دسترسی در سایتِ http://jnrm.srbiau.ac.ir
سال ششم، شماره بیست و هشتم، بهمن و اسفند ۱۳۹۹
شماره شاپا: ۲۵۸۸-۵۸۸X

دانشگاه آزاد اسلامی، واحد علوم و تحقیقات

پژوهش‌های نوین در ریاضی

تسهیم چندراز پیش‌نگر با استفاده از درونیابی لاگرانژ و قضیه باقیمانده چینی

ابراهیمی کیاسری محمد ابراهیم[۱]، میرقدری عبدالرسول[۲] ،پاک‌نیت نصراله[۳]*، نظری مجتبی[۴]

[۱] گروه ریاضی، واحد خرم‌آباد، دانشگاه آزاد اسلامی، خرم‌آباد، ایران
[۲] دانشکده و پژوهشکده فناوری اطلاعات و ارتباطات، دانشگاه جامع امام حسین(ع)، تهران، ایران
[۳] پژوهشکده علوم اطلاعات، پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)، تهران، ایران
[۴] گروه ریاضی، واحد خرم‌آباد، دانشگاه آزاد اسلامی، خرم‌آباد، ایران

تاریخ ارسال مقاله: ۱۳۹۸/۰۵/۰۶ تاریخ پذیرش مقاله: ۱۳۹۸/۱۰/۱۹

چکیده

در یک طرح تسهیم چندراز پیش‌نگر، یک یا چند راز به گونه‌ای بین مجموعه‌ای از شرکت‌کنندگان تسهیم می‌شود که ۱) امکان نوسازی سهام در فواصل زمانی مشخص بدون کمک تسهیم‌کننده وجود داشته باشد و ۲) در حالی که زیرمجموعه‌هایی مشخص از شرکت‌کنندگان به نام زیرمجموعه‌های مجاز قادر به بازسازی راز(ها) هستند، سایر زیرمجموعه‌ها قادر به کسب اطلاع در مورد راز(ها) نباشند. تنها طرح تسهیم چندراز پیش‌نگر موجود را می‌توان به عنوان ترکیبی از یک طرح تسهیم (تک) راز پیش‌نگر شناخته شده و چندین بار استفاده از سیستم رمزنگاری یک بار مصرف در نظر گرفت. این طرح دارای امنیت ضعیف است. به عبارت دیگر، افشا یا بازسازی یک یا چند راز در این طرح منجر به افشای سایر رازها می‌شود. علاوه براین، در این طرح، امکان بازسازی تدریجی رازها وجود نداشته و در آن تمام رازها به صورت هم‌زمان بازسازی می‌شوند. برای حل این مشکلات، در این مقاله با استفاده از درونیابی لاگرانژ، قضیه باقیمانده چینی و سختی مساله لگاریتم گسسته یک طرح تسهیم چندراز پیش‌نگر جدید ارایه شده که امکان بازسازی تدریجی رازها با ترتیبی از پیش تعیین شده را فراهم می‌کند. همچنین با توجه به سختی مساله لگاریتم گسسته، این طرح ویژگی وارسی‌پذیری را برآورده کرده و دارای امنیت قوی است.

واژه‌های کلیدی: تسهیم چندراز، امنیت پیش‌نگر، وارسی‌پذیری، درونیابی لاگرانژ، قضیه باقیمانده چینی.

* عهده‌دار مکاتبات: Email: pakniat@irandoc.ac.ir

۱- مقدمه

در سال ۱۹۷۹، شمیر[۱] [۱] و بلکلی[۲] [۲] مفهوم تسهیم راز را مستقل از یکدیگر معرفی کردند. در یک طرح تسهیم راز، یک تسهیم‌کننده مقدار یک راز را به‌گونه‌ای مابین مجموعه‌ای از شرکت‌کنندگان تسهیم می‌کند که در آینده شرکت‌کنندگان موجود در برخی زیرمجموعه‌های مشخص (که زیرمجموعه‌های مجاز نامیده می‌شوند) بتوانند با استفاده از سهام خود، راز را بازسازی کنند و سایر زیرمجموعه‌ها (که زیرمجموعه‌های غیرمجاز نامیده می‌شوند) نتوانند با استفاده از سهام خود اطلاعی درباره راز به دست آورند. مجموعه تمام زیرمجموعه‌های مجاز در یک طرح تسهیم راز را ساختار دسترسی آن طرح گویند. ساختار دسترسی آستانه‌ای (t, n) پرکاربردترین نوع ساختار دسترسی طرح‌های تسهیم راز بوده که در آن هر زیرمجموعه‌ای شامل حداقل t شرکت‌کننده مجموعه‌ای مجاز است. ذکر این نکته در اینجا ضروری است که ساختار دسترسی هر دو طرح شمیر [۱] و بلک‌لی [۲] آستانه‌ای است. در یک طرح تسهیم راز معمولی، تسهیم‌کننده راز و شرکت‌کنندگان قادرند با ارایه سهام نامعتبر به سوء استفاده از سایر شرکت‌کنندگان بپردازند. برای جلوگیری از این کار، چور[۳] و همکاران [۳]، مفهوم تسهیم راز وارسی‌پذیر را ارایه کرده‌اند. امنیت یک طرح تسهیم راز را می‌توان در برابر دو نوع متخاصم ایستا یا متخاصم سیار بررسی کرد. امنیت در برابر متخاصم ایستا برای رازهای با طول عمر کم کافی است. اما در بسیاری از کاربردها مانند تسهیم کلیدهای اصلی رمزنگاری، فایل‌های داده، اسناد حقوقی و غیره نیاز است که رازها برای مدت زمانی طولانی ذخیره شوند. در این شرایط، یک متخاصم سیار قادر است با توجه به وجود زمان کافی، در طول زمان به سهام متناظر با هر زیرمجموعه مجازی از شرکت‌کنندگان دست یافته و راز را بازسازی کند. در نتیجه، برای اطمینان از امنیت رازهای با طول عمر زیاد باید سهام متناظر با راز در زمان‌هایی مشخص به‌گونه‌ای نوسازی شوند که سهام موجود در بازه‌های زمانی قبل در بازه زمانی جدید بدون ارزش شوند. این دقیقا همان کاری است که در تسهیم راز پیش‌نگر انجام می‌شود. در یک طرح تسهیم راز پیش‌نگر، زمان به چندین زیربازه تقسیم شده و در آغاز هر زیربازه، شرکت‌کنندگان به کمک یکدیگر سهام جدید خود از راز را به دست آورده و سهام قبلی خود را حذف می‌کنند [۴، ۵].

۱-۱هدف و ضرورت

متاسفانه، اغلب طرح‌های تسهیم راز پیش‌نگر موجود، تنها قادر به تسهیم یک راز در هر بار اجرای خود هستند. تنها طرح تسهیم چند راز پیش‌نگر ارایه شده [۶] و همچنین، تنها روش ارایه شده برای تبدیل طرح‌های تسهیم (یک) راز به طرح‌های تسهیم چند راز [۷] نیز از مجموعه‌ای از نقطه‌ضعف‌ها رنج می‌برند که از آن جمله می‌توان به موارد زیر اشاره کرد:

۱. امکان بازسازی تدریجی رازها در آن وجود ندارد.
۲. در صورت افشا یک راز، سایر رازها نیز افشا می‌شوند.
۳. مقادیر اعلام عمومی شده، اطلاعاتی را در مورد رازها افشا می‌کنند.

۱-۲ نوآوری

در این مقاله، برای حل مشکلات فوق، از ایده طرح تسهیم چند راز ارایه شده در [۲] استفاده کرده و با استفاده از خواص چندجمله‌ای‌ها و قضیه باقیمانده چینی[۴]، یک طرح تسهیم چندراز پیش‌نگر جدید ارایه می‌کنیم که در آن ویژگی وارسی‌پذیری[۵] نیز با توجه به سختی حل مساله لگاریتم گسسته[۶] تامین شده است. در ادامه، امنیت طرح پیشنهادی و کارایی آن را بررسی کرده و به مقایسه آن با طرح‌های مشابه موجود می‌پردازیم. نتایج ارزیابی نشان‌دهنده این است که طرح پیشنهادی از نظر هزینه محاسباتی، مخابراتی و اندازه سهام از کارایی بهتری در مقایسه با طرح‌های موجود برخوردار بوده و در عین حال ویژگی‌های قابلیت بازسازی تدریجی و ترتیبی رازها و همچنین امنیت قوی در تسهیم چند راز را فراهم می‌کند.

---

[۱] Shamir
[۲] Blakley
[۳] Chor
[۴] Chinese remainder theorem
[۵] Verifiability
[۶] Discrete logarithm problem

۳-۱ کارهای مرتبط

امنیت طرح‌های تسهیم راز در برابر متخاصم سیار اولین بار توسط استروسکی[۷] و یانگ[۸] [۴] مورد بحث واقع شده است، اما اولین طرح تسهیم راز پیش‌نگر در [۵] توسط هرزبرگ و همکاران ارایه شده است. در [۸]، ژو[۹] و همکاران یک طرح تسهیم راز پیش‌نگر جدید ارایه کرده‌اند. متاسفانه در این طرح، بازسازی سهام نیازمند به مشارکت تسهیم‌کننده است. در سال ۲۰۰۵، ژاو[۱۰] و همکاران [۹] یک طرح تسهیم راز پیش‌نگر جدید ارایه کردند که قابل استفاده در سیستم‌های غیرهمگام است. در سال ۲۰۱۰، اسکولتز[۱۱] و لیسکو[۱۲] [۱۰] یک طرح تسهیم راز پیش‌نگر جدید ارایه کردند که در آن مجموعه شرکت‌کنندگان نیز در طول زمان متغیر است. در [۱۱]، نویسندگان یک طرح تسهیم راز پیش‌نگر با ساختار دسترسی کلی ارایه کرده‌اند. تسهیم راز اجتماعی [۱۲-۱۴] یکی از کاربردهای اصلی تسهیم راز پیش‌نگر است که در آن نیاز به نوسازی سهام وجود داشته و ارزش سهام شرکت‌کنندگان نیز در طول زمان متغیر است.

در همه روش‌های بررسی شده تا بدین‌جا، در هر اجرا تنها یک راز قابل تسهیم است. به عبارت دیگر برای تسهیم چند راز با استفاده از این روش‌ها، باید هر یک از این روش‌ها را به تعداد رازها اجرا کرد. با توجه به این مساله، این طرح‌ها در موقعیت‌هایی که تسهیم همزمان چندین راز مدنظر است ناکارا هستند. مفهوم تسهیم چند راز برای اولین بار در سال ۱۹۹۵ توسط هارن[۱۳] [۱۵] ارایه شده است. در ادامه، طرح‌های تسهیم چند راز زیادی ارایه شده که در آن‌ها سعی شده کارایی یا امنیت افزایش یافته و یا قابلیت‌های جدیدی ارایه شده و یا از ساختار دسترسی‌های گسترده‌تری پشتیبانی شود. برای کسب اطلاع بیشتر در مورد این طرح‌ها، خوانندگان علاقمند به [۱۶-۲۲] ارجاع داده می‌شوند. در [۷]، نویسندگان با استفاده از اتوماتای سلولی و رمزگذاری متقارن روشی ارایه کرده‌اند که با استفاده از آن می‌توان هر طرح تسهیم راز تکی را به یک طرح تسهیم چند راز تبدیل کرد.

در [۶]، فنگ[۱۴] و همکاران یک طرح تسهیم چندراز پیش‌نگر ارایه کرده‌اند. در این طرح، یکی از رازها با استفاده از روش هرزبرگ[۱۵] و همکاران [۵] مابین مجموعه شرکت‌کنندگان تسهیم شده و نتیجه xor سایر رازها با این راز اعلام عمومی می‌شود. برای بازسازی رازها، نیز در ابتدا از فرایند بازیابی طرح هرزبرگ و همکاران استفاده شده و راز تسهیم شده بازسازی می‌شود. در ادامه سایر رازها، با xor مقدار به دست آمده و مقادیر اعلام عمومی شده محاسبه می‌شوند.

۴-۱ ساختار مقاله

در ادامه این مقاله، در بخش ۲، به بررسی پیش‌نیازهای این مقاله شامل درونیابی لاگرانژ، قضیه باقیمانده چینی و مساله لگاریتم گسسته پرداخته می‌شود. در بخش ۳، طرح تسهیم چند راز پیش‌نگر پیشنهادی ارایه شده و امنیت و کارایی آن در بخش ۴ بررسی می‌شود. در نهایت، نتیجه‌گیری‌ها در بخش۵ بیان شده است.

۲- مباحث مقدماتی

۲-۱ درونیابی لاگرانژ

تعریف ۲-۱-۱ درونیابی لاگرانژ[۱۶]: فرض کنیم نقاط (x_n, y_n)،..،(x_0, y_0) با مولفه‌های اول متمایز داده شده باشند. مساله درونیابی لاگرانژ متناظر با نقاط فوق عبارت است از محاسبه چندجمله‌ای $p(x)$ با کمترین درجه ممکن به طوری که

$$\{p(x_i) = y_i\}_{i=0}^{n} \qquad (۱)$$

برای محاسبه جواب مساله درونیابی لاگرانژ فوق، چندجمله‌ای $p(x)$ را به صورت زیر می‌سازیم:

$$p(x) = \sum_{i=0}^{n} y_i . L_i(x) \qquad (۲)$$

که $L_i(x)$ ها چندجمله‌ای‌های لاگرانژ بوده و به صورت زیر محاسبه می‌شوند:

---

[۷] Ostrovsky
[۸] Yung
[۹] Xu
[۱۰] Zou
[۱۱] Schultz
[۱۲] Liskov
[۱۳] Harn
[۱۴] Feng
[۱۵] Herzberg
[۱۶] Lagrange interpolation

$$L_i(x) = \prod_{0\le m\le n, m\neq i} \left(\frac{x-x_m}{x_i-x_m}\right) \quad (۳)$$

۲-۲ مسئله لگاریتم گسسته (DLP)

امنیت بسیاری از سیستم‌های رمزنگاری بر حل یک مسئله‌ی سخت ریاضی به نام مسئله لگاریتم گسسته استوار است. مسائلی مانند توافق کلید دیفی–هلمن و مشتقات آن، سیستم رمزنگاری الجمال، امضای دیجیتال الجمال و مشتقات آن و غیره از این دسته‌اند.

تعریف ۲-۲-۱ فرض کنید G یک گروه دوری متناهی از مرتبه n با عملگر $\times$، $g \in G$ یک مولد و $h \in G$ یک عضو دلخواه از آن باشد. لگاریتم گسسته h در پایه g، که با $Log_g h$ نشان داده می‌شود، عدد صحیحی مثل $x\,(0 \le x \le n-1)$ است که $\underbrace{g \times g \times ... \times g}_{x \text{ مرتبه با}} = h$.

تعریف ۲-۲-۲ مسئله لگاریتم گسسته تعمیم‌یافته $[GDLP]$: اگر G یک گروه دوری متناهی از مرتبه n با عملگر $\times$ $g \in G$ یک مولد و $h \in G$ یک عضو دلخواه از آن باشد، عدد صحیح x را بیابید که $\underbrace{g \times g \times ... \times g}_{x \text{ مرتبه با}} = h$. همان‌طور که از نام این مسئله مشخص است، این مسئله تعمیم‌یافته مسئله لگاریتم گسسته است که تنها حالاتی را در نظر می‌گیرد که $G = \mathbb{Z}_p^*$ و p عددی اول باشد.

۲-۳ قضیه باقیمانده چینی (CRT)

فرض کنید $m_1, m_2, ..., m_r$ اعداد صحیح مثبت باشند. به طوری که دو به دو نسبت به هم اول باشند. فرض کنید $a_1, a_2, ..., a_r$ نیز اعدادی صحیح و دلخواه باشند. آن‌گاه دستگاه $x \equiv a_i \pmod{m_i},\ 1 \le i \le r$ فقط و فقط یک جواب در پیمانه $M = m_1 \times m_2 \times .... \times m_r$ دارد که برابر است با:

$$x = \sum_{i=1}^{r} a_i . M_i . y_i \quad (۴)$$

که در آن $y_i = M_i^{-1} \bmod m_i, M_i = \frac{M}{m_i}$. اثبات در [۲۳].

۳- طرح پیشنهادی

در این بخش، یک طرح تسهیم چند راز پیش‌نگر جدید ارایه می‌شود. در طرح پیشنهادی در ابتدا مجموعه‌ای از m راز مابین مجموعه شرکت‌کنندگان تسهیم می‌شود. در ادامه، شرکت‌کنندگان می‌توانند رازها را به ترتیبی از پیش تعیین‌شده بازسازی کنند. در طرح ارایه شده، برای به دست آوردن امنیت در دراز مدت، شرکت‌کنندگان قادر هستند بدون نیاز به کمک تسهیم‌کننده سهام خود را از مجموعه رازها نوسازی کرده و بدین طریق، در صورتی که متخاصمی سیار سعی کند در طول زمان به سراغ شرکت‌کنندگان موجود در مجموعه‌ای مجاز رفته، سهام آن‌ها را به دست آورده و از آن برای بازسازی راز استفاده کند، تلاش‌های این متخاصم را بی‌اثر کنند. برای سادگی، در طرح جدید ارایه شده برای تمام رازها یک ساختار دسترسی یکسان درنظر گرفته شده است اما به آسانی می‌توان آن را به‌گونه‌ای تغییر داد که هر راز ساختار دسترسی دلخواه منحصر به خود را داشته باشد.

فرض کنید $P = \{P_1, P_2, ..., P_n\}$ مجموعه‌ای شامل n شرکت‌کننده و $t \le n$ مقداری آستانه‌ای باشد. همچنین، فرض کنید $S = \{S_1, S_2, ..., S_m\} \subset Z_q$ مجموعه رازهایی باشد که قصد تسهیم آن‌ها مابین مجموعه شرکت‌کننده‌ها وجود دارد. به‌علاوه، q را به عنوان عددی اول و بزرگ در نظر بگیرید. طرح تسهیم چند راز پیش‌نگر پیشنهادی از سه پروتکل ۱) تسهیم راز، ۲) نوسازی سهام و ۳) بازیابی راز، تشکیل شده که در ادامه جزئیات این پروتکل‌ها بررسی می‌شوند.

۳-۱ تسهیم راز

برای تسهیم مجموعه رازهای $S = \{S_1, S_2, ..., S_m\} \subset Z_q$ مابین مجموعه شرکت‌کننده‌های $P = \{P_1, P_2, ..., P_n\}$ از پروتکل تسهیم راز با گام‌های زیر استفاده می‌شود:

تسهیم‌کننده راز:

۱- اعداد $q_1, q_2, ..., q_n$ را که نسبت به هم اول هستند به عنوان پیمانه‌های متناظر با قضیه باقیمانده چینی انتخاب می‌کند.

۲- مولد ضربی g در Z_q^* را انتخاب می‌کند.

۳- اعداد تصادفی $v_2, v_3, ..., v_m$ را متناظر با رازهای $S_2, S_3, ..., S_m$ را انتخاب می‌کند.

۴- مقدار i را برابر با m قرار می‌دهد.

۵- مقدار T_i را به صورت تصادفی از Z_q انتخاب می‌کند.

۶- مقادیر $a_{1,i}, a_{2,i}, \dots, a_{t-1,i}$ را به صورت تصادفی از Z_q انتخاب، مقدار $a_{.,i} = S_i || T_i$ را محاسبه کرده و چندجمله‌ای زیر را می‌سازد:

$$f_i(x) = a_{.,i} + a_{1,i}x + a_{2,i}x^2 + \cdots + a_{t-1,i}x^{t-1} \quad (۵)$$

۷- برای $j = 1, \dots, n$: سهم شرکت‌کننده P_j از راز S_i را به صورت $SH_j^i = f_i(x_j) \pmod q$ محاسبه می‌کند.

۸- برای $k = 0, \dots, t-1$: مقادیر $y_k^i = g^{a_{k,i}} \pmod q$ را محاسبه می‌کند.

۹- مقدار $C_i = CRT(SH_1^i, SH_2^i, \dots, SH_n^i)$ را محاسبه می‌کند.

۱۰- مقدار $T_i = C_i + V_i$ را محاسبه می‌کند.

۱۱- مقدار i را برابر با $i-1$ قرار داده و در صورتی که $i \geq 1$ باشد به مرحله ۶ برمی‌گردد.

۱۲- از طریق یک کانال امن مقادیر $v_2, v_3, \dots, v_m$ را به شخص سوم مورداعتماد و سهم‌های (SH_1^1, q_1)، (SH_2^1, q_2)، ... و (SH_n^1, q_n) را به ترتیب به شرکت‌کننده‌های P_1، P_2، ... و P_n ارسال می‌کند.

۱۳- مقادیر q، g، n، m و y_k^i (برای $i = 1, \dots, m$ و $k = 0, \dots, t-1$) را اعلام عمومی می‌کند.

هر شرکت‌کننده P_j، پس از دریافت سهم (SH_j^1, q_j) درستی سهم دریافتی را به صورت زیر بررسی می‌کند:

$$g^{SH_j^1} =^? \prod_{k=0}^{t-1} (y_k^1)^{x_j{}^k} \pmod q \quad (۶)$$

در صورت برقراری رابطه فوق، P_j سهم دریافتی را پذیرفته و در غیر این صورت آن را رد کرده و علیه تسهیم‌کننده اعلام شکایت می‌کند.

۳-۲ نوسازی سهام

از طریق این پروتکل، سهم شرکت‌کننده‌ها در زمان‌هایی مشخص نوسازی می‌شود. این پروتکل نیازی به برخط بودن تسهیم‌کننده رازها نداشته و مجموعه‌ای مجاز از کاربران قادرند با کمک یکدیگر این پروتکل را اجرا کرده و سهم همه کاربران را نوسازی کنند. فرض کنید Sub مجموعه‌ای از شرکت‌کنندگان باشد که قصد دارند در فرایند نوسازی سهام شرکت کنند و S_i را از متناظر با سهم‌های فعلی شرکت‌کنندگان باشد. در این پروتکل، هر شرکت‌کننده $P_j \in Sub$:

۱- چندجمله‌ای زیر را می‌سازد:

$$g_{i,j}(x) = a_{.,i,j} + a_{1,i,j}x + a_{2,i,j}x^2 + \cdots + a_{t-1,i,j}x^{t-1} \quad (۷)$$

که $a_{.,i,j}, a_{1,i,j}, \dots, a_{t-1,i,j}$ به صورت تصادفی از Z_q انتخاب شده‌اند.

۲- سهم هر شرکت‌کننده $P_l \in P$ از چندجمله‌ای $g_{i,j}(x)$ را به‌صورت $SH_l^{i,j} = g_{i,j}(x_l) \pmod q$ محاسبه و از طریق یک کانال امن به او ارسال می‌کند.

۳- برای $k = 0, \dots, t-1$: مقادیر $y_k^{i,j} = g^{a_{k,i,j}} \pmod q$ را محاسبه و اعلام عمومی می‌کند.

هر شرکت‌کننده $P_r \in P$، پس از دریافت سهام خود از شرکت‌کنندگان موجود در Sub:

۱- برای هر j که $P_j \in Sub$: درستی سهم دریافتی خود از P_j را به صورت زیر بررسی می‌کند:

$$g^{SH_r^{i,j}} =^? \prod_{k=0}^{t-1} (y_k^{i,j})^{x_r{}^k} \pmod q \quad (۸)$$

در صورت عدم برقراری رابطه فوق علیه P_j اعلام شکایت می‌کند.

۲- در صورتی که حداکثر $t-1$ شرکت‌کننده علیه P_j اعلام شکایت کرده باشند، P_j را به مجموعه (ابتدا" تهی) QSub اضافه می‌کند و P_j سهم شرکت‌کننده‌هایی که علیه او اعلام شکایت کرده‌اند، را اعلام عمومی می‌کند.

۳- در صورتی که $|QSub| \geq t$، سهم جدید خود از رازهای بازسازی نشده را به صورت زیر بازسازی می‌کند:

$$(SH_r^i = SH_r^i + \sum_{j:P_j \in QSub} SH_r^{i,j}, q_r) \quad (۹)$$

۳-۳ بازسازی راز

از طریق پروتکل بازسازی شرکت‌کنندگان قادر به بازسازی رازها به ترتیب از پیش تعیین‌شده هستند. فرض کنید Sub مجموعه‌ای از شرکت‌کنندگان باشد که قصد دارند بازسازی راز را انجام دهند. علاوه‌براین، فرض کنید S_i آخرین رازی است که در ترتیب در نظر گرفته شده بازسازی نشده است. با توجه به این موارد، برای بازسازی S_i:

هر شرکت‌کننده $P_j \in Sub$:

مقدار SH_j^i متناظر با سهم خود از راز S_i را از طریق کانال امن به شخص مورد اعتماد ارسال می‌کند.

شخص مورد اعتماد:

۱- با توجه به رابطه (۱۰) درستی سهم متناظر با P_j را بررسی می‌کند:

$$g^{SH_j^i} =^? \prod_{k=.}^{t-1}(y_k^i)^{x_j{}^k} \pmod q \quad (۱۰)$$

۲- در صورت برقراری رابطه فوق P_j را به مجموعه (ابتدا" تهی) QSub اضافه می‌کند.

۳- در صورتی که $|QSub| \geq t$، با اعمال درون‌یابی لاگرانژ بر روی مجموعه زوج‌های (x_j, SH_j^i) برای $j \in QSub$ و استفاده از ضریب ثابت چندجمله‌ای درونیابی شده راز $S_i||T_i$ را بازسازی می‌کند.

۴- راز S_i را از طریق کانال امن به اعضای QSub ارسال می‌کند.

۵- در صورتی که $i = ۰$ مقدار v_i را برابر با رشته‌ای تماما صفر قرار می‌دهد.

۶- مقدار $C_{i+1} = V_{i+1} \oplus T_i$ را محاسبه کرده و از طریق کانال امن به همه شرکت‌کنندگان ارسال می‌کند.

هر شرکت‌کننده $P_j \in P$:

۱- سهم خود از راز S_{i+1} را برابر با $(SH_j^{i+1} = C_i\ (mod\ q_j), q_j)$ قرار می‌دهد.

۲- درستی سهم خود از راز S_{i+1} را به صورت زیر بررسی می‌کند:

$$g^{SH_j^{i+1}} =^? \prod_{k=.}^{t-1}(y_k^{i+1})^{x_j{}^k} \pmod q \quad (۱۱)$$

٤- بررسی امنیت و کارایی طرح پیشنهادی

در این بخش، ابتدا امنیت طرح پیشنهادی و سپس کارایی آن بررسی شده و با طرح‌های مشابه موجود مورد مقایسه قرار می‌گیرد.

٤-۱ بررسی امنیت

در این بخش، امنیت طرح پیشنهادی مورد بررسی قرار می‌گیرد. امنیت طرح پیشنهادی وابسته به امنیت طرح ارایه شده توسط زارع‌پور و همکاران [۲۲] و طرح فلدمن [۲۴] است. در ادامه این بخش، برای بررسی امنیت طرح پیشنهادی، سناریوی حملات ممکن مورد بررسی قرار خواهد گرفت.

حمله: تعداد $t - ۱$ یا کمتر شرکت‌کننده قصد بازسازی یک راز را داشته باشند.

تحلیل:

فرض کنید S_i آخرین رازی باشد که در ترتیب در نظر گرفته شده بازسازی نشده است. فرض کنید $t - ۱$ شرکت‌کننده که بدون از دست رفتن کلیت مساله و برای سادگی فرض می‌کنیم $B = \{P_۱, P_۲, \dots, P_{t-۱}\}$ باشند، قصد بازسازی راز را داشته باشند. مجموعه شرکت‌کنندگان موجود در B به سهام خود از راز S_i یعنی $SH_۱^i$، $SH_۲^i$، ...، $SH_{t-۱}^i$ دسترسی دارند، اما برای بازسازی راز با توجه به ویژگی‌های درونیابی لاگرانژ نیاز به t سهم وجود دارد که با توجه به عدم دسترسی به سهم آخر، بازسازی راز ناممکن می‌شود.

حمله: t شرکت‌کننده تلاش به بازسازی رازها در ترتیبی مغایر با ترتیب از پیش تعیین‌شده دارند.

تحلیل:

بازسازی هر راز نیازمند به بازسازی یک چندجمله‌ای (رابطه (۵)) است که راز موردنظر ضریب ثابت آن چندجمله‌ای است. برای بازسازی چندجمله‌ای موردنظر در روش پیشنهادی نیازمند به t مقدار از آن چندجمله‌ای هستیم. از آن‌جا که در روش پیشنهادی، در هر زمان هر شرکت‌کننده تنها به سهم خود از آخرین راز دسترسی داشته و محاسبه سهم شرکت‌کننده از راز بعدی نیازمند محاسبه راز قبلی و مشارکت شخص مورد اعتماد است، چنین چیزی ناممکن است و در نتیجه رازها به همان ترتیب از پیش تعیین‌شده قابل بازیابی هستند.

حمله: t شرکت‌کننده به بازسازی یکباره همه رازها اقدام کنند.

تحلیل: در عمل ممکن است مجموعه‌ای از شرکت‌کنندگان، برخلاف اهداف سیستم، تصمیم به بازسازی یک‌باره همه رازها بگیرند. در روش پیشنهادی از آن‌جا که شرکت‌کنندگان برای محاسبه سهم خود از راز بعدی نیازمند مشارکت شخص سوم مورداعتماد هستند، قادر نیستند به دلخواه خود همه رازها را بازسازی کنند و

شخص سوم مورد اعتماد می‌تواند در صورت مشاهده سوءاستفاده از سیستم از بازسازی سایر رازها جلوگیری کند.
حمله: یک متخاصم سعی کند در دراز مدت سهم متناظر با t شرکت‌کننده را به دست آورد.
تحلیل: در طرح ارایه شده، همانند سایر طرح‌های تسهیم راز پیش‌نگر، در زمان‌هایی مشخص و از پیش تعیین‌شده سهام شرکت‌کنندگان از آخرین راز قابل بازسازی نوسازی می‌شود. نحوه نوسازی نیز بدین طریق است که در هر نوسازی سهام شرکت‌کنندگان از یک چندجمله‌ای جدید تنها با ضریب ثابت یکسان با چندجمله‌ای قبل محاسبه و در اختیار شرکت‌کنندگان قرار می‌گیرد. در نتیجه، در صورتی که سهام در دسترس متخاصم متناظر با بازه‌های زمانی متفاوت باشد آن‌گاه متخاصم قادر به استفاده همزمان از آن‌ها نبوده و تنها می‌تواند سهام به دست آمده در یک بازه زمانی را مورد استفاده قرار دهد. با توجه به فرض اینکه، متخاصم در یک بازه زمانی حداکثر قادر به دستیابی به $t-۱$ راز است، می‌توان نتیجه گرفت در سناریوی در نظر گرفته شده متخاصم مزیتی نداشته و قادر به کسب اطلاعی در مورد راز نیست.
حمله: متخاصم تلاش کند تا یک سهم جعلی را به عنوان یک سهم واقعی در نوسازی سهم‌ها یا بازسازی یک راز وارد کند.
تحلیل: برای بررسی این سناریو باید موارد زیر را در نظر گرفت: ۱) سهام دریافتی شرکت‌کنندگان از تسهیم‌کننده یا هر یک از شرکت‌کنندگانی که در پروتکل نوسازی سهام مشارکت می‌کنند معتبر باشد. ۲) سهم ارایه شده توسط یک کاربر برای بازسازی یک راز معتبر باشد. با توجه به عمومی‌سازی g به توان ضرایب چندجمله‌ای به کار رفته توسط تسهیم‌کننده و شرکت‌کنندگان اجرا کننده پروتکل نوسازی سهام و خواص روش‌های تسهیم راز مبتنی بر چندجمله‌ای [۲۴] دریافت‌کننده یک سهم به راحتی می‌تواند تولید سهم خود از چندجمله‌ای یکسان را بررسی کند. علاوه‌براین، روابط (۶) و (۸)، اطمینان از ارایه سهام صحیح در پروتکل بازسازی رازها را ایجاد می‌کند.
حمله: استفاده از رازهای محاسبه یا افشا شده توسط متخاصم برای دستیابی به سایر رازها.
تحلیل: با توجه به این که بازسازی راز ناشناخته نیازمند مقادیر محرمانه در اختیار شخص سوم مورداعتماد و همچنین پیمانه‌های در اختیار شرکت‌کنندگان است، در اختیار داشتن چندین راز هیچ مزیتی را برای متخاصم در راستای به دست آوردن سهام شرکت‌کنندگان و درنتیجه بازسازی رازهای نامعلوم ایجاد نمی‌کند. لازم به ذکر است که یک طرح تسهیم چند راز که در این سناریو حمله امن باشد را یک طرح تسهیم چند راز با امنیت قوی گویند و در غیر این صورت یک طرح تسهیم راز با امنیت ضعیف.

۴-۲ مقایسه با چند طرح مرتبط

در این بخش طرح پیشنهادی با چند طرح مرتبط موجود مقایسه می‌شود. مقایسه از نظر پیچیدگی محاسباتی، پیچیدگی مخابراتی، قابلیت تسهیم چند راز، قابلیت بازسازی رازها به مرور زمان، وجود ترتیب در بازسازی رازها، تصدیق‌پذیری و اندازه سهام صورت خواهد گرفت.
برای بررسی پیچیدگی محاسباتی، تنها عملگرهای محاسباتی هزینه‌بر را در نظر گرفته و از عملگرهای سبک شامل xor، باقیمانده پیمانه‌ای، جمع و تفریق چشم‌پوشی خواهد شد. در طرح ارایه‌شده، تسهیم‌کننده رازها برای محاسبه سهم شرکت‌کنندگان نیاز به محاسبه mn مقدار چندجمله‌ای از درجه t دارد که t مقدار آستانه، n تعداد کل شرکت‌کنندگان و m تعداد رازهاست. با توجه به نیاز به $۲(t-۱)$ عمل ضرب برای محاسبه مقدار یک چندجمله‌ای در یک نقطه، کل محاسبات قابل انجام توسط تسهیم‌کننده در این قسمت برابر با $۲mn(t-۱)$ است. علاوه بر محاسبه سهام، تسهیم‌کننده باید مقادیری را نیز برای تصدیق‌پذیری سهام محاسبه و اعلام عمومی کند. محاسبات موردنیاز برای پردازش این قسمت برابر با mt عمل توان‌رسانی است. لذا هزینه محاسباتی کل موارد مربوط به تسهیم‌کننده رازها برابر با است با $۲mn(t-۱)C_M + mtC_E$ که C_M هزینه محاسباتی یک عمل ضرب پیمانه‌ای و C_E هزینه محاسباتی یک عمل توان‌رسانی پیمانه‌ای است. هر شرکت‌کننده هم باید صحت سهم خود را از راز آخر در این پروتکل بررسی کند که با توجه به رابطه (۶) هزینه محاسباتی وارده به هر شرکت‌کننده برابر است با $۲(t-۱)C_M + tC_E$.

هر شرکت‌کننده P_j که در پروتکل نوسازی سهام طرح پیشنهادی مشارکت می‌کند، باید یک چندجمله‌ای از درجه $t-1$ ساخته، مقدار این چندجمله‌ای را در n نقطه محاسبه کرده و مقادیری را برای بررسی صحت سهام تولیدشده محاسبه و عمومی کند که هزینه این محاسبات برابر است با $2n(t-1)C_M + tC_E$. علاوه‌براین، همه شرکت‌کنندگان باید اعتبار سهام دریافتی از سایر شرکت‌کنندگان را در پروتکل نوسازی سهام بررسی کرده و سهم نهایی خود را با استفاده از آن‌ها محاسبه کنند. برای این منظور، شرکت‌کنندگان باید از رابطه (۸) استفاده کنند که با توجه به این رابطه، هزینه محاسباتی هر شرکت‌کننده برابر است با $t(t-1)C_M + t^2C_E$. در بازسازی راز، شرکت‌کنندگان سهام خود را به شخص سوم مورد اعتماد ارسال کرده و او راز را بازسازی و در اختیار شرکت‌کنندگان قرار می‌دهد. بدین منظور، شخص سوم مورد اعتماد اعتبار سهام دریافتی را بررسی کرده، راز را با استفاده از درونیابی لاگرانژ محاسبه کرده و در اختیار شرکت‌کنندگان قرار می‌دهد. هزینه محاسباتی وارده به شخص سوم مورد اعتماد بدین منظور عبارت است از $2(t-1)^2 + O(n\log^2 n))C_M + (t^2)C_E$. علاوه‌براین، هر شرکت‌کننده P_j نیز باید با استفاده از مقادیر دریافتی از شخص سوم، سهم جدید خود را محاسبه و صحت آن را بررسی کند که هزینه محاسباتی وارده به هر شرکت‌کننده بدین منظور عبارت است از $2(t-1)C_M + tC_E$. هزینه‌های محاسباتی طرح پیشنهادی به طور خلاصه در جدول ۱ در زیر آورده شده است. لازم به ذکر است که از آن‌جا که سایر طرح‌های مرتبط [۵، ۶] ویژگی وارسی‌پذیری را تامین نمی‌کنند لذا مقایسه کارایی طرح پیشنهادی و سایر طرح‌های مرتبط عقلانی نبوده و در این مقاله انجام نخواهد شد.

برای بررسی هزینه مخابراتی، به بررسی اندازه مجموع پیام‌های ارسالی در پروتکل‌های مختلف طرح ارایه شده پرداخته می‌شود. در این راستا، تنها پیام‌های ارسالی از طریق کانال امن در نظر گرفته شده و از سایر مقادیر ارسالی صرف‌نظر خواهد شد. به عبارت دیگر، تنها هزینه مخابراتی کانال امن در نظر گرفته خواهد شد. در پروتکل تسهیم طرح پیشنهادی، تسهیم‌کننده سهام شرکت‌کنندگان را به آن‌ها ارسال کرده و مقادیری را نیز در اختیار شخص سوم مورد اعتماد قرار می‌دهد که مجموع اندازه این مقادیر برابر با $(2n+m-1)|q|$ بیت است. در پروتکل نوسازی سهام، هر شرکت‌کننده عضو مجموعه اجراکننده این پروتکل، مقدار یک چندجمله‌ای در یک نقطه را محاسبه و به سایرین ارسال می‌کند. در نتیجه، مجموع اندازه مقادیر ارسالی در این‌جا برابر با $\big(t(n-1)\big)|q|$ بیت است. در پروتکل بازسازی، در ابتدا شرکت‌کنندگان موجود در یک مجموعه مجاز سهم خود را به شخص سوم مورد اعتماد ارسال می‌کنند. در ادامه، شخص سوم مورد اعتماد راز را بازسازی کرده و راز و مقداری که با استفاده از آن سهم جدید شرکت‌کنندگان محاسبه می‌شود را به شرکت‌کنندگان ارسال می‌کند. در نتیجه مجموع اندازه مقادیر ارسالی در این پروتکل طرح پیشنهادی برابر با $(t+2n)|q|$ بیت است. نتایج مقایسه هزینه‌های مخابراتی طرح پیشنهادی با سایر طرح‌های مرتبط در جدول ۲ آورده شده است. در این جدول و همچنین جدول ۳ منظور از [۵]+[۷] پیاده‌سازی روش تعمیم تسهیم راز تکی به تسهیم چند راز ارایه شده در [۷] با استفاده از روش تسهیم راز پیش‌نگر [۵] است.

اندازه سهم هر شرکت‌کننده در یک طرح تسهیم راز برابر با میزان اطلاعاتی است که شرکت‌کننده باید محرمانه نگهداری کند و از اهمیت بالایی در طرح‌های تسهیم راز برخوردار است. هر سهم در طرح پیشنهادی از دو قسمت تشکیل شده است، ۱) مقدار یک چندجمله‌ای در یک نقطه در پیمانه q و ۲) یک پیمانه متناظر با باقیمانده چینی که این پیمانه نیز از مرتبه q است. در نتیجه اندازه سهم هر شرکت‌کننده در طرح پیشنهادی برابر با $2|q|$ بیت است. در جدول ۳ نتایج مقایسه طرح پیشنهادی با سایر طرح‌های مرتبط با توجه به اندازه سهام و ویژگی‌های ارایه شده توسط آن‌ها آورده شده است. همان طور که نتایج جداول ۱ تا ۳ نشان می‌دهد، طرح پیشنهادی از نظر هزینه محاسباتی، مخابراتی و اندازه سهام از کارایی بهتری برخوردار بوده و در عین حال ویژگی‌های قابلیت بازسازی

تدریجی و ترتیبی رازها و همچنین امنیت قوی در تسهیم چند راز را فراهم می‌کند.

۵- نتیجه‌گیری

در ابتدا مشکلات موجود در طرح‌های تسهیم چند راز پیش‌نگر مورد بررسی قرار گرفت. در ادامه، با استفاده از درونیابی لاگرانژ، قضیه باقیمانده چینی و سختی مساله لگاریتم گسسته، یک طرح تسهیم چند راز پیش‌نگر جدید ارایه شد که امکان بازسازی تدریجی و ترتیبی رازها را فراهم کرده، با توجه به سختی مساله لگاریتم گسسته ویژگی وارسی‌پذیری را ارایه کرده و دارای امنیت قوی است. طرح پیشنهادی از نظر هزینه محاسباتی، مخابراتی و اندازه سهام از کارایی بهتری برخوردار بوده و در عین حال ویژگی‌های قابلیت بازسازی تدریجی و ترتیبی رازها و همچنین امنیت قوی در تسهیم چند راز را فراهم می‌کند.

جدول ۱: هزینه محاسباتی وارده به موجودیت‌های مختلف درگیر در پروتکل‌های مختلف طرح پیشنهادی.

پروتکل بازسازی		پروتکل نوسازی		پروتکل تسهیم راز	
$P_i \in P$	TTP	$P_i \in P$	$P_i \in Sub$	$P_i \in P$	D
$۲(t-۱)C_M + tC_E$	$(۲(t-۱)^۲ + O(nlog^۲ n))C_M + (t^۲)C_E$	$t(t-۱)C_M + t^۲C_E$	$۲n(t-۱)C_M + tC_E$	$۲(t-۱)C_M + tC_E$	$۲mn(t-۱)C_M + mtC_E$

جدول ۲: بررسی هزینه مخابراتی طرح‌های مختلف

پروتکل بازسازی	پروتکل نوسازی	پروتکل تسهیم راز	طرح
$t\|q\|$	$t(n-۱)\|q\|$	$n\|q\|$	[۵]
$t\|q\|$	$t(n-۱)\|q\|$	$n\|q\|$	[۵] و [۷]
$t\|q\|$	$t(n-۱)\|q\|$	$n\|q\|$	[۶]
$(t+۲n)\|q\|$	$t(n-۱)\|q\|$	$(۲n+m-۱)\|q\|$	پیشنهادی

جدول ۳: مقایسه چند طرح مختلف با طرح پیشنهادی از لحاظ شاخصه‌های امنیت و کارایی

امنیت	قابلیت بازسازی تدریجی رازها	قابلیت بازسازی ترتیبی رازها	قابلیت تسهیم چند راز	وارسی پذیری	اندازه‌ی سهام	طرح
قوی	خیر	خیر	خیر	خیر	$\|q\|$	[۵]
قوی	خیر	خیر	بلی	خیر	$\|q\|$	[۵] و [۷]
ضعیف	خیر	خیر	بلی	بلی	$\|q\|$	[۶]
قوی	بلی	بلی	بلی	بلی	$۲\|q\|$	پیشنهادی

مراجع

[۱] Shamir, A. (۱۹۷۹). How to share a secret. Communications of the ACM, ۲۲(۱۱), ۶۱۲-۶۱۳.

[۲] Blakley, G. R. (۱۹۷۹, June). Safeguarding cryptographic keys. In Proceedings of the national computer conference (Vol. ۴۸, No. ۳۱۳).

[۳] Chor, B., Goldwasser, S., Micali, S., & Awerbuch, B. (۱۹۸۵, October). Verifiable secret sharing and achieving simultaneity in the presence of faults. In ۲۶th Annual Symposium on Foundations of Computer Science (sfcs ۱۹۸۵) (pp. ۳۸۳-۳۹۵). IEEE.

[۴] Ostrovsky, R., & Yung, M. (۱۹۹۱, August). How to withstand mobile virus attacks. In PODC (Vol. ۹۱, pp. ۵۱-۵۹).

[۵] Herzberg, A., Jarecki, S., Krawczyk, H., & Yung, M. (۱۹۹۵, August). Proactive secret sharing or: How to cope with perpetual leakage. In Annual International Cryptology Conference (pp. ۳۳۹-۳۵۲). Springer, Berlin, Heidelberg.

[۶] Feng, B., Guo, C., Li, M., & Wang, Z. H. (۲۰۱۵). A Novel Proactive Multi-secret Sharing Scheme. IJ Network Security, ۱۷(۲), ۱۲۳-۱۲۸.

[۷] Pakniat N., Noroozi M., & Eslami Z. (۲۰۱۶). Reducing Multi-Secret Sharing Problem to Sharing a Single Secret Based on Cellular Automata. Journal on Computer Science and Engineering, ۱۴(۱), ۳۸ - ۴۳.

[۸] Min, X. C. X. W. S., & Zhen, X. G. (۲۰۰۲). A Secret Sharing Scheme with Periodic Renewing to Identify Cheaters. Chinese Journal of Computers, ۶.

[۹] Zhou, L., Schneider, F. B., & Van Renesse, R. (۲۰۰۵). APSS: Proactive secret sharing in asynchronous systems. ACM transactions on information and system security (TISSEC), ۸(۳), ۲۵۹-۲۸۶.

[۱۰] Schultz, D., Liskov, B., & Liskov, M. (۲۰۱۰). MPSS: mobile proactive secret sharing. ACM Transactions on Information and System Security (TISSEC), ۱۳(۴), ۳۴.

[۱۱] Nikov, V., Nikov, S., Preneel, B., & Vandewalle, J. (۲۰۰۲). Applying General Access Structure to Proactive Secret Sharing Schemes. IACR Cryptology ePrint Archive, ۲۰۰۲, ۱۴۱.

[۱۲] Nojoumian, M., Stinson, D. R., & Grainger, M. (۲۰۱۰). Unconditionally secure social secret sharing scheme. IET information security, ۴(۴), ۲۰۲-۲۱۱.

[۱۳] Eslami, Z., Pakniat, N., & Nojoumian, M. (۲۰۱۶). Ideal social secret sharing using Birkhoff interpolation method. Security and Communication Networks, ۹(۱۸), ۴۹۷۳-۴۹۸۲.

[۱۴] Pakniat, N., & Eslami, Z. (۲۰۱۷). Verifiable Social Multi-Secret Sharing Secure in Active Adversarial Model. Journal of Computing and Security, ۴(۱), ۳-۱۲.

[۱۵] Harn, L. (۱۹۹۵). Efficient sharing (broadcasting) of multiple secrets. IEE Proceedings-Computers and Digital Techniques, ۱۴۲(۳), ۲۳۷-۲۴۰.

[۱۶] Eslami, Z., Pakniat, N., & Noroozi, M. (۲۰۱۵, October). Hierarchical threshold multi-secret sharing scheme based on Birkhoff interpolation and cellular automata. In ۲۰۱۵ ۱۸th CSI International Symposium on Computer Architecture and Digital Systems (CADS) (pp. ۱-۶). IEEE.

[۱۷] Eslami, Z., & Rad, S. K. (۲۰۱۲). A new verifiable multi-secret sharing scheme based on bilinear maps. Wireless Personal Communications, ۶۳(۲), ۴۵۹-۴۶۷.

[۱۸] Mashhadi, S., & Dehkordi, M. H. (۲۰۱۵). Two verifiable multi secret sharing schemes based on nonhomogeneous linear recursion and LFSR public-key

cryptosystem. Information Sciences, ۲۹۴, ۳۱-۴۰.

[۱۹] Liu, Y., Zhang, F., & Zhang, J. (۲۰۱۶). Attacks to some verifiable multi-secret sharing schemes and two improved schemes. Information Sciences, ۳۲۹, ۵۲۴-۵۳۹.

[۲۰] Dehkordi, M. H., & Oraei, H. (۲۰۱۹). How to construct a verifiable multi-secret sharing scheme based on graded encoding schemes. IET Information Security.

[۲۱] Tentu, A. N., Venkaiah, V. C., & Prasad, V. K. (۲۰۱۸). CRT based multi-secret sharing schemes: revisited. International Journal of Security and Networks, ۱۳(۱), ۱-۹.

[۲۲] Zarepour-Ahmadabadi, J., Shiri-Ahmadabadi, M., Miri, A., & Latif, A. (۲۰۱۸). A new gradual secret sharing scheme with diverse access structure. Wireless Personal Communications, ۹۹(۳), ۱۳۲۹-۱۳۴۴.

[۲۳] Cohen, H. (۲۰۱۳). A course in computational algebraic number theory (۴th ed., vol. ۱۳۸). Berlin: Springer.

[۲۴] Feldman, P. (۱۹۸۷, October). A practical scheme for non-interactive verifiable secret sharing. In ۲۸th Annual Symposium on Foundations of Computer Science (sfcs ۱۹۸۷) (pp. ۴۲۷-۴۳۸). IEEE.