نشریه بین المللی علوم مهندسی دانشگاه علم و صنعت ایران، شماره ۷، جلد ۱۹، سال ۱۳۸۷، صفحه ۸۶-۸۳
مهندسی شیمی، ریاضی و کامپیوتر

# USING ORTHOGONAL PIECEWISE CONSTANT BASIS FUNCTIONS IN SHAMIR THRESHOLD SCHEME

**Kh. Maleknezhad, M. Shahrezaee & M. Falah. Aliabadi**

**Iran University of Science and Technology,**
**maleknejad@iust.ac.ir**

**Abstract:** In Shamir threshold scheme one that is called dealer, chooses the key and then shares some partial information about it, called among the participants, secretly. In this paper, we use some numerical methods with piecewise constant basis functions in Shamir threshold scheme. We first introduce operational matrix of this functions and then show how dealer multiplies this matrix by vector of shares to obtain a new vector and distributes it.

# استفاده از توابع پایه‌ای قطعه‌ای ثابت متعامد در طرح آستانه شمیر (*shamir*)

**خسرو مالک نژاد، محسن شاهرضایی و مهناز فلاح علی آبادی**

**چکیده:** در طرح آستانه شمیر (*shamir*) فردی به نام واسطه تعدادی سهام را بین سهامداران توزیع می‌کند که منجر به یک چند جمله ای می شود. برای محاسبه ضرایب این چند جمله ای که منجر به یافتن کلید می شود روشهای گوناگونی وجود دارد. [۱و۲]. جایگزینی روش ورونیابی تفاضلهای منقسم به جای درونیابی لاگرانژ و رجحان این روش به لحاظ تعداد عملیات در مرجع [۶] نشان داده شده است. در این مقاله ضمن استفاده از روش درونیابی تفاضلهای منقسم، مقادیر توزیع شده توسط واسطه به عنوان یک بردار درنظر گرفته شده و با استفاده از ماتریس عملیاتی توابع پایه ای متعامد قطعه ای ثابت [۳و۴] بردار جدیدی تولید می شود و در اختیار سهامداران قرار می‌گیرد. واسطه می تواند یکی از سهامداران ویژه را انتخاب کرده و ماتریس به کار رفته را در اختیار او قرار دهد. بدیهی است که یافتن کلید مجهول بدون حضور این سهام دار ویژه امکان پذیر نیست.

**کلمات کلیدی:** رمز، رمزنگاری، رمزگشایی، توابع پایه ای متعامد قطعه ای ثابت، درونیابی، تفاضلات منقسم نیوتن

## ۱. مقدمه

استفاده از توابع پایه‌ای قطعه‌ای ثابت (*PCBF*) به دلیل آنکه ماتریس‌های متناظرشان اسپارس می‌باشند در روشهای عددی متداول است. از جمله این گونه توابع می توان به توابع بلاک-پالس، هار و والش اشاره کرد [۴]. در این مقاله ابتدا روش $(t,w)$- طرح آستانه شمیر توضیح داده می‌شود، سپس ضمن معرفی توابع بلاک-پالس و ماتریسهای عملیاتب متناظر، طرز استفاده از آنها در توزیع سهام تشریح خواهد شد.

## ۲. طرح آستانه شمیر

فرض کنید $t$ و $w$ اعدا صحیح مثبت باشند و $t \le w$، یک $(t,w)$- طرح آستانه روشی برای سهم بندی یک کلید $k$ بین مجموعه ای از $w$ سهام دار است (که با $p$ نشان داده می‌شود) به نحوی که هر $t$ تا سهام

**تاریخ وصول: ۸۴/۲/۱۵**
**تاریخ تصویب: ۸۵/۱/۲۶**

**دکتر خسرو مالک نژاد،** عضو هیات علمی دانشکده ریاضی، دانشگاه علم و صنعت ایران، maleknejad@iust.ac.ir
**محسن شاهرضایی،** مجتمع دانشگاهی علوم و مهندسی دانشگاه امام حسین(ع)- گروه ریاضی و آمار
**مهناز فلاح علی آبادی،** دانشکده ریاضی، دانشگاه علم و صنعت ایران،

دار بتوانند مقدار $k$ را بدست آورند اما هیچ گروهی از ($t$-۱) سهام دار نتوانند این کار را انجام دهند. $K$ را یکی از سهام داران مخصوص که واسطه (*dealer*) نامیده می شود انتخاب می‌کند. این سهام دار مخصوص را به $D$ نشان می دهیم و فرض می‌شود که $D \notin P$.

وقتی $D$ می‌خواهد کلید $k$ را بین سهام داران در $P$ تقسیم کند، به هر سهام دار مقداری از اطلاعات جزئی را که "سهم" نامیده می‌شود تخصیص می‌دهد. سهم ها باید به طور مخفی توزیع شوند که هیچ سهام‌داری از سهم دیگران اطلاع نداشته باشد. بعداً یک زیر مجموعه از سهام داران مانند $Q(Q \subseteq P)$ سهم هایشان را روی هم خواهند گذاشت تا کلید $K$ را بیابند. اگر $|Q| \geq t$ آنگاه آن‌ها باید قادر به محاسبه $k$ باشند ولی اگر $|Q| < t$ آن‌ها باید قادر به محاسبه $k$ نباشند.

نمادیهایی که در این مقاله مورد استفاده واقع می‌شوند عبارتند از :

مجموعه $P$، $w$ سهامدار $P = \{P_i : ۱ \leq i \leq w\}$

مجموعه $K$، مجموعه تمام کلیدهای ممکن

مجموعه $S$، مجموعه تمام سهم‌های ممکن

اکنون فرض می‌کنیم $k = z_p$ که $P$ یک عدد اول است و $P \geq w+1$ و $S = Z_p$، آنگاه کلید یک عنصر از $Z_p$ خواهد بود اکنون $D$ طبق الگوریتم زیر به توزیع سهم‌ها می‌پردازد:

۱) $D$، $W$ عنصر غیر صفر مجزا از $z_p$ را انتخاب می کند، آنها را با $x_i (۱ \leq i \leq w)$ نمایش می‌دهیم. برای $۱ \leq i \leq w$، $D$ هر مقدار $x_i$ را به یک $p_i$ می دهد ($x_i$ ها را همه می توانند بدانند)

۲) $D$ برای تقسیم کلید $k$ ($k \in z_p$) به صورت تصادفی $t$-۱ عنصر $a_۱, ..., a_{t-۱}$ را از $z_p$ به طور مخفیانه انتخاب می کند.

۳) $D$ مقدار $y_i = p(x_i), (۱ \leq i \leq w)$ را محاسبه می کند که:

$$P(x) = K + \sum_{j=۱}^{t-۱} a_i x_j \pmod p$$

۴) برای $D, ۱ \leq I \leq w$ سهم $y_i$ را به $P_i$ می‌دهد.

بنابراین مشاهده می شود که در این طرح، واسطه ($D$) یک چند جمله ای مانند $P(x)$ را که حداکثر از درجه $t$-۱ است به صورت تصادفی می سازد که در آن جمله ثابت همان کلید است و به هر سهام‌دار $P_i$ یک زوج $(x_i, y_i)$ از این چند جمله ای تعلق می گیرد.

اکنون می خواهیم بدانیم چگونه یک زیر مجموعه $Q$ از $t$ سهام دار می‌توانند کلید $k$ را بیابید. فرض کنید سهام داران: $P_{i_۱}, ...., P_{i_t}$ بخواهند کلید $k$ را پیدا کنند آنها می دانند که $y_{ij} = p(x_{ij})$ , $(۱ \leq J \leq t)$ که $P(x)$ یک چند جمله ای در $z_p[x]$ است. (این چند جمله ای مخفی است و فقط $D$ آن را می داند) چون $P(x)$ حداکثر از درجه $t$-۱ است پس $P(x)$ را می توان به صورت زیر نوشت :

$$P(x) = a_۰ + a_۱ x + a_۲ x^۲ + ... + a_{t-۱} x^{t-۱} \qquad (۱\text{-}۱)$$

که $a_۰$ تا $a_{t-۱}$ مجهولند و $a_۰ = k$. برای محاسبه $P(x)$ روشهای مختلفی وجود دارد، مثلاً می توان از روش حل دستگاه معادلات خطی استفاده کرد اما چون روش‌های مستقیم حل دستگاه معادلات خطی تعداد عملیات نسبتاً زیادی (از مرتبه $n^۳$) لازم دارند، می‌توان برای محاسبه ضرایب چند جمله‌ای $P(x)$ از برخی روش‌های درونیابی مثل درونیابی لاگرانژ استفاده کرد [۱و۲].

اما در [۶] نشان داده شده است که استفاده از روش درونیابی تفاضلهای منقسم از نظر تعداد عملیات مقرون به صرفه است. در این روش با مفروض بودن زوجهای $(x_{ik}, P(x_{ik}) = y_{ik})$ که $(۱ \leq k \leq t)$ و تعریف زیر:

$$P[x_{i_t}, x_{i_{t-۱}}, ..., x_{i_۱}] = \frac{P[x_{i_t}, ..., x_{i_۲}] - P[x_{i_{t-۱}}, ..., x_{i_۱}]}{x_{i_t - x_{i_۱}}} \qquad (۲\text{-}۱)$$

که تفاضل منقسم مرتبه $t$ام است [۵] چند جمله ای تفاضلی تقسیمی زیر ساخته می‌شود:

$$P_n(x) = y_{i_۱} + (x - x_{i_۱}) P[x_{i_۲}, x_{i_۱}] + ... + (x - x_{i_۱})(x - x_{i_۲})..(x - x_{i_{t-۱}}) P[x_{i_t}, x_{i_{t-۱}}, ..., x_{i_۱}] \qquad (۳\text{-}۱)$$

اکنون، اگر در ۱-۳، $x = ۰$ قرار داده شود کلید $k$ محاسبه می گردد.

## ۳. معرفی توابع *PCBF* و ماتریسهای عملیاتی آنها

مجموعه $\{\theta_i\} \in L^۲$ که $\{\theta_i\}$ را متعامدی که نامیم اگر

$$< \theta_i(t), \theta_j(t) > = \begin{cases} ۰ & i \neq j \\ ۱ & i = j \end{cases}$$

اگر $\theta_i$ سیستم متعامد یکه از توابع پایه باشد، آنگاه هر $f(t) \in L^۲$ را می‌توانیم به صورت $f(t) = \sum_{i=۱}^{\infty} f_i \theta_i$ نمایش دهیم که $f_i = < f, \theta_i >$.

فرض کنیم $t_z$ بازه واحد $[۰,۱)$ باشد و $\theta_i$ها را توابعی قطعه ای ثابت در هر زیر بازه $\left[\frac{i-۱}{m}, \frac{i}{m}\right)$ که $i = ۱,۲,..., m$ انتخاب کنیم، این مجموعه را *PCBF* گوییم.

تبصره- اگر مساله در بازه $z \in [a,b)$ مطالعه شود، می توانیم همیشه آن را به مساله ای معادل در بازه $t \in [۰,T)$ تبدیل کنیم :

$$t = \frac{z-a}{b-a} \tau$$

در ادامه این قسمت قوانین عملگری روی *PCBF* را شرح می دهیم، جزئیات را می توان در [۳و۴] دید.

**۳-۱. تابع ثابت :** برای یک تابع حقیقی ثابت $f(t)=k$ ، سری $PCBF$ به صورت زیر است:

$$k \approx k\sum_{i=1}^{m}\theta_i(t)$$

به فرم برداری:

$$k = k(kk...k)\theta(t)$$

**۳-۲. جمع (تفریق):**

اگر $c(t)=f(t)\pm g(t)$ آنگاه

$$c = f \pm g$$

که

$$c=[c_1,c_2,...,c_m]^T$$
$$c_i =< c(t),\theta_i(t) >$$
$$f=[f_1,f_2,...,f_m]$$
$$g=[g_1,g_2,...,g_m]$$

**۳-۳. ضرب (تقسیم):**

اگر $c(t)=f(t)g(t)$ آنگاه

$$c = f \otimes g$$

و اگر برای $g(t)\neq 0 > t\in t_z$ :

$$c(t)=f(t)/g(t)$$
$$c = f \div g$$

**۳-۴. ضرب تابع در اسکالر:** اگر یک تابع در یک اسکالر حقیقی ضرب شده داریم:

$$kf(t)\approx\sum_{i=1}^{m}(kf_i)\theta_i(t)=k\sum_{i=1}^{m}f_i\theta_i(t)$$

به فرم برداری:

$$kf(t)=kF^T\theta(t)$$

**۳-۵. انتگرال گیری نسبت به $t$ :** انتگرال روبرو را در نظر بگیرید:

$$\int_0^t f(\lambda)d\lambda \quad t\in t_z$$

اگر $f(t)=F^T\theta(t)$ داریم :

$$\int_0^t F^T\theta(\lambda)d\lambda$$

حال ما از هر کدام از اعضای بردار ستونی $\theta(t)$ انتگرال می‌گیریم و نتیجه را در سری $\{\theta_i(t)\}$ دوباره بسط می دهیم حال داریم:

$$\int_0^t F^T\theta(\lambda)d\lambda = F^TE\theta(t)$$

که $E$ یک ماتریس ثابت معکوس پذیر است و به ماتریس عملیاتی معروف است.

## ۴. طرح آستانه شمیر با استفاده از توابع *PCBF*

واسطه با استفاده از چند جمله‌ای ۱-۱، ها را تعیین کرده و در برداری مانند $A$ ذخیره می‌کند. سپس بردار $A$ را از سمت راست در ماتریس عملیاتی یکی از توابع متعامد $PCBF$ به طور تصادفی ضرب می‌کند تا بردار $B$ بدست آید. سپس بردار $B$ را به بردار $E$ تبدیل می‌کند که مولفه‌های آن به پیمانه $p$ نمایش داده شده‌اند. در این نحوه نمایش قسمت صحیح عددی که به صورت اعشاری است، خارج قسمت و قسمت اعشاری باقیمانده تقسیم عدد اولیه بر $p$ می باشد. در ضمن برای اعداد منفی حاصل نماد $x^-$ را به کار می بریم. مولفه های بردار اخیر به صورت $y_{ij}$ در اختیار سهام داران قرار داده می‌شود. واسطه ماتریس به کار رفته را در اختیار یکی از سهام داران که آن را سهام دار ویژه می نامیم قرار می دهد. این سهام ار ویژه می تواند فردی باشد که از نظر مقام کاری به دیگران رجحان دارد.

در قسمت بعد در قالب چند مثال نشان می‌دهیم که سهام داران چگونه می توانند با استفاده از سهم های خود، کلید رمز را بیابند.

## ۵. مثال‌ها

در مثال‌های زیر از ماتریس عملیاتی تابع بلاک-پالس [۳و۴] استفاده شده است. این ماتریس به صورت زیر تعریف می‌شود:

$$E_B=\frac{1}{m}\left[\frac{I_2}{2}+\sum_{i=1}^{m-1}\Delta^i\right]=\frac{1}{2m}(I+\Delta)(I-\Delta)^{-1}$$

که در آن:

$$\Delta_{m\times m}=\begin{bmatrix}0 & & I_{(m-1)(m-1)}\\ 0 & & 0\end{bmatrix}$$

و:

$$\Delta^i=0 \qquad (i\geq m)$$

مثال ۱- فرض کنید $p=11$ ، $t=3$ ، $w=5$ و $x_i=i \;\; (1\leq i\leq 5)$. همچنین فرض کنید $Q=\{P_1,P_2,P_5\}$ سهم هایشان را روی هم گذاشته باشند که به ترتیب عبارتند از : ۱/۱،۲/۲⁻،۳/۹ پس داریم:

$$y_{i_1}=1/1 \qquad y_{i_2}=2/2^- \qquad y_{i_3}=3/9$$

برای یافتن کلید $k$ ، ابتدا بردار سهام را به سیستم ده دهی اعداد تبدیل می کنیم، یعنی برای بردار $E=[1/1,2/2^-,3/9]^T$ داریم:

$$B=[12,-24,42]^T$$

اینک از ماتریس عملیاتی بلاک- پالس با ابعاد $3\times 3$ استفاده می کنیم تا سهام واقعی به دست آیند.

$$\frac{1}{3}\begin{bmatrix} \frac{1}{2} & 1 & 1 \\ 0 & \frac{1}{2} & 1 \\ 0 & 0 & \frac{1}{2} \end{bmatrix}\begin{bmatrix} 12 \\ -24 \\ 42 \end{bmatrix}=\begin{bmatrix} 8 \\ 10 \\ 7 \end{bmatrix}$$

بنابراین داریم:

$$y_{i_1}^{*}=8 \qquad y_{i_2}^{*}=10 \qquad y_{i_3}^{*}=7$$

اکنون از رابطه۱-۲ و $x_{i_1}=1$ ، $x_{i_2}=3$ ، $x_{i_3}=5$ داریم:

$$p[x_{i_2},x_{i_1}]=1 \ , \ p[x_{i_3},x_{i_2}]=4 \ , p[x_{i_3},x_{i_2},x_{i_1}]=9$$

و از رابطه۱-۳ خواهیم داشت:

$$p_n(x)=8+(1)(x-x_{i_1})+9(x-x_{i_1})(x-x_{i_2})$$

که با قرار دادن $x=0$ داریم:

$$K=8-1+9(-1)(-3)=1 \pmod{11}$$

مثال۲- فرض کنید

$p=11, t=5, w=8$ , $x_i=i^2 \ (1\le i\le 10)$ . همچنین فرض کنید $Q=\{P_1,P_2,P_3,P_4,P_5,P_6,P_7,P_8,P_9,P_{10}\}$ با قرار دادن سهم هایشان روی هم بخواهند کلید مجهول $k$ را بیابند. اگر داشته باشیم

$$x_1=1 , \quad x_2=4 , \quad x_4=16$$
$$x_6=13 \quad x_7=3 , \quad x_8=18$$
$$x_9=12 \quad x_{10}=8 , \quad y_{i_1}=27/3$$
$$y_{i_2}=28/12 \quad y_{i_3}=18/18 \quad y_{i_4}=6/22$$
$$y_{i_5}=7/15 \quad y_{i_6}=19/11 \quad y_{i_7}=22/6$$
$$y_{i_8}=13/21$$

برای یافتن کلید $k$، ابتدا بردار سهام را به سیستم ده دهی اعداد تبدیل می کنیم، خواهیم داشت:

$$B=[624,-656,432,-160,-176,448,-512,320]^T$$

اینک از ماتریس عملیاتی بلاک –پالس با ابعاد $8\times 8$ استفاده می‌کنیم تا سهام واقعی به دست آید:

$$\frac{1}{8}\begin{bmatrix} \frac{1}{2} & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \frac{1}{2} & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & \frac{1}{2} & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & \frac{1}{2} & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & \frac{1}{2} & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \end{bmatrix}\begin{bmatrix} 624 \\ -656 \\ 432 \\ -160 \\ -176 \\ 448 \\ -512 \\ 320 \end{bmatrix}=\begin{bmatrix} 31 \\ 3 \\ 17 \\ 0 \\ 21 \\ 4 \\ 8 \\ 20 \end{bmatrix}$$

پس $A=[1,3,17,0,21,4,8,20]^T$ و یا

$$y_{i_1}^{*}=1, \quad y_{i_2}^{*}=3, \quad y_{i_3}^{*}=17, \quad y_{i_4}^{*}=0$$
$$y_{i_5}^{*}=21, \quad y_{i_6}^{*}=4, \quad y_{i_7}^{*}=8, \quad y_{i_8}^{*}=20$$

اکنون از روابط ۱-۲ و ۱-۳ با قرار دادن $x=0$ کلید مجهول $k$ معین می شود و خواهیم داشت :

$$k=16$$

## ۶. نتیجه گیری

با توجه به آن که، به دلیل تنوع $PCBF$ها، واسطه در به کار بردن ماتریس عملیاتی انتخابهای زیادی خواهد داشت، پس به این طریق امنیت سیستم رمزنگاری نسبت به طرح اولیه شمیر، افزایش می یابد. همچنین در لحظه واگذاری سهام به سهام داران، واسطه می تواند به جای در اختیار قرار دادن تمام ماتریس عملیاتی به سهام دار ویژه، تنها یک ستون ماتریس را به وی بدهد (چون از قابلیت های ماتریس عملیاتی $PCBF$ ها است که تمام ماتریس از روی یک ستون آن قابل نوشتن است.) بنابراین در تبادل اطلاعات صرفه جویی نیز خواهیم داشت.

## مراجع


[1] Shamir, A., How to share a secret, comm. Of the ACM 22 1979, 612-613.

[2] CRYPTOGRAPHY Theory and Practice, Douglas R. Stinson, University of Nebraska, 1995, Lincoln.

[3] Ganti, Trasada Rao, Piecewise constant orthogonal functions and their application to system and control, 1983, Stringer-Verlag.

[4] Razzaghi, M., Nazarzadeh, J., Walsh functions, Wiley encyclopedia of electrical and electronics in engineering, 23, 1990, 429-440.

[5] Numerical Analylis, Burden, R.L., Faires, T.D., Reynolds, A.C., Prindle, weber and Schmidt, 1978, Boston, Masschvsetts.

[۶]مالک نژاد، خسرو.، شاهرضایی، محسن.، فلاح، مهناز.، استفاده از روشهای درونیابی برای رمزگشایی در طرح آستانه شمیر (*shamir*)، سی و سومین کنفرانس ریاضی ایران، دانشگاه فردوسی مشهد، تابستان ۱۳۸۱.