کاربرد چندجمله‌ای دو متغیره‌ی متقارن در شناسایی تقلب

دکتر عباس چراغی چالشتری[1]، فاطمه حسامی[2]، مژگان نخعی

دانشگاه خوانسار، گروه ریاضی، خوانسار، ایران

چکیده

در طرح تسهیم راز (k,n) هر k تا کاربر یا بیشتر می‌توانند راز را بازسازی کنند اما کاربران با تعداد کمتراز k تا نمی‌توانند هیچ‌گونه اطلاعاتی در مورد راز به‌دست آورند. در هنگام بازسازی راز برخی از کاربران سهام جعلی را برای فریب دادن دیگر کاربران ارسال می‌کنند، به این کاربران متقلبین می‌گویند به همین دلیل روش‌های شناسایی تقلب بسیار مورد توجه قرار گرفته است. لیو و همکارانش درسال 2018 برای رفع مشکل تقلب با استفاده از چند جمله‌ای دو متغیره الگوریتمی ارائه دادند. این الگوریتم، وجود تقلب در مرحله بازسازی را توسط m کاربری که در بازسازی راز شرکت دارند مشخص می‌کند. در این مقاله به بررسی الگوریتمی می‌پردازیم که در آن شناسایی تقلب بر اساس خاصیت متقارن بودن چند جمله‌ای دو متغیره و همچنین خطی بودن چندجمله‌ای درون‌یابی‌شده، پایه‌ریزی شده‌است. در نهایت یک $(7,9)$-طرح تسهیم راز با قابلیت شناسایی تقلب ارائه می‌دهیم به‌طوری‌که از بین 7 کاربر شرکت کننده در بازسازی راز، 2 کاربر به عنوان متقلب شناخته می‌شوند.

کلمات کلیدی: شناسایی تقلب، چندجمله‌ای دومتغیره، طرح تسهیم راز، تقارن

۱. مقدمه

شامیر[3] [1] و بلاکلی[4] [2] تسهیم راز را در سال 1979 با هدف ایمن نگه داشتن اطلاعات راز در بین کاربران معرفی کردند. تامپا و وول[5] [3] مشکل تقلب را در طرح تسهیم راز پیشنهاد دادند، به‌طوری‌که متقلبین سهام جعلی خود را در طول بازسازی راز ارائه می‌دهند. این باعث می‌شود کاربران صادق، یک راز جعلی را بازسازی کنند در صورتی‌که متقلبین به صورت منحصر به‌فرد راز را به دست می‌آورند.

در[۴] طرحی برای تشخیص تقلب ارائه‌شده، که کاربران صادق می‌توانند رفتار تقلب را تشخیص دهند اما نمی‌توانند متقلبین را شناسایی کنند. اکثر طرح‌های تسهیم راز قابل تشخیص تقلب، مبتنی بر کار شامیر [1] بوده است که تمام سهم‌ها از چندجمله‌ای تک متغیره درجه‌ی $k-1$ محاسبه می‌شود، علاوه بر این، چندجمله‌ای دو متغییره

[1] a.cheraghi@khn.ui.ac.ir
[2] corresponding author
[3] Shamir
[4] Blakly
[5] Tompa and Woll

$F(x,y)$ نیز یک ابزار اساسی برای برخی از توابع طرح‌های تسهیم راز بوده است که در آن تمامی کاربران صحت سهام خود را قبل از بازسازی بررسی می‌کنند.

در این مقاله الگوریتمی برای شناسایی تقلب، در طرح‌های تسهیم راز، با استفاده از چندجمله‌ای دو متغیره متقارن بررسی می‌شود به‌طوری‌که سهم تمام کاربران با استفاده از یک چندجمله‌ای دو متغیره متقارن محاسبه می‌شود.

از مزایای این الگوریتم می‌توان به دو مورد زیر اشاره کرد:

۱- شناسایی متقلب توسط m تا کاربری که در بازسازی راز شرکت می‌کنند صورت می‌گیرد.

۲- در هنگام استفاده از این الگوریتم به هیچ‌گونه اطلاعات اضافی احتیاج نیست.

۲. معرفی الگوریتم

برای ارائه یک طرح تسهیم راز با قابلیت شناسایی متقلب دو مرحله زیر را در نظر می‌گیریم[3]. مرحله اول *اشتراک‌گذاری راز* است، در واقع در فاز اول الگوریتم نحوه‌ی توزیع سهم‌ها در بین تمامی سهام‌داران شرح داده خواهد شد. در مرحله دوم علاوه بر بازسازی راز *صحت سهم سهام‌داران* نیز تعیین می‌شود به عبارت دیگر در صورت وجود تقلب، متقلب نیز شناسایی می‌شود.

فاز رمزگذاری:

گام اول: واسطه یک چندجمله‌ای دو متغیره متقارن همانند $F(x,y)$ را از درجه‌ی $k-1$ انتخاب می‌کند، که راز همان $S=F(0,0)$ است.

گام دوم: واسطه سهم هر کاربر P_i را با استفاده از چندجمله‌ای همانند $f_i(j)=F(i,j)$ محاسبه می‌کند و آن را از طریق کانال امن برای P_i ارسال می‌کند.

فاز بازسازی و تشخیص تقلب:

فرض کنید در این مرحله $m \geq k$ و سهام‌داران شرکت کننده در طرح، که آن‌ها را با نماد $P_1,\dots,P_m$ نشان می‌دهیم شرکت می‌کنند. در ادامه الگوریتمی که فاز بازسازی و تشخیص تقلب در آن صورت می‌گیرد را شرح می‌دهیم.

گام اول: هر کدام از m سهامدار دو عدد تصادفی $d_1, d_2 > n$ را انتخاب می‌کنند. به ازای هر $1 \leq i \leq m$ سهامدار P_i سهمِ راز $v_i = f_i(0)$ و دو سهم تشخیص $e_{i,2} = f_i(d_2)$ و $e_{i,2} = f_i(d_1)$ خود را به صورت عمومی اعلام می‌کند.

گام دوم: m سهام‌دار سهم راز و دو سهم تشخیص خود را در اختیار یکدیگر قرار می‌دهند، چند جمله‌ای‌های متقارن $g_0(x)$ و $g_{d1}(x)$ و $g_{d2}(x)$ را روی مجموعه مقادیر

$$\{v_1,\dots,v_m\} \text{ و } \{e_{1,1},\dots,e_{m,1}\} \text{ و } \{e_{1,2},\dots,e_{m,2}\}$$

محاسبه می‌کنند که از درجه $k-1$ می‌باشند. اگر شرایط زیر برقرار باشد

$$g_{d1}(d_2) = g_{d2}(d_1) \qquad g_{d1}(0) = g_0(d_1) \qquad g_{d2}(0) = g_0(d_1)$$

آنگاه $S = g_0(0)$ است در غیراینصورت برای تشخیص تقلب باید به گام سوم برویم.

گام سوم: همه‌ی m سهام‌دار $i = 1,\dots,m$ مقدار $f_i(j)$ را که چندجمله‌ای سهام است محاسبه و منتشر می‌کنند اگر سهام‌داری در هنگام انتشار سهام چندجمله‌ای، سهم راز و همچنین سهم تشخیص بخشی از این سهام‌ها را ارائه ندهد مشخص است که سهام‌دار صادقی محسوب نشده و می‌توان آن را به‌عنوان شخص متقلب در نظر گرفت.

حال **تمام** کاربران دو به دو به صورت زیر به یکدیگر رای می‌دهند:

اگر $f_i(j) = f_j(i)$ در نتیجه p_j و p_j به یکدیگر رای می‌دهند.

اگر $f_i(j) \neq f_j(i)$ در نتیجه p_i و p_j به یکدیگر رای نمی‌دهند.

گام چهارم: در این مرحله فرض کنید p_i ها به تعداد v_i رای دریافت می‌کنند، هر کاربر p_i که کمتر از $T = \frac{m+k-5}{2}$ رای بگیرند متقلب شناخته می‌شوند

همچنین فرض کنید L مجموعه‌ای از متقلبین است اگر $m - |L| \geq k$ آنگاه راز را توسط کاربران صادق بازسازی می‌شود و خروجی برابر است با (S, L) در غیر اینصورت راز جعلی بازسازی می‌شود.

در [3] یک کران بالا برای تعداد متقلبین ارائه شده است.

قضیه: [5] اگر $t < \frac{m-k+3}{2}$ آنگاه متقلبین توسط الگوریتم ارائه شده شناسایی می‌شوند.

قضیه فوق نشان می‌دهد، حداکثر تعداد متقلبین کمتر از $\frac{m-k+3}{2}$ است. الگوریتم معرفی شده تقلب را توسط کاربرانی که در بازسازی راز شرکت می‌کنند تشخیص می‌دهد، در بخش بعد یک طرح تسهیم راز (7,9) ارائه می‌دهیم که در آن با استفاده از آنچه در بخش 2 گفته شد تقلب را شناسایی می‌کنیم.

۳. طرح تسهیم راز(7,9) با قابلیت شناسایی تقلب و متقلب

در این بخش تمامی محاسبات به پیمانه 23 انجام می‌شود. ابتدا واسطه چندجمله‌ای دو متغیره و متقارن از درجه حداکثر $k-1$ زیر را به دلخواه و به‌طور تصادفی در نظر می‌گیرد و سهم هر کاربر را از طریق آن محاسبه و سپس از طریق کانال امن برای هر سهام‌دار ارسال می‌کند

$$f_x(y) = F(x,y) = x^4 + y^4 + 3x^2y^2 - 8$$

چندجمله‌ای‌های سهام $p_1, \ldots, p_7$ به صورت زیر نشان داده می‌شود:

$$\begin{aligned}
p_1 &: f_1(y) = y^4 + 3y^2 - 7 \\
p_2 &: f_2(y) = y^4 + 12y^2 + 8 \\
p_3 &: f_3(y) = y^4 + 4y^2 + 4 \\
p_4 &: f_4(y) = y^4 + 2y^2 + 18 \\
p_5 &: f_5(y) = y^4 + 6y^2 + 19 \\
p_6 &: f_6(y) = y^4 + 16y^2 + 8 \\
p_7 &: f_7(y) = y^4 + 11y^2 + 9
\end{aligned}$$

طرح ارائه شده دردو فاز زیر صدق می‌کند:

۱- *فاز رمزگذاری*: از آنجایی که با داشتن 7 *سهم* فوق 7 نقطه متمایز از چندجمله‌ای $F(x,y)$ را داریم، با توجه به خواص درونیابی لاگرانژ این چندجمله‌ای به صورت منحصر به‌فرد بازسازی می‌شود یعنی راز یکتا به‌دست می‌آید.

۲- *فاز بازسازی*: یک زیرمجموعه‌ی غیر مجاز کمتر از 7 نقطه از چندجمله‌ای $F(x,y)$ را دارد لذا با توجه به درون‌یابی لاگرانژ و طرح شامیر این طرح نیز همانند طرح شامیر امنیت دارد.

7 سهام‌دار $p_1, \ldots, p_7$ را در نظر بگیرید که در بازسازی راز شرکت می‌کنند. بدون کم شدن از کلیت مساله فرض کنید در بین این سهام‌داران دو سهام‌دار p_2 و p_4 تقلب کرده باشند در این صورت عدد تقلب $t=2$ است زیرا $t < \frac{7-5+3}{2} = \frac{5}{2}$ لذا حداکثر دو متقلب داریم.

تعداد کاربران صادق را با k نشان می‌دهیم و در این مثال چون فرض کردیم دو کاربر متقلب وجود دارد پس تعداد کاربران صادق برابر5 می‌باشد، لذا $k = 5$.

حال طبق الگوریتم گفته شده هر کدام از سهام‌داران باید دو عدد تصادفی d_1 و d_2 را به دلخواه انتخاب کنند به‌طوری‌که $d_1, d_2 > 9$

سهام‌دار p_2 دو عدد تصادفی $d_1 = 10$ و $d_2 = 12$ را انتخاب می‌کند وسهام‌دار p_4 نیز دو عدد تصادفی $d_1 = 11$ و $d_2 = 13$ را انتخاب می‌کند.

سهام‌دار p_2 سهم راز و دو سهم تشخیص خود را به‌صورت زیر محاسبه می‌کند:

سهم راز:

$$v_2 = f_2(0) = 8$$

دو سهم تشخیص:

$$e_{2,1} = f_2(d_1) = 7$$

$$e_{2,2} = f_2(d_2) = 1$$

همچنین سهام‌دار p_4 سهم راز و دو سهم تشخیص خود را به صورت زیر محاسبه می‌کند:

سهم راز:

$$v_4 = f_4(0) = 18$$

دو سهم تشخیص:

$$e_{4,1} = f_4(d_1) = 20$$

$$e_{4,2} = f_4(d_2) = 6$$

کاربر p_2 چندجمله‌ای جعلی $f_2^* = y^4 + 12y^2 + 10$ و دو سهم تشخیص $e_{2,1} = 7$ و $e_{2,2} = 1$ و همچنین کاربر p_4 چندجمله‌ای جعلی $f_4^* = y^4 + 2y^2 + 21$ و دو سهم تشخیص $e_{4,1} = 20$ و $e_{4,2} = 6$ را برای دیگر کاربران ارسال می‌کنند. در این صورت دو کاربر متقلب می‌توانند راز را به صورت منحصر بفرد با استفاده از چندجمله‌ای سهامِ کاربران صادق، بازسازی کنند.

پس از بررسی برابری چندجمله‌ای‌هایی مانند تساوی‌های زیر نتیجه می‌گیریم که هرکدام از کاربران متقلب یک رای دریافت می‌کنند:

$$f_4^*(4) = f_4(4) \quad و \quad f_2^*(7) = f_2(7)$$

همچنین نابرابری‌های زیر نشان می‌دهد که هیچ دو کاربر از کاربران p_2 و p_4 و p_6 هیچ رای از یکدیگر دریافت نمی‌کنند

$$f_2^*(4) \neq f_4(2) \quad و \quad f_2^*(6) \neq f_6(2) \quad و f_4^*(6) \neq f_6(4)$$

طبق گام چهارم الگوریتم چون $1 < \mathrm{T} = \frac{m-k+5}{2} = \frac{7}{2}$ در نتیجه اطمینان حاصل می‌شود که P_2 و P_4 متقلب هستند. لازم به ذکر است هرکدام ازکاربران صادق طبق رابطه‌ی زیر ۶ رای دریافت می‌کنند

$$n - t - 1 = 9 - 2 - 1 = 6$$

در این مقاله روشی برای شناسایی کاربرانی ارائه شده‌است که در حین بازسازی راز قصد فریب دادن دیگر کاربران را دارند ارایه شده‌است. ابتدا یک روش در قالب الگوریتم در بخش ۲ ارائه شده و در نهایت در بخش ۳ این الگوریتم را به صورت کاربردی اجرا کردیم.

4. کارهای آینده

با توجه به آنچه گفته شد استفاده از الگوریتم پیشنهادی در بازسازی راز، مشکل تقلب را برطرف می‌کند. شناسایی تقلب در طرح ارایه شده تنها براساس خاصیت چندجمله‌ای دومتغیره متقارن و خطی بودن چندجمله‌ای درون‌یابی شده است که فاقد اطلاعات اضافی در سهام می‌باشد. یکی از مشکلات طرح لیو و همکارانش حجم زیاد محاسبات است که باعث می‌شود زمان اجرای الگوریتم در لحظه، افزایش یابد این مشکل می‌تواند موضوع تحقیقات بعدی خوانندگان علاقه‌مند باشد.

5. مراجع

[1]. Shamir, A. (1979), "How to share a secret", Commun. ACM، **22** (11), pp. 612–613.
[2]. Blakley, GR. (1979), "Safeguarding cryptographic keys", in: Proceedings of the AFIPS pp. 313–317.

[3].Tompa, M. and Woll, H. (1989), "How to share a secret with cheaters", Journal of Cryptology, **1** (3), pp. 133–138 .

[4]. LIU,Y.X. (2016), "Linear secret sharing scheme with cheating detection", Secur. Commun. Netw. 9 (13) 2115–2121 .

[5]. Liu,Y. and Yung, Ch. and Wang, Y. and Zhu, L. and Ji, W. (2018), "Cheating identifiable secret sharing scheme using symmetric bivariate polynomial", Information Sciences, **453**, , pp. 21-29.