Scientific Journal of Electronic & Cyber Defense
Vol. 12, No. 2, Summer 2024, Serial No. 46
ISSN: 2322-4347 , E-ISSN: 2980-8979

Enhancing secret sharing security: A cheating detection approach based on inverse polynomial coefficients

A. Havasi [1] , M. Hadian Dehkordi [2*]
Professor, Iran University of Science and Technology, Tehran, Iran.
(Received: 2024/05/28, Revised: 2024/08/01, Accepted: 2024/08/13, Published: 2024/08/31)
DOR:

ABSTRACT

Secret sharing is the process of distributing a secret among n shareholders, in such a way that only a subset of them can recover the secret, while unauthorized subsets, referred to as dishonest shareholders, cannot access the secret. During the secret reconstruction phase, when shareholders present their shares, a dishonest shareholder or shareholders can always obtain the secret exclusively by presenting fake shares, thus leaving the honest shareholders with nothing but a fake secret. Detecting cheating is crucial for achieving a fair secret reconstruction. In this paper, it has been proposed a cheating-detecting secret sharing scheme that utilizes polynomial coefficients for cheat detection in secret reconstruction. It is leveraged the invertibility property of polynomial coefficients in the z_q field to detect cheat and employ relationships that follow a linear equation.

Keywords: Secret sharing, Cheating detection, Cryptography, Linear secret sharing.

*Corresponding Author Email: mhadian@iust.ac.ir

"پدافند الکترونیکی و سایبری"
سال دوازدهم، شماره ۲، تابستان ۱۴۰۳، ص ۱۱۴-۱۰۹

علمی – پژوهشی

افزایش امنیت تسهیم راز: یک رویکرد تشخیص تقلب مبتنی بر وارون ضرایب چندجمله‌ای

علی هواسی[۱]، مسعود هادیان دهکردی[۲*]

۱- دانشجوی دکتری ۲- استاد، دانشگاه علم و صنعت، تهران، ایران.

(دریافت: ۱۴۰۳/۰۳/۰۸، بازنگری: ۱۴۰۳/۰۵/۱۱، پذیرش: ۱۴۰۳/۰۵/۲۳، انتشار: ۱۴۰۳/۰۶/۱۰)

DOR:

ناشر: دانشگاه جامع امام حسین (ع) نویسندگان

چکیده

تسهیم راز، اشتراک‌گذاری یک راز بین n سهام‌دار است؛ به‌طوری‌که فقط زیرمجموعه‌ای از آنها قادرند راز را بازیابی کنند و زیرمجموعه‌هایی که غیرمجاز نامیده می‌شوند، نمی‌توانند به راز دسترسی داشته باشند. هنگامی که سهام‌داران، سهم‌های خود را در مرحله بازسازی راز ارائه می‌کنند، سهام‌دار یا سهام‌داران متقلب همیشه می‌توانند با ارائه سهم‌های جعلی، به طور انحصاری راز را به دست آورند، بنابراین سایر سهام‌داران صادق، چیزی جز یک راز جعلی به دست نمی‌آورند. تشخیص تقلب برای دستیابی به بازسازی عادلانه یک راز بسیار مهم است. در این مقاله، یک طرح تسهیم راز باقابلیت تشخیص تقلب ارائه می‌شود که در آن از دو چندجمله‌ای، برای تشخیص تقلب سهم در بازسازی راز استفاده می‌شود. در این طرح از خاصیت وارون‌پذیر بودن ضرایب چندجمله‌ای در میدان z_q برای تشخیص تقلب استفاده می‌شود و روابط مورد استفاده خطی خواهند بود.

کلیدواژه‌ها: تسهیم راز، تشخیص تقلب، رمزنگاری، تسهیم راز خطی

۱- مقدمه

در عصر ارتباطات و توزیع اطلاعات، پیشرفت سریع و همه‌جانبه ارتباطات ماهواره‌ای، گسترش شبکه‌های مخابراتی، استفاده روزافزون از کارت‌های هوشمند و... نیاز به حفاظت از اصل داده و محرمانه بودن اطلاعات در حال پردازش، یک ضرورت اساسی و چالش‌برانگیز است. طرح‌های تسهیم راز، در ارتباطات امن و علم رمزنگاری نقش حیاتی دارند. این طرح‌ها امکان تقسیم یک راز به چندین بخش و توزیع آن بین‌گروهی از شرکت‌کنندگان را فراهم می‌کنند؛ به‌طوری‌که فقط زمانی راز قابل‌بازسازی است که تعداد کافی از بخش‌ها ترکیب شوند.

در سال ۱۹۷۹، شامیر [۱] و بلکلی [۲] طرح‌های تسهیم راز را به طور مستقل به‌عنوان راه‌حلی برای حفاظت از کلیدهای رمزنگاری ارائه کردند و امروزه این طرح‌ها، جایگاه ویژه‌ای در علم رمزنگاری دارند. در این طرح‌ها، توزیع‌کننده، یک راز را به n سهم تقسیم می‌کند و بین n سهامدار به اشتراک می‌گذارد؛ به‌طوری‌که هر t یا بیش از t سهم، قادر به بازسازی راز باشند. بااین‌حال، سهم‌های کمتر از t قادر به بازسازی راز نیستند. این طرح‌ها به عنوان طرح‌های تسهیم راز آستانه‌ای (t, n) نیز شناخته می‌شوند.

در طرح شامیر فرض بر این است که توزیع‌کننده بدون اشتباه راز را بین سهام‌داران تقسیم می‌کند و کلیه سهام‌داران باید به اعتبار سهم دریافتی اطمینان کامل داشته باشند. سهام‌داران نیز هیچ اطلاعات غلطی را برای ترکیب‌کننده ارسال نمی‌کنند. بااین‌حال در مواقع عملی، حضور شرکت‌کنندگان نا صادق یک تهدید قابل‌توجه برای امنیت طرح‌های تسهیم راز به‌حساب می‌آید. این شرکت‌کنندگان، ممکن است در فاز بازسازی راز با ارسال سهم‌های جعلی تلاش کنند به بازسازی امن راز آسیب بزنند.

تومپا و وول [۳]، اولین افرادی بودند که ایده تقلب را ارائه کردند. آنها مسئله تقلب را در طرح تسهیم راز ارائه نمودند؛ به‌گونه‌ای که سهم‌های جعلی توسط متقلبان در جریان بازسازی راز ارائه می‌شود؛ بنابراین، درحالی‌که یک راز نادرست توسط سایر سهام‌داران صادق بازسازی می‌شود، متقلبان می‌توانند راز واقعی را به طور انحصاری بازیابی کنند. در یک بررسی [۴]، مدل تقلب جدیدی ارائه‌شده است که در آن $t-1$ شرکت‌کننده نا صادق می‌توانند شرکت‌کننده t اُم را فریب دهند. در مطالعه‌ای دیگر [۵]، یک طرح تسهیم راز خطی همراه با جلوگیری از تقلب ارائه شده است که سهم‌های شرکت‌کنندگان را به زیرسهم‌های مستقل تبدیل می‌کند تا از

* رایانامه نویسنده مسئول: mhadian@iust.ac.ir

تقلب جلوگیری شود. لیو و همکاران [۶]، یک طرح تشخیص تقلب ارائه کردند. آنها برای اینکه نشان دهند که اگر حداکثر $t-1$ شرکت‌کننده ناصادق، سهم‌های خود را برای فریب دادن نفر صادق t اُم تغییر دهند، این طرح بدون تقلب باقی می‌ماند، از دو چندجمله‌ای و دو تابع تشخیص تقلب استفاده می‌کنند.

در پژوهشی دیگر [۷]، طرح تسهیم راز باقابلیت شناسایی متقلب پیشنهاد می‌شود که تغییرات در راز توسط یک شرکت‌کننده نا صادق ایجاد می‌شود و سهام زیرمجموعه‌ای غیرمجاز از شرکت‌کنندگان را تغییر می‌دهد. این طرح حفاظت را در برابر یک فرد متقلب فراهم می‌کند که علاوه بر دسترسی به سهام یک مجموعه غیرمجاز، دسترسی به نشت اطلاعات از سهام سایر شرکت‌کنندگان را نیز دارد. در بررسی دیگر [۸]، یک طرح تسهیم چند راز قابل‌تأیید معرفی می‌شود که به تشخیص تقلب و شناسایی شرکت‌کنندگان نا صادق، می‌پردازد. این طرح از ℓ-جفت از کدهای دوری به‌عنوان ابزار اصلی استفاده می‌کند. در مقاله‌ای دیگر [۹]، یک طرح تشخیص تقلب با استفاده از یک تابع احراز هویت - ساخته‌شده با هوموروفیسم ضربی - ارائه‌شده است. کابلو و همکاران [۱۰]، یک طرح تسهیم راز خطی باقابلیت تشخیص تقلب برای یک ساختار دسترسی عمومی پیشنهاد کردند که می‌تواند بر روی طرح‌های تسهیم راز (t,n) اعمال شود. سیانچیلو و همکاران [۱۱]، طرح تشخیص تقلبی را ارائه نمودند که از کد تشخیص تغییر جبری برای تشخیص تقلب استفاده می‌کند؛ اما در این طرح قبل از بازسازی راز، شرکت‌کنندگان سهم‌های خود را برای شبکه‌های اعتبار سنجی ارسال می‌کنند. این شبکه‌ها بدون بازیابی راز، تقلب را ارزیابی می‌کنند تا در صورت وقوع تقلب، فرایند بازیابی راز را متوقف کنند و مطمئن شوند هیچ‌کس اطلاعات محرمانه‌ای دریافت نکرده است.

ساختار این مقاله به شرح زیر سازمان‌دهی شده است. در بخش ۲، مقدماتی ارائه می‌شود که شامل تعاریف تسهیم راز، تسهیم راز خطی و تسهیم راز باقابلیت تشخیص تقلب می‌شود. در بخش ۳، یک طرح پیشنهادی ارائه‌شده است که از خاصیت وارون‌پذیری ضرایب دو چندجمله‌ای برای تشخیص تقلب استفاده می‌کند. تحلیل امنیتی مرتبط با این طرح پیشنهادی در بخش ۴ بررسی می‌شود. در بخش ۵، یک مقایسه بین طرح پیشنهادی این مقاله و طرح‌های مشابه قبلی، صورت می‌گیرد. درنهایت، نتیجه‌گیری مطالعه در بخش ۶ ارائه‌شده است.

۲- پیش‌نیازها

۲-۱- تعاریف و مفاهیم اولیه

در این بخش، به طور مختصر به طرح اصلی تسهیم راز شامیر با پارامترهای (t,n) اشاره می‌شود. فرض کنید عدد اول q و راز S در مجموعه اعداد صحیح مقداردهی شده‌اند. مراحل تولید سهم و بازسازی راز در طرح شامیر، به‌صورت زیر تشریح می‌شوند.

مرحله تولید سهم: یک شرکت‌کننده خاص به‌عنوان توزیع‌کننده، یک راز $\boldsymbol{S}$ را از میدان $\boldsymbol{z_q}$ انتخاب می‌کند. سپس یک چندجمله‌ای از درجه‌ای $\boldsymbol{t-1}$ با ضرایب تصادفی $\boldsymbol{a_1, a_2, \dots, a_{t-1}}$ و جمله ثابت $\boldsymbol{a_0 = S}$ را به‌صورت رابطه (۱) تولید می‌کند.

$$\boldsymbol{f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}} \quad (1)$$

سپس سهم‌های $\boldsymbol{(i = 1, 2 \dots, n)\ \ d_i = f(i)}$ توسط توزیع‌کننده محاسبه می‌شود و هر سهم $\boldsymbol{d_i}$ را در یک کانال امن برای هر سهامدار ارسال می‌کند.

مرحله بازسازی راز: برای بازسازی راز، هر $\boldsymbol{t}$ سهام‌دار یا بیشتر، باید مقادیر سهم خود را افشا کنند. سپس با داشتن $\boldsymbol{t}$ زوج $\boldsymbol{(i, f(i))}$ و با استفاده از درونیابی‌لاگرانژ[1]، چندجمله‌ای $\boldsymbol{f(x)}$ به صورت زیر بازسازی می‌شود و راز به صورت $\boldsymbol{S = f(0)}$ بدست می‌آید.

$$f(x) = \sum_{i=1}^{t} f(i) \left(\prod_{j=1}^{t, j \neq i} \frac{x-j}{i-j} \right) \quad (2)$$

تسهیم راز باقابلیت تشخیص تقلب: در یک طرح تسهیم راز با $\boldsymbol{n}$ شرکت‌کننده، خروجی مرحله بازسازی راز که قابلیت تشخیص تقلب به‌اندازه $\boldsymbol{(t, n, \epsilon)}$ دارد، تسهیم راز باقابلیت تشخیص تقلب گفته می‌شود، که در آن $\boldsymbol{\epsilon}$ احتمال موفقیت در تقلب و $\boldsymbol{t}$ تعداد بیشینه افراد متقلبی است که در صورت حضور در طرح، امکان تشخیص آنها با حداقل احتمال $\boldsymbol{1-\epsilon}$ به ازای مقدار ناچیز $\boldsymbol{\epsilon > 0}$ وجود دارد.

۲-۲- طرح تسهیم راز خطی

باتوجه‌به تعریف ارائه شده توسط پیپرزیک و ژانگ [۵]، طرح تسهیم راز (t,n) یک طرح تسهیم راز خطی است، هرگاه n سهم $d_1, d_2, \dots, d_n$ در رابطه خطی زیر صدق کنند.

$$(d_1, d_2, \dots, d_n) = (r_1, r_2, \dots, r_t)M \quad (3)$$

در رابطه (۳)، Mیک ماتریس $t \times n$ است که درایه‌های آن از $GF(q)$ انتخاب می‌شود و هر زیر ماتریس $t \times t$ از آن غیرمنفرد است. مقادیر r_i توسط توزیع‌کننده به‌طور تصادفی انتخاب می‌شود. باتوجه‌به رابطه (۳)، می‌توان دید که طرح

[1] Lagrange interpolation

تسهیم راز شامیر، یک طرح تسهیم راز خطی است.

۳- طرح پیشنهادی

فرض کنید $GF(q)$ یک میدان متناهی با q عنصر باشد که در اینجا q توانی از یک عدد اول و بزرگ‌تر از n است $(q > n)$. هم‌چنین فرض می‌شود S، توسط یک شرکت‌کننده خاص به نام توزیع‌کننده، انتخاب‌شده است.

۳-۱- مرحله تسهیم راز

توزیع‌کننده، مشابه طرح شامیر، طرح آستانه‌ای (t, n) را برای راز $S \in GF(q)$ اجرا می‌کند. با انتخاب تعداد $t-1$ مقدار تصادفی $a_1, a_2, \dots, a_{t-1} \in z_q$ و جمله ثابت $a_0 = S$، یک چندجمله‌ای از درجه‌ای $t-1$ به‌صورت رابطه (۴) تولید می‌کند.

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \quad (۴)$$

ابتدا توزیع‌کننده، اندیس‌های $0 \le i, j \le t-i, j$ $(i \neq j\ 1)$, را انتخاب می‌کند و آنها را مخفی نگه می‌دارد. سپس با انتخاب مقدار تصادفی $m \in z_q$، یک چندجمله‌ای دیگر مانند $g(x)$ از درجه $t-1$ را به‌صورت رابطه (۵) تولید می‌کند که چندجمله‌ای پشتیبان نامیده می‌شود.

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{t-1} x^{t-1} \quad (۵)$$

در رابطه (۵)، توزیع‌کننده همه ضرایب $g(x)$ به‌جز b_i, b_j را به‌طور تصادفی انتخاب می‌کند. ضرایب b_i, b_j نیز، طوری انتخاب می‌شود که در رابطه (۶) صدق کنند:

$$\begin{cases} a_i \cdot b_i = m \\ a_j \cdot b_j = m \end{cases} \quad \begin{pmatrix} 0 < m < q \\ 0 \le i, j \le t-1 \end{pmatrix} \quad (۶)$$

چنین b_i, b_j هایی وجود دارند زیرا در $GF(q)$ همه اعضا وارون پذیر هستند. بنابراین طبق رابطه (۷) می‌توان نوشت:

$$\exists h\ s.t\ \ a_i \cdot h = 1 \Rightarrow a_i \underbrace{(m \cdot h)}_{b_i} = m \quad (۷)$$

به طور مشابه:

$$\exists h'\ \ s.t\ \ a_j \cdot h' = 1 \Rightarrow a_j \underbrace{(m \cdot h')}_{b_j} = m \quad (۸)$$

در واقع می‌توان گفت دو چندجمله‌ای $f(x)$ و $g(x)$ به هم مرتبط هستند؛ به عبارت دیگر تغییر در دو ضریب مورد نظر منجر به تغییر در چندجمله‌ای دیگر می‌شود.

توزیع‌کننده، n مقدار نا صفر و متمایز $x_1, x_2, \dots, x_n \in GF(q)$ را انتخاب کرده و آنها را منتشر می‌کند و با محاسبه سهم هر شرکت‌کننده به‌صورت $d_i = (f(x_i), g(x_i))$، مقدار d_i را برای شرکت‌کننده P_i در یک کانال امن ارسال می‌کند.

۳-۲- مرحله بازسازی راز

فرض کنید ترکیب‌کننده، t سهم $d_1, d_2, \dots, d_t$ را دریافت کند. او چندجمله‌ای $f(x)$ را با استفاده از سهم‌های $(x_1, f(x_1)), (x_2, f(x_2)), \dots, (x_t, f(x_t))$ و با استفاده از درونیابی‌لاگرانژ به‌صورت رابطه (۹) بازسازی می‌کند.

$$f(x) = \sum_{i=1}^{t} f(x_i) \left(\prod_{j=1, j \neq i}^{t} \frac{x - x_j}{x_i - x_j} \right) \quad (۹)$$

به همین ترتیب، او چندجمله‌ای $g(x)$ را نیز بازسازی می‌کند.

۳-۳- مرحله تشخیص تقلب

پس از بازسازی چندجمله‌ای‌های $f(x)$ و $g(x)$، اگر اعداد $0 < m < q$ و $0 \le i, j \le t-1$ وجود داشته باشند که در روابط $a_i \cdot b_i = m$ و $a_j \cdot b_j = m$ صدق کنند، آنگاه می‌توان گفت، تقلبی رخ نداده است و راز به‌صورت امن بازسازی می‌شود. در غیر این صورت، تقلب اتفاق افتاده و فرایند بازسازی راز متوقف می‌شود.

۴- تحلیل امنیتی طرح پیشنهادی

طرح تسهیم راز پیشنهادی شامل سه مرحله یعنی تولید سهم، بازسازی راز و تشخیص تقلب است. این بخش، یک تجزیه‌وتحلیل امنیتی دقیق، برای هر یک از آنها ارائه می‌کند. بااین‌حال، مرحله بازسازی راز که توسط یک شرکت‌کننده به نام ترکیب‌کننده اجرا می‌شود، با استفاده از سایر سهم‌ها و درون‌یابی لاگرانژ، ازنظر رمزنگاری امن است؛ زیرا سهم‌های شرکت‌کنندگان به‌صورت خصوصی مبادله می‌شوند. تجزیه‌وتحلیل‌های امنیتی برای مراحل باقی‌مانده، در ادامه ارائه‌شده است.

طرح تسهیم راز پیشنهادی این بررسی، برای تولید سهام شرکت‌کنندگان، از طرح شامیر پیروی می‌کند که در آن یک چندجمله‌ای تصادفی $f(x)$ از درجه $t-1$ با ضرایبی از z_q انتخاب می‌شود. علاوه بر این، یک چندجمله‌ای دیگر مانند $g(x)$، به‌عنوان چندجمله‌ای پشتیبان $f(x)$ در نظر گرفته می‌شود؛ به‌طوری‌که به‌جز دو ضریب که با ضریب $f(x)$ مطابقت دارند، همه ضرایب تصادفی هستند. درنتیجه، سهم‌های $f(x)$ به سهم‌های $g(x)$ و سهم‌های $g(x)$ به سهم‌های $f(x)$ مربوط می‌شوند. این نکته، هیچ نقطه‌ضعفی در تولید سهم ایجاد

نمی‌کند. برای این موضوع در ادامه یک قضیه ارائه‌شده است.

قضیه ۴-۱- طرح پیشنهادی، یک طرح تسهیم راز کامل (t,n) است.

اثبات: همان‌طور که گفته شد، یک طرح تسهیم راز، یک طرح تسهیم راز کامل (t,n) است؛ هرگاه t سهم یا بیشتر بتوانند راز را بازسازی کنند. اما $t-1$ سهم یا کمتر نمی‌توانند هیچ اطلاعاتی در مورد راز دریافت کنند. در این طرح، راز S با استفاده از طرح اصلی شامیر، به n سهم تقسیم می‌شود. بدیهی است که t سهم یا بیشتر، می‌توانند راز را بازسازی کنند.

در ادامه مشخص می‌شود $t-1$ سهام‌دار، نمی‌توانند هیچ اطلاعاتی را در مورد راز دریافت کنند. ازآنجایی‌که در طرح پیشنهادی، ارتباط ضرایب a_i, b_i و a_j, b_j به نحوی است که در روابط $a_j \cdot b_j = m$ و $a_i \cdot b_i = m$ صدق می‌کنند، اکثر افراد معتقدند حمله جستجوی فراگیر[1]، بهترین روش برای به دست آوردن راز است. روش جستجوی فراگیر را می‌توان بدین شرح توصیف کرد.

$t-1$ سهام‌دار، هر سهم احتمالی از t اُمین سهامدار را امتحان می‌کنند و به تعداد rچندجمله‌ای متناظر با $\mathrm{f_i(x)}$ و همچنین rچندجمله‌ای متناظر با $g_j(x)$ $(i,j \in [1,r])$ به دست می‌آورند. حال اگر یک چندجمله‌ای مانند $f_i(x)$ و $g_j(x)$ در روابط $a_i \cdot b_i = m$ و $a_j \cdot b_j = m$ صدق کنند، در این صورت $f_i(x)$ و $g_j(x)$چندجمله‌ای‌های اصلی خواهند بود و $S = f_i(0)$ برقرار است.

در اینجا اثبات می‌شود که روش جستجوی فراگیر در طرح پیشنهادی این مقاله عمل نمی‌کند. فرض کنید u_t^*، سهم t اُمین سهامدار است که تصادفی انتخاب می‌شود. سپس $t-1$ سهامدار، یک چندجمله‌ای $f_i(x)$ از درجه $t-1$ با سهم‌های (t,u_t^*)و $(x_1, f(x_1)), (x_2, f(x_2)), \dots, (x_{t-1}, f(x_{t-1}))$ تشکیل می‌دهند. همان‌طور که در روش جستجوی فراگیر گفته شد، چندجمله‌ای $g_j(x) = b'_0 + b'_1 x + \cdots + b'_{t-1} x^{t-1}$ از درجه‌ای $t-1$ وجود دارد که با استفاده از v_t^* تشکیل‌شده است (v_t^* سهم سهامدار t اُم است که می‌تواند هر مقداری در z_q باشد) و ضرایب هر دو چندجمله‌ای در روابط (۱۰) صدق می‌کنند.

$$a'_i \cdot b'_i = m \quad \text{و} \quad a'_j \cdot b'_j = m \qquad (10)$$

در این صورت $S = f'(0)$ خواهد بود. اما بر اساس این مشاهدات، با استفاده از روش جستجوی فراگیر، $t-1$ سهامدار متوجه خواهند شد که راز S، می‌تواند هر مقداری در z_q باشد.

در ادامه با یک مثال مشخص می‌شود که چگونه این حمله در طرح پیشنهادی این مقاله، کار نمی‌کند.

مثال ۴-۱- فرض کنید $t = 4$ و دو چندجمله‌ای $f(x) = 2x^3 + x^2 + 5x + 4$ و $g(x) = x^3 + 5x^2 + 2x + 6$ از درجه $t-1$ روی میدان z_7 توسط توزیع‌کننده انتخاب شده‌اند. قابل‌ملاحظه است که روابط $a_0 \cdot b_0 = 3$ و $a_1 \cdot b_1 = 3$ در دو چندجمله‌ای f و g برقرارند. فرض کنید سهامداران P_1, P_2, P_3, P_4 ، در بازسازی راز شرکت دارند و سهم هرکدام به‌صورت زیر است.

$$P_1 = (u_1 = 5, v_1 = 0)$$
$$P_2 = (u_2 = 4, v_2 = 3)$$
$$P_3 = (u_3 = 5, v_3 = 2)$$
$$P_4 = (u_4 = 0, v_4 = 4)$$

حال فرض کنید سهامداران P_1, P_2, P_3 بخواهند با روش جستجوی فراگیر به راز دست یابند. همان‌طور که قبلا تشریح شد، آنها می‌توانند سهم سهامدار P_4 را برابر $u_4^* = 6$ فرض کنند و چندجمله‌ای $f'(x) = 2x^3 + 3x^2 + 4x + 3$ را با استفاده از درون‌یابی لاگرانژ محاسبه کنند. درگام بعدی، آنها می‌توانند تمام سهم‌های ممکن v_4^* از سهامدار P_4 را امتحان کنند که آیا مناسب است یا خیر؟ وقتی آنها $v_4^* = 3$ را امتحان می‌کنند، چندجمله‌ای درونیابی شده $g'(x) = x^3 + 6x^2 + 6x + 1$ را بدست می‌آورند که ضرایب آن در $a'_0 \cdot b'_0 = 3$ و $a'_1 \cdot b'_1 = 3$ صدق می‌کنند. در این صورت آنها باور خواهند کرد که $f'(x)$ و $g'(x)$ چندجمله‌ای‌های اصلی هستند که توسط توزیع‌کننده انتخاب شده‌اند و راز $S = f'(0) = 3$ است. ولی بدیهی است که آنها راز را اشتباه بدست آورده‌اند. در واقع با استفاده از روش جستجوی فراگیر متوجه خواهند شد، هر سهم ممکن u_4^* سهم صحیح P_4 خواهد بود زیرا برای هر سهم ممکن u_4^*، یک سهم v_4^* وجود دارد که روابط مربوطه را برآورده می‌کند. در نتیجه $t-1$ سهامدار نمی‌توانند هیچ اطلاعاتی در مورد راز دریافت کنند.

قضیه ۴-۲- هنگامی که $t-1$ متقلب در مرحله بازسازی راز حضور داشته باشند، طرح پیشنهادی می‌تواند تقلب‌ها را با پارامترهای، احتمال موفقیت در تقلب $\epsilon = \frac{2}{t(t-1)q}$، اندازه راز برابر با طول بیتی q و اندازه سهم $|d| = 2|S|$ تشخیص دهد.

اثبات: فرض کنید $P_1, P_2, \dots, P_t$ سهامدار، در مرحله بازسازی

[1] Exhaustion attack

راز شرکت داشته باشند و $P_1, P_2, \dots, P_{t-1}$ سهامدار بخواهند سهامدار P_t را فریب دهند و راز را بدست آورند. همچنین فرض کنید، سهامداران ناصادق، چندجمله‌ای $f'(x) = a'_0 + a'_1 x + \cdots + a'_{t-1} x^{t-1}$ را با استفاده از سهم‌های $(1, u'_1), (2, u'_2), \dots, (t, 0)$ و به‌وسیله‌ای درونیابی‌لاگرانژ طوری بازسازی کنند که $f'(t) = 0$ باشد. به همین ترتیب چندجمله‌ای $g'(x) = b'_0 + b'_1 x + \cdots + b'_{t-1} x^{t-1}$ را با استفاده از سهم‌های $(1, v'_1), (2, v'_2), \dots, (t, 0)$ بازسازی کنند. سپس سهامداران با ارائه سهم‌های

$d_i = (u_i + u'_i, v_i + v'_i)(i = 1, 2, \dots, t-1)$ و

سهم سهامدار t اُم $d_t = (u_t, v_t)$، دو چندجمله‌ای $f''(x) = f(x) + f'(x)$ و $g''(x) = g(x) +$ $g'(x)$ را می‌سازند. چون $f'(x)$ و $g'(x)$توسط سهامداران ناصادق ساخته شده‌اند، پس مقدار m' وجود دارد که در روابط $a'_0 \cdot b'_0 = m'$ و $a'_1 \cdot b'_1 = m'$ صدق می‌کند. حال طبق طرح ارائه شده، اگر m' در روابط (۱۱) صدق کند، تقلب تشخیص داده نمی‌شود.

$$\begin{cases} \left(a_0 + a'_0\right) \cdot \left(b_0 + b'_0\right) = m' \\ \left(a_1 + a'_1\right) \cdot \left(b_1 + b'_1\right) = m' \end{cases} \qquad (11)$$

پس می‌توان نتیجه گرفت تقلب زمانی موفق خواهد بود که $m = m'$ باشد و جایگاه ضرایب، یعنی i, j، درست تشخیص داده شوند. اما سهامداران هیچ اطلاعی از مقدار m و i, j ندارند. می‌دانیم $\binom{t}{2} = \frac{t(t-1)}{2}$ حالت، برای انتخاب i, j وجود دارد؛ پس احتمال این که اندیس‌های i, j درست انتخاب شوند برابر $\frac{2}{t(t-1)}$ است. همچنین چون $m \in z_q$ است، پس احتمال اینکه $m = m'$ باشد، برابر $\frac{1}{q}$ است. بنابراین $\epsilon = \frac{2}{t(t-1)q}$ خواهد بود. از طرفی چون راز S از میدان z_q انتخاب می‌شود، اندازه راز برابر با طول بیتی q و اندازه سهم‌ها نیز برابر $|d| = 2|S|$ خواهد بود.

۵- مقایسه طرح پیشنهادی با طرح‌های مشابه قبلی

در اکثر طرح‌های موجود در زمینه تشخیص تقلب، شرکت‌کنندگان به دو گروه صادق و نا صادق تقسیم می‌شوند. شرکت‌کنندگان صادق نقش تشخیص متقلب را از میان مجموعه شرکت‌کنندگان نا صادق بازی می‌کنند؛ بنابراین، برای تعداد شرکت‌کنندگان نا صادق جهت تشخیص توسط طرح تسهیم راز باقابلیت تشخیص تقلب، یک مقدار آستانه وجود دارد. در این مقاله، این مقدار آستانه به‌عنوان توانایی تشخیص تقلب نامیده شده است. در این بخش، طرح پیشنهادی از نظر تشخیص تقلب، حداکثر تعداد تقلب‌هایی که می‌تواند تشخیص داده شود، اندازه سهم‌ها و احتمال موفقیت در تقلب با طرح‌های تسهیم راز با تشخیص تقلب موجود مقایسه می‌شود. باتوجه‌به جدول (۱) در طرح پیشنهادی، احتمال موفقیت در تقلب توسط شرکت‌کنندگان نا صادق برابر مقدار ناچیز $\epsilon = \frac{2}{t(t-1)q}$ است. باتوجه به اینکه حداقل آستانه در طرح‌های تسهیم راز برابر ۲ است، بنابراین $t(t-1) \geq 2$ بوده و این موضوع کارآیی طرح پیشنهادی نسبت به طرح‌های موجود را نشان می‌دهد.

جدول (۱): مقایسه طرح پیشنهادی با طرح‌های قبلی

طرح	اندازه سهم	بیشینه تقلب قابل‌تشخیص	احتمال موفقیت در تقلب
طرح هارن [۱۲]	$\|d\| = \|S\|$	بدون تشخیص تقلب	×
طرح پیپرزیک [۵]	$\|d\| = \|S\|$	۱	$\epsilon = \frac{1}{q}$
طرح کابلو [۱۰]	$\|d\| = \frac{2\|S\|}{\epsilon}$	$t-1$	$\epsilon = \frac{2}{q}$
طرح لیو [۶]	$\|d\| = \frac{\|S\|}{\epsilon}$	$t-1$	$\epsilon = \frac{1}{q}$
طرح ساتو [۹]	$\|d\| = p\|S\|$	$t-1$	$\epsilon = \frac{1}{q}$
طرح پیشنهادی	$\|d\| = 2\|S\|$	$t-1$	$\epsilon = \frac{2}{t(t-1)q}$

۶- نتیجه‌گیری

در این مقاله، به‌منظور تشخیص تقلب در تسهیم راز، به بررسی خاصیت وارون‌پذیر بودن ضرایب چندجمله‌ای‌ها و همچنین اهمیت تشخیص تقلب در طرح‌های تسهیم راز خطی پرداخته شده است. نتایج حاصل از این تحقیق نشان می‌دهد با استفاده از خاصیت وارون‌پذیری ضرایب چندجمله‌ای‌ها، می‌توان با اطمینان بالایی تأیید کرد که تسهیم راز صحیحی انجام شده و هیچ‌گونه تقلبی رخ نداده است.

روش ارائه شده در این مقاله، علاوه بر دقت بالا، مشابه طرح شامیر است؛ با این تفاوت که از دو چندجمله‌ای استفاده می‌شود بنابراین، می‌توان این طرح را در محیط‌های عملی و در سیستم‌های رمزنگاری آستانه‌ای دیگر که بر اساس طرح شامیر هستند بکار گرفت تا به‌عنوان یک ابزار مؤثر در تشخیص تقلب عمل کند. این مطالعه می‌تواند به توسعه روش‌های جدید و بهبود ابزارهای موجود در زمینه تسهیم راز و امنیت اطلاعات کمک کند. همچنین، در این طرح فقط یک سهام‌دار صادق، می‌تواند تقلب را از بین $t-1$ متقلب دیگر تشخیص دهد و این می‌تواند مزیت قابل‌توجهی محسوب گردد. به طور خلاصه، مهم‌ترین نوآوری‌ها و دستاوردهای این مقاله عبارت‌اند از:

- از خاصیت وارون‌پذیری ضرایب چندجمله‌ای‌ها، برای تشخیص تقلب در تسهیم راز استفاده شده است.
- این طرح، امکان بازیابی درست راز با طول سهم‌های کوتاهی را فراهم کرده است که سربار مخابراتی طرح را کاهش می‌دهد.
- بازیابی صحیح راز، بسیار ساده‌تر از طرح‌های موجود انجام‌پذیر است و دیگر نیازی به محاسبات پیچیده برای بازیابی درست راز وجود ندارد.
- این طرح مشابه طرح شامیر است؛ با این تفاوت که از دو چندجمله‌ای استفاده می‌شود بنابراین، می‌توان این طرح را در محیط‌های عملی و در سیستم‌های رمزنگاری آستانه‌ای دیگر استفاده کرد.

در این طرح تنها یک سهام‌دار صادق می‌تواند تقلب را از بین $t-1$ متقلب دیگر تشخیص دهد.

۶. مراجع

[1] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, pp. 612-613, 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys," in Managing Requirements Knowledge, International Workshop on, pp. 313-313, IEEE Computer Society, 1979. Doi: 10.1109/AFIPS.1979.98

[3] M. Tompa and H. Woll, "How to share a secret with cheaters," journal of Cryptology, vol. 1, no. 3, pp. 133-138, 1989. Doi: https://doi.org/10.1007/BF02252871

[4] M. Carpentieri, A. D. Santis, and U. Vaccaro, "Size of shares and probability of cheating in threshold schemes," in Workshop on the Theory and Application of of Cryptographic Techniques, pp. 118-125, Springer, 1993. Doi: https://doi.org/10.1007/3-540-48285-7_10

[5] J. Pieprzyk and X.-M. Zhang, "Cheating prevention in linear secret sharing," in Australasian Conference on Information Security and Privacy, pp. 121-135, Springer, 2002. Doi: https://doi.org/10.1007/3-540-45450-0_9

[6] Y. Liu, "Linear (k, n) secret sharing scheme with cheating detection," Security and Communication Networks, vol. 9, no. 13, pp. 2115-2121, 2016. Doi: https://doi.org/10.1002/sec.1467

[7] S. Dutta, S. Jiang, and R. Safavi-Naini, "Lower bounds on the share size of leakage resilient cheating detectable secret sharing," in International Conference on Cryptology and Network Security, pp. 468-493, Springer, 2023. Doi: https://doi.org/10.1007/978-981-99-7563-1_21

[8] M. A. Hossain and R. Bandi, "A verfiable multi-secret sharing scheme based on l-intersection pair of cyclic codes," International Journal of Foundations of Computer Science, pp. 1-21, 2023. Doi: https://doi.org/10.1142/S0129054123500284

[9] K. Sato and S. Obana, "Cheating detectable secret sharing scheme from multiplicative homomorphic authentication function," in 2021 Ninth International Symposium on Computing and Networking Workshops (CANDARW), pp. 372-378, IEEE, 2021. Doi: 10.1109/CANDARW53999.2021.00069

[10] S. Cabello, C. Padro, and G. Saez, "Secret sharing schemes with detection of cheaters for a general access structure," Designs, Codes and Cryptography, vol. 25, pp. 175-188, 2002. Doi: https://doi.org/10.1023/A:1013856431727

[11] L. Cianciullo and H. Ghodosi, "Outsourced cheating detection for secret sharing," International Journal of Information Security, vol. 20, no. 6, pp. 871-878, 2021. Doi: https://doi.org/10.1007/s10207-021-00538-7

[12] L. Harn and C. Lin, "Detection and identification of cheaters in (t, n) secret sharing scheme," Designs, Codes and Cryptography, vol. 52, no. 1, pp. 15-24, 2009. Doi: https://doi.org/10.1007/s10623-008-9265-8

[13] Z. Noroozi and E. Mohamady, "Detection and correction of cheat in the secret sharing schemes with ternary codes,"Journal of Advanced Defense Science and; Technology, vol. 1, no. 2, pp. 5-12, 2019. (in Persian)

[14] M. Farhadi, H. Bypour, and R. Mortazavi, "A hash-based multi-use multi-stage secret sharing scheme with general access structure," Electronic and Cyber Defense, vol. 6, no. 3, pp. 107-115, 2018. (in Persian). Dor: https://dor.isc.ac/dor/20.1001.1.23224347.1397.6.3.9.9

[15] M. Dadfarnia and F. Adibnia, "Collusive fraud classification in network of online auction using similaritymeasure incollective classication,"Electronic and Cyber Defense, vol. 7, no. 1, pp. 95-103, 2019. (in Persian)

[16] M. Hadian Dehkordi, S. Mashhadi, and N. Kiamary, "Two verifiable multi-secret sharing schemes: A linear scheme with standard security and a lattice-based scheme," Electronic and Cyber Defense, vol. 8, no.3,pp.101-115,2020.(inPersian).Dor: https://dor.isc.ac/dor/20.1001.1.23224347.1399.8.3.8.2