \frac{n}{2^u} \right) - \log_2 n \right\rceil$$

1	1	...	1	0	...	0	← r
1	1	...	1	1	...	1	
.	.	...	.	.	...	.	
.	.	...	.	.	...	.	
.	.	...	.	.	...	.	
1	1	...	1	1	...	1	
1	1	...	1	1	...	1	
$X_1$	$X_2$	...	$X_j$	$X_{j+1}$	...	$X_n$	

شکل ۱

$$\begin{aligned} X_{u+1}^* &= [n2^{-(r+1)}]2^{r+1} - n + 2^{r+1} \\ &= 2^{r+1} - n = 2^r + 2^r - n \\ &= X_u^* + 2^r \end{aligned} \quad (25)$$

که به وضوح، داریم:

$$wt(X_{u+1}^*) = wt(X_u^*) + 1 \quad (26)$$

پس اگر وزن جواب بهینه برای معادله‌ی  $X_1 + X_2 + \dots + X_n = 2^u$  برابر  $w_u$  باشد، وزن جواب بهینه برای معادله‌ی  $X_1 + X_2 + \dots + X_n = 2^{u+1}$  برابر است با:

$$\begin{aligned} n(r+1) + j - wt(X_{u+1}^*) \\ = nr + n + j - wt(X_u^*) - 1 \\ = w_u + (n-1) \end{aligned} \quad (27)$$

### ۵- کاربرد ی از قضیه‌ی اصلی!

تبدیلات  $PHT$ ، یکی از تبدیلات کاربردی در رمزنگاری هستند که از عملگر جمع پیمانه‌ای استفاده می‌کنند. اگر ورودی‌های این تبدیل در حالت دو عملوند،  $(x, y)$  و خروجی‌های آن برابر  $(x', y')$  باشد، داریم:

$$(x', y') = (x + y, 2x + y) \quad (28)$$

درجه‌ی جبری مؤلفه‌ی اول، در بخش قبلی به دست آمد. در ادامه، درجه‌ی جبری رابطه‌ی دوم را می‌یابیم: برای این منظور، از تابع  $f$ ، تعریف شده توسط مؤلفه‌ی دوم در (28) استفاده می‌کنیم:

$$f(\bar{x}, \bar{y}) = \bigoplus_{\substack{k, k' \geq 0 \\ k+k'=2^r}} (2\bar{x})^k \bar{y}^{k'} \quad (29)$$

درجات جبری مؤلفه‌ی  $2x + y$ ، به ازای  $2^0, 2^1, \dots, 2^{r-1}$  به دست می‌آید. در رابطه‌ی بالا، با توجه به این که بیت کم ارزش  $2x$  همواره برابر صفر است، برای به دست آوردن بیشترین درجه، لزوماً باید  $k$  عددی زوج باشد. پس برای این منظور، باید جوابی از رابطه‌ی زیر با بیشترین وزن را بیابیم:

$$k + k' = 2^u; \quad k, k' \geq 0, \quad k \bmod 2 = 0 \quad (30)$$

برای به دست آوردن مقدار  $j$ ، به صورت زیر عمل می‌کنیم:

$$n(2^r - 1) + (j-1)2^r < 2^u \leq n(2^r - 1) + j2^r \quad (15)$$

که پس از ساده کردن رابطه‌ی فوق، داریم:

$$j = 2^{u-r} + [n2^{-r}] - n + 1 \quad (19)$$

چون درایه‌ی واقع در سطر  $r+1$  و ستون  $j$ -ام، درایه‌ای است که با افزودن آن، مجموع مقادیر ارزش‌های جدول، از  $2^u$  بیشتر می‌شود، پس بیشترین وزن، با کم کردن وزن مقدار اضافی از وزن کل جدول به دست می‌آید؛ این مقدار اضافی به صورت زیر محاسبه می‌شود:

$$X^* = (n(2^r - 1) + j2^r) - 2^u \quad (20)$$

حال، با قرار دادن مقدار  $r$  و  $j$  در رابطه‌ی بالا، به تساوی زیر می‌رسیم:

$$X^* = [n2^{-r}]2^r - n + 2^r \quad (21)$$

نتیجه ۴-۴: اگر برای معادله‌ی (9) داشته باشیم  $2^r > n$ ، آنگاه وزن جواب بهینه‌ی معادله‌ی  $X_1 + X_2 + \dots + X_n = 2^{u+1}$  با افزودن  $n-1$  واحد به وزن جواب بهینه‌ی معادله‌ی (9) به دست می‌آید.

برهان: با فرض  $2^r > n$ ، چون همواره  $2^u \geq 2^r$ ، با توجه به (18) و با استفاده از زیرنویس به جهت رفع ابهام، رابطه  $r_{u+1}$  به صورت زیر به دست می‌آید:

$$\begin{aligned} r_{u+1} &= (u+1) + \left[ \log_2 \left( 1 + \frac{n}{2^{u+1}} \right) - \log_2 n \right] \\ &= \left( u + \left[ \log_2 \left( 1 + \frac{n}{2^{u+1}} \right) - \log_2 n \right] \right) + 1 = r_u + 1 \end{aligned} \quad (22)$$

همچنین مقدار  $j$  برای دو معادله تغییر نمی‌کند، زیرا

$$\begin{aligned} j_{u+1} &= [2^{(u+1)-(r+1)} + n2^{-(r+1)} - n] + 1 \\ &= 2^{u-r} + [n2^{-(r+1)}] - n + 1 = j_u \end{aligned} \quad (23)$$

با توجه به رابطه‌ی  $2^r > n$ ، مقدار  $X^*$  برای معادله‌ی  $X_1 + X_2 + \dots + X_n = 2^u$  به صورت زیر تغییر می‌کند:

$$X_u^* = 2^r - n \quad (24)$$

از نتایج مقدار  $X^*$  برای معادله‌ی  $X_1 + X_2 + \dots + X_n = 2^{u+1}$  از رابطه‌ی ذیل به دست می‌آید:

پس وزن جواب بهینه برای این تبدیل، از رابطه‌ی ذیل محاسبه می‌شود:

$$2r-1-wt(X^*) \quad (38)$$

که در حالات  $u \neq 0,1$  داریم:

$$\begin{aligned} 2r-u+1 & \quad j=1 \\ 2r-u & \quad j=2 \end{aligned} \quad (39)$$

به همین طریق، می‌توان درجه جبری تبدیلاتی به صورت  $2^l x + y$  و یا  $2^l x + 2^{l/2} y$  را که تعمیمی از تبدیلات شبه آدامار هستند، به دست آورد. در ادامه، درجه‌ی جبری تبدیلات شبه آدامار به فرم

$$\sum_{i=1}^n 2^{l_i} x_i \quad (40)$$

را در حالت کلی می‌یابیم. (توجه داشته باشید که باید داشته باشیم  $2^{l_i} \leq 2^u$ ؛ زیرا در غیر این صورت، متغیر  $X_i$  نمی‌تواند تأثیری داشته باشد.) برای یافتن درجه‌ی جبری توابع مؤلفه‌ای این تبدیل، با استفاده از تابع  $f$  مناسب، داریم:

$$f(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n) = \bigoplus_{\substack{k_1, \dots, k_n \geq 0 \\ k_1 + \dots + k_n = 2^u}} (2^{l_1} \bar{x}_1)^{k_1} \dots (2^{l_n} \bar{x}_n)^{k_n} \quad (41)$$

بیشترین درجه، با یافتن جوابی از معادله  $k_1 + k_2 + \dots + k_n = 2^u$  با بیشترین وزن و صادق در قیدهای  $k_1 > 2^{l_1}, \dots, k_n > 2^{l_n}$ ، به دست می‌آید؛ البته، قبل از یافتن درجه جبری، بدون کاسته شدن از کلیت، فرض می‌کنیم که معادله ساده شده باشد: یعنی عوامل مشترک ضربی از دو طرف معادله حذف شده‌اند. در این قسمت نیز همواره فرض می‌کنیم  $n \leq 2^u$ .

برای یافتن جواب بهینه، از الگوریتم [1]، با جدول تغییر یافته‌ی شکل ۳ استفاده می‌کنیم. چون در تبدیل برداری  $2^{l_i} X_i$ ، به تعداد  $l_i$  بیت با شروع از بیت کم ارزش برابر صفر است، در جدول، برای ستون متناظر با  $X_i$  از سطر پایین تا سطر  $l_i$  را برابر صفر قرار می‌دهیم.

j						
1	...	1	0	...	0	← r
1		1	1		1	
.		.	.		.	
.		.	.		.	
1		1	1		1	
0	...	1	1	...	1	
0		1	0		1	
0		0	0		0	
.		.	.		.	
.		.	.		.	
0	...	0	0	...	0	
$X_1$		$X_j$	$X_{j+1}$		$X_n$	

شکل ۳

الگوریتم مطلوب را بر جدولی تغییر یافته به صورت شکل ۲ اعمال می‌کنیم:

j		
1	0	← r
1	1	
.	.	
.	.	
1	1	
1	1	
0	1	
$2x$	$y$	

شکل ۲

برای به دست آوردن  $r$ ، داریم:

$$2(2^r-1)-1 \leq 2^u < 2(2^{r+1}-1)-1 \quad (31)$$

که پس از ساده کردن نامساوی فوق، به رابطه‌ی ذیل برای  $r$  دست می‌یابیم:

$$r = \lceil \log_2(2^u + 3) \rceil - 1 \quad (32)$$

مقدار  $r$  برای تمامی حالت‌ها، بجز حالتی که  $u=0,1$ ، به صورت زیر ساده می‌شود:

$$r = u + \left\lceil \log_2 \left(1 + \frac{3}{2^u}\right) \right\rceil - 1 = u - 1 \quad (33)$$

مقدار  $j$  نیز به صورت زیر محاسبه می‌شود:

$$2(2^r-1) + (j-1)2^r - 1 < 2^u \leq 2(2^r-1) + j2^r - 1 \quad (34)$$

و

$$j = 2^{u-r} + \lceil 3.2^{-r} \rceil - 1 \quad (35)$$

برای تمامی حالت‌ها، بجز حالتی که  $u=0,1$ ، چون  $r = u - 1$  داریم:

$$j = \lceil 3.2^{-r} \rceil + 1 \quad (36)$$

چون  $r > 0$ ، پس همواره  $j=1,2$  و

$$\begin{aligned} X^* &= 2(2^r-1)-1 + j2^r - 2^u \\ &= (j+2)2^r - 2^u - 3 \end{aligned} \quad (37)$$

برای حالتی که  $u \neq 0,1$  و  $j=1$ ، داریم:  $X^* = 2^{u-1} - 3$  و  $wt(X^*) = u - 2$  و برای  $j=2$  داریم:  $X^* = 2^u - 3$  و  $wt(X^*) = u - 1$ .

مؤلفه‌های تبدیلات PHT را مورد بررسی قرار دادیم. روشن است که در ادامه‌ی تحقیق جاری، می‌توان اطلاعات بیشتری از ANF توابع مؤلفه‌های مذکور را، در حالت کلی، استخراج کرد.

### مراجع

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

[2] 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>.

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

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

[5] 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, 2003.

حال، مقدار  $r$  از رابطه‌ی زیر به دست می‌آید:

$$n(2^r - 1) - \sum_{i=1}^n (2^{l_i} - 1) \leq 2^u \quad (42)$$

$$< n(2^{r+1} - 1) - \sum_{i=1}^n (2^{l_i} - 1)$$

که پس از ساده کردن به تساوی زیر می‌رسیم:

$$r = \left\lceil \log_2 \left( 2^u + \sum_{i=1}^n 2^{l_i} \right) - \log_2 n \right\rceil \quad (43)$$

$$r = u + \left\lceil \log_2 \left( 1 + \left( \sum_{i=1}^n 2^{l_i} \right) / 2^u \right) - \log_2 n \right\rceil \quad (44)$$

چون همواره  $n \leq 2^u$ ، پس  $\log_2 n \leq u$  و در نتیجه  $r \geq 0$  است و

زمانی که  $\sum_{i=1}^n 2^{l_i} > 2^u$ ، آنگاه  $r = 0$  می‌شود. برای محاسبه‌ی  $j$  به صورت زیر عمل می‌کنیم:

$$n(2^r - 1) - \sum_{i=1}^n (2^{l_i} - 1) + (j-1)2^r < 2^u \quad (45)$$

$$\leq n(2^r - 1) - \sum_{i=1}^n (2^{l_i} - 1) + j2^r$$

پس از ساده کردن، داریم:

$$j = 2^{u-r} + \left\lceil \left( \sum_{i=1}^n 2^{l_i} \right) / 2^r \right\rceil - n + 1 \quad (46)$$

و مقدار  $X^*$  نیز به شکل زیر به دست می‌آید:

$$X^* = n(2^r - 1) - \sum_{i=1}^n (2^{l_i} - 1) + j2^r - 2^u \quad (47)$$

$$= (j+n)2^r - \sum_{i=1}^n 2^{l_i} - 2^u$$

و وزن جواب بهینه برابر است با

$$nr + j - wt(X^*) - \sum_{i=1}^n l_i \quad (48)$$

### ۶- نتیجه گیری!

در این مقاله، به بررسی خواص جبری جمع پیمانه‌ای به پیمانه‌ی  $2^t$  پرداختیم. بهترین تفسیر جبری یک عملگر عبارت است از به دست آوردن ANF توابع مؤلفه‌ای آن و البته یافتن درجه‌ی جبری توابع مؤلفه‌ای نیز از اهمیت بسیار بالایی برخوردار است. ما این درجات را برای جمع پیمانه‌ای، در حالت کلی، به دست آوردیم و به عنوان کاربردی از نتایج به دست آمده، درجه‌ی جبری توابع