

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 می‌شود. برای محاسبه ضرایب این چند جمله ای که منجر به یافتن کلید می‌شود روشهای گوناگونی وجود دارد. [۲ و ۱]. جایگزینی روش ورونیایی تفاضلهای منقسم به جای درونیایی لاگرانژ و رجحان این روش به لحاظ تعداد عملیات در مرجع [۶] نشان داده شده است. در این مقاله ضمن استفاده از روش درونیایی تفاضلهای منقسم، مقادیر توزیع شده توسط واسطه به عنوان یک بردار در نظر گرفته شده و با استفاده از ماتریس عملیاتی توابع پایه ای متعامد قطعه ای ثابت [۳ و ۴] بردار جدیدی تولید می‌شود و در اختیار سهامداران قرار می‌گیرد. واسطه می‌تواند 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، درونیایی، 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 می‌توان 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 عملیاتی متناظر، طرز استفاده از آنها در توزیع سهام تشریح خواهد شد.

۲. طرح آستانه شمیر

فرض کنید t و w اعداد صحیح مثبت باشند و $t \leq w$ ، 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،

که a تا a_{t-1} مجهولند و $a_t = k$. 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^3) لازم دارند، می توان برای محاسبه ضرایب چند جمله ای $P(x)$ از برخی روشهای درونیایی مثل درونیایی لاگرانژ استفاده کرد [۲ و ۱].

اما در [۶] نشان داده شده است که استفاده از روش درونیایی 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 $(1 \leq k \leq t)$ و تعریف زیر:

$$P[x_{i_1}, x_{i_{t-1}}, \dots, x_{i_1}] = \frac{P[x_{i_1}, \dots, x_{i_t}] - P[x_{i_{t-1}}, \dots, x_{i_1}]}{x_{i_t} - x_{i_1}} \quad (2-1)$$

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

$$P_n(x) = y_{i_1} + (x - x_{i_1})P[x_{i_2}, x_{i_1}] + \dots + (x - x_{i_1})(x - x_{i_2}) \dots (x - x_{i_{t-1}})P[x_{i_t}, x_{i_{t-1}}, \dots, x_{i_1}] \quad (3-1)$$

اکنون، اگر در $x = 0, 1, 2, \dots, t-1$ قرار داده شود کلید k محاسبه می گردد.

۳. معرفی توابع PCBF و ماتریسهای عملیاتی آنها

مجموعه $\{\theta_i\} \in L^2$ که $\{\theta_i\}$ را متعامدی که نامیم اگر

$$\langle \theta_i(t), \theta_j(t) \rangle = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$$

اگر θ_i سیستم متعامد یکه از توابع پایه باشد، آنگاه هر $f(t) \in L^2$ را می توانیم به صورت $f(t) = \sum_{i=1}^{\infty} f_i \theta_i$ نمایش

دهیم که $f_i = \langle f, \theta_i \rangle$.

فرض کنیم t_z بازه واحد $[0, 1]$ باشد و θ_i ها را توابعی قطعه ای ثابت در هر زیر بازه $\left[\frac{i-1}{m}, \frac{i}{m}\right]$ که $i = 1, 2, \dots, m$ انتخاب کنیم، این مجموعه را PCBF گوئیم.

تبصره- اگر مساله در بازه $z \in [a, b]$ مطالعه شود، می توانیم همیشه آن را به مساله ای معادل در بازه $t \in [0, T]$ 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 [۳ و ۴] دید.

دار بتوانند مقدار k را بدست آورند اما هیچ گروهی از $(t-1)$ سهام دار نتوانند این کار را انجام دهند. K را یکی از سهام داران مخصوص که واسطه (dealer) نامیده می شود انتخاب می کند. این سهام دار مخصوص را به D نشان می دهیم و فرض می شود که $D \notin P$.

وقتی D می خواهد کلید k را بین سهام داران در P تقسیم کند، به هر سهام دار مقداری از اطلاعات جزئی را که "سهام" نامیده می شود تخصیص می دهد. سهام ها باید به طور مخفی توزیع شوند که هیچ سهام داری از سهام دیگران اطلاع نداشته باشد. بعداً یک زیر مجموعه از سهام داران مانند $Q \subseteq P$ سهام هایشان را روی هم خواهند گذاشت تا کلید K را بیابند. اگر $|Q| \geq t$ آنگاه آن ها باید قادر به محاسبه k باشند ولی اگر $|Q| < t$ آن ها باید قادر به محاسبه k نباشند. نمادهایی که در این مقاله مورد استفاده واقع می شوند عبارتند از:

مجموعه P سهامدار $w = \{P_i : 1 \leq i \leq w\}$ مجموعه K مجموعه تمام کلیدهای ممکن

مجموعه S مجموعه تمام سهام های ممکن

اکنون فرض می کنیم $k = z_p$ 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 سهام ها می پردازد:

۱) D, W عنصر غیر صفر مجزا از Z_p را انتخاب می کند، آنها را با x_i ($1 \leq i \leq w$) نمایش می دهیم. برای $1 \leq i \leq w$ 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 $t-1$ عنصر a_1, \dots, a_{t-1} را از Z_p به طور مخفیانه انتخاب می کند.

۳) D مقدار $D = p(x_i)$ را محاسبه می کند که:

$$P(x) = K + \sum_{j=1}^{t-1} a_j x_j \pmod{p}$$

۴) برای $1 \leq I \leq w$ سهم y_i را به P_i می دهد.

بنابراین مشاهده می شود که در این طرح، واسطه (D) یک چند جمله ای مانند $P(x)$ را که حداکثر از درجه $t-1$ است به صورت تصادفی می سازد که در آن جمله ثابت همان کلید است و به هر سهام دار 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 می توانند کلید k را بیابند. فرض کنید سهام داران: P_{i_1}, \dots, P_{i_t} بخواهند کلید k را پیدا کنند آنها می دانند که $y_{i_j} = p(x_{i_j})$ که $(1 \leq j \leq t)$ 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 $t-1$ است پس $P(x)$ را می توان به صورت زیر نوشت:

$$P(x) = a + a_1 x + a_2 x^2 + \dots + a_{t-1} x^{t-1} \quad (1-1)$$

پس $A = [1, 3, 17, 0, 21, 4, 8, 20]^T$ و یا

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

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

بنابراین داریم:

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

اکنون از رابطه ۱-۲ و ۱-۳ ، $x_{i_1} = 1$ ، $x_{i_2} = 3$ ، $x_{i_3} = 5$ داریم:

$$p[x_{i_1}, x_{i_2}] = 1, \quad p[x_{i_2}, x_{i_3}] = 4, \quad p[x_{i_3}, x_{i_4}] = 9$$

و از رابطه ۱-۳ خواهیم داشت:

$$p_n(x) = 8 + (1)(x - x_{i_1}) + 9(x - x_{i_2})(x - x_{i_3})$$

که با قرار دادن $x = 0$ داریم:

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

مثال ۲- فرض کنید

$(1 \leq i \leq 10) x_i = i^t, w = 8, t = 5, p = 11$. 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

$$\begin{matrix} x_1 = 1 & x_2 = 4 & x_4 = 16 \\ x_6 = 13 & x_7 = 3 & x_8 = 18 \\ x_9 = 12 & x_{10} = 8 & y_{i_1} = 27/3 \\ y_{i_2} = 2812 & y_{i_3} = 1818 & y_{i_4} = 6/22 \\ y_{i_5} = 7/15 & y_{i_6} = 1911 & y_{i_7} = 226 \\ y_{i_8} = 1321 \end{matrix}$$

برای یافتن کلید k ، ابتدا بردار سهم 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 8×8 استفاده می کنیم تا سهم واقعی به دست آید:

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

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 سهم 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، شاهرزایی، محسن، فلاح، مهناز، استفاده از روشهای درونبایی برای رمزگشایی در طرح آستانه شمیر (*shamir*)، سی و سومین کنفرانس ریاضی ایران، دانشگاه فردوسی مشهد، تابستان ۱۳۸۱.