نشریه علمی "پدافند الکترونیکی و سایبری"

سال دوازدهم، شماره ۱، بهار ۱۴۰۳، ص۱۳-۲۶

شاپا الکترونیکی: ۸۹۷۹-۲۹۸۰ شاپا چاپی: ۴۳۴۷-۲۳۲۲

علمی – پژوهشی

بررسی برخی طرح‌های تسهیم راز مبتنی بر روش‌های درون‌یابی

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

۱- دانشجوی دکتری گروه ریاضی، واحد خرم آباد، دانشگاه آزاد اسلامی، خرم آباد، ایران۲- دانشیار، دانشکده و پژوهشکده فناوری اطلاعات و ارتباطات، دانشگاه جامع امام حسین (ع)، تهران،ایران ۳- استادیار گروه ریاضی، واحد خرم آباد، دانشگاه آزاد اسلامی، خرم‌آباد، ایران ۴- دانشیار، پژوهشکده علوم اطلاعات، پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)، تهران، ایران

(دریافت: ۱۴۰۲/۰۴/۰۵، بازنگری: ۱۴۰۲/۰۶/۲۱، پذیرش: ۱۴۰۲/۰۷/۱۹، انتشار: ۱۴۰۳/۰۳/۱۳)

2- DOR: https://dorl.net/dor/

چکیده

تسهیم راز یکی از مباحث جذاب علم رمزنگاری است که در امنیت اطلاعات کاربرد زیادی دارد. مسئله‌ی تسهیم راز به فرایندی گفته می‌شود که در آن یک یا چند راز بین تعدادی از شرکت‌کنندگان صلاحیت‌دار و یا با اعتبار متفاوت، به اشتراک گذاشته می‌شود. در زمان‌هایی که نیاز به بازیابی راز باشد، تعدادی از افراد که به آنها افراد مجاز می‌گوییم با تجمیع سهم‌های خود اقدام به بازیابی راز مورد نظر می‌نمایند. تا کنون انواع مختلفی از طرح‌های تسهیم راز مبتنی بر درون‌یابی پیشنهاد شده‌اند. در این طرح‌های تسهیم راز از درون‌یابی‌های مختلف، بسته به نیاز ساختاری طرح، استفاده شده است. در این مقاله چند طرح تسهیم راز مبتنی بر درون‌یابی مورد مطالعه و بررسی قرار می‌گیرند. سپس با تحلیل و مقایسه ویژگی‌های اساسی این طرح‌ها، مشاهده می‌شود که دو طرح تسهیم راز مبتنی بر درون‌یابی برکهف نسبت به سایر طرح‌های بررسی شده دارای کارایی بهتری هستند.

کلیدواژه‌ها: رمزنگاری، طرح تسهیم راز، تسهیم راز آستانه‌ای، درون‌یابی لاگرانژ، درون‌یابی برکهف

۱-مقدمه

در سال ۱۹۷۹ برای اولین بار مفهوم طرح تسهیم راز با استفاده از درون‌یابی لاگرانژ توسط شمیر[۱] معرفی گردید [۱]. در یک طرح تسهیم راز، یک تسهیم‌کننده مقدار یک راز را به‌گونه‌ای مابین مجموعه‌ای از شرکت‌کنندگان توزیع می‌کند که در آینده شرکت‌کنندگان موجود در برخی زیرمجموعه‌های مشخص (با نام زیرمجموعه مجاز) بتوانند با استفاده از سهام خود، راز را بازسازی کنند و سایر زیرمجموعه‌های غیرمجاز نتوانند با استفاده از سهام خود اطلاعی درباره راز به‌دست آورند. مجموعه‌ی تمام زیرمجموعه‌های مجاز در یک طرح تسهیم راز را ساختار دسترسی آن طرح گویند. ساختار دسترسی طرح شمیر، آستانه‌ای است. ساختار دسترسی آستانه‌ای (t,n) پرکاربردترین نوع ساختار دسترسی طرح‌های تسهیم راز است که در آن هر زیرمجموعه‌ای شامل حداقل t شرکت‌کننده، مجموعه‌ای مجاز می‌باشد. بیشتر کارهای انجام گرفته در زمینه رمزنگاری توزیع شده مختص به سامانه‌های با ساختار دسترسی آستانه‌ای است که این سامانه‌ها را سامانه‌های رمزنگاری آستانه‌ای گویند. در یک سامانه رمزنگاری آستانه‌ای، تمام افراد دارای صلاحیت یکسان هستند و اگر تعداد افراد مایل به مشارکت در اجرای سامانه مورد نظر از مقدار آستانه‌ای بیشتر باشد، اجرای سامانه امکان‌پذیر خواهد بود. در دنیای واقعی، فرض صلاحیت یکسان برای شرکت‌کنندگان فرضی نامعقول است. به عنوان مثال، فرض کنید یک گروه تحقیقاتی از یک دانشگاه، متشکل از ۹ نفر شامل ۲ نفر از اعضای هیئت‌علمی دانشگاه، ۳ نفر از دانشجویان مقطع دکتری و ۴ نفر دیگر از دانشجویان مقطع کارشناسی ارشد می‌باشند که قرار است در مورد یکی از محورهای پژوهشی تصمیم‌گیری کنند. همچنین فرض کنید جلسه تصمیم‌گیری در خصوص تصویب محورهای پژوهشی با توجه به شیوع ویروس کرونا به صورت مجازی برگزار شود. با توجه به ساختار سلسله مراتبی موجود در این مثال، منطقی و منصفانه نیست که از یک سامانه امضای آستانه‌ای

[1] Shamir

* Corresponding Author E-mail: Amrghdri@ihu.ac.ir

معمولی (برای مثال (۹و۴)) استفاده شود و برای همه اعضای گروه صلاحیت یکسانی در نظر گرفته شود. ممکن است استفاده از این رویکرد باعث شود که برنامه‌ی مورد تایید ۴ دانشجوی کارشناسی ارشد عضو گروه، یک برنامه معتبر قلمداد شود در صورتی که به خاطر فقدان تجربه کافی تصمیم‌گیرندگان، شاید این برنامه به ضرر گروه تحقیقاتی باشد. با توجه به این مثال و عدم کارایی سامانه‌های رمزنگاری آستانه‌ای ساده در چنین موقعیت‌هایی، باید از سامانه‌های رمزنگاری توزیع‌شده با ساختارهای دسترسی کلی‌تر استفاده شود. طرح‌های رمزنگاری توزیع‌شده با ساختار دسترسی «آستانه‌ای سلسله‌مراتبی» یکی از انواع طرح‌هایی است که توزیع اجرای سامانه را مابین مجموعه‌ای از افراد با صلاحیت‌های متفاوت امکان‌پذیر می‌نماید. تسهیم راز آستانه‌ای سلسله‌مراتبی فصلی برای اولین بار در سال ۱۹۹۰ توسط سایمونز[۲] و بریکل[۳] [۲] مورد بررسی قرار گرفته است.

در سال ۲۰۰۹ تاسا[۴] [۳] با استفاده از درون‌یابی برکهف، یک طرح کارامد، ایده‌آل و کاملاً امن برای این ساختار دسترسی ارائه کرد. ایده استفاده شده در طرح تاسا به این صورت است که ضریب انتهایی یک چندجمله‌ای را به عنوان راز قرار داده و پس از محاسبه مشتق‌های این چندجمله‌ای از مرتبه‌های مناسب، به هر شرکت‌کننده مقدار یکی از این مشتقات (انتخاب مرتبه مناسب مشتق بر اساس سطحی که این شرکت‌کننده به آن تعلق دارد) در یک نقطه داده می‌شود. برای بازسازی راز، یک مجموعه مجاز با اعمال درون‌یابی برکهف روی سهام خود، مشتقی از چندجمله‌ای تسهیم‌شده را بازیابی کرده و ضریب انتهایی مورد استفاده در تسهیم راز را به عنوان راز بازسازی شده در نظر می‌گیرند.

یک طرح تسهیم راز ساده تنها قادر به تسهیم یک راز عددی در هر مرحله تسهیم می‌باشد [۲و۳]. اما، در بسیاری از کاربردها تسهیم همزمان چندین راز مورد نیاز است. اجرای مکرر یک طرح تسهیم راز معمولی برای تسهیم جداگانه هر یک از رازها راه‌حلی بدیهی، اما ناکارامد برای این مسأله است. در صورت استفاده از این رویکرد، هر کاربر به ازای هر راز یک سهم دریافت می‌کند و در نتیجه، در این حالت کاربران باید اطلاعات زیادی را به طور محرمانه نگهداری کنند. طرح‌های تسهیم راز چندگانه با هدف کاهش میزان سهم نهایی دریافتی هر کاربر ابداع شده‌اند.

مفهوم تسهیم چندراز برای اولین بار توسط هارن[۵] [۴] ارائه شده است. در این طرح، سهام شرکت‌کنندگان در طول زمان ثابت است. این مساله برای رازهای با طول عمر زیاد مناسب نیست چرا که در این حالت یک متخاصم سیار می‌تواند در طول زمان سهام متناظر با هر مجموعه مجاز را به دست آورده و راز را بازسازی کند. برای حل این مشکل، نیکوف[۶] و همکاران [۵] مفهوم تسهیم راز پیش‌نگر را معرفی کردند. در طرح‌های تسهیم راز پیش‌نگر، سهام شرکت‌کنندگان در بازه‌های زمانی مشخصی و بدون نیاز به حضور توزیع‌کننده به‌روزرسانی می‌شود. در نتیجه این عمل، تنها سهام شرکت‌کنندگان یک مجموعه مجاز در بازه زمانی مشابه برای بازسازی راز مورد نیاز است و متخاصم سیار از طول عمر زیاد راز بهره‌ای نمی‌برد.

در این طرح‌های معرفی‌شده، ارزش سهام شرکت‌کنندگان در طول زمان ثابت است. برای اختصاص سهامی با ارزش متفاوت به شرکت‌کنندگان، طرح‌های تسهیم راز چندبخشی قابل استفاده هستند [۶ و ۷]. با این حال، این طرح‌ها نیز در موقعیت‌هایی که صلاحیت شرکت‌کنندگان در طول زمان متغیر باشد، کاربردی نیستند. برای حل این مشکل، نجومیان و همکاران مفهوم تسهیم راز اجتماعی را معرفی کردند [۸]. در یک طرح تسهیم راز اجتماعی، ارزش سهامی که شرکت‌کنندگان از راز دریافت می‌کنند وابسته به اعتبار و رفتار آن‌ها در طول زمان است. در این طرح‌ها، سهام شرکت‌کنندگان در بازه‌های زمانی مشخص، به‌روز شده و ارزش سهم هر شرکت‌کننده بر اساس رفتار و اعتبار او در زمان تغییر می‌کند.

در ادامه این مقاله در بخش ۲ به معرفی تسهیم راز آستانه‌ایی پرداخته شده و انواع مختلف طرح‌های تسهیم راز آستانه‌ای و چندبخشی در بخش‌های ۲ و ۳ معرفی شده‌اند. در بخش ۴ درونیابی‌های مورد استفاده معرفی و در بخش ۵ کارایی طرح‌های تسهیم راز مورد نظر تحلیل شده‌اند. همچنین در بخش ۶ طرح-های تسهیم راز بررسی شده با هم مقایسه شده‌اند. در نهایت در بخش ۷ نتیجه‌گیری بررسی طرح‌ها بیان شده است.

۲- مفاهیم اساسی طرح‌های تسهیم راز

در این بخش مفاهیم اساسی طرح‌های تسهیم راز را معرفی می-شوند. همان‌طوری که در بخش قبل ذکر شد، در یک طرح تسهیم راز، تعدادی سهام بین سهام‌داران توزیع می‌شود، به گونه‌ای که زیرمجموعه‌های خاصی از سهام‌داران بتوانند با به اشتراک گذاشتن سهم‌های خود به راز برسند. این زیرمجموعه‌های خاص را زیرمجموعه‌های مجاز می‌نامیم. طرح-های تسهیم راز آستانه‌ای و بلک‌لی به شرح ذیل معرفی می‌گردند.

۲-۱- طرح تسهیم راز آستانه‌ای

[2] Simmon
[3] Brickel
[4] Tasa
[5] Haren
[6] Nikov

همان‌طوری که در بخش قبل ذکر شد، در یک طرح تسهیم راز، تعدادی سهم بین سهام‌داران توزیع می‌شود. به گونه‌ای که زیرمجموعه‌های خاصی از سهام‌داران بتوانند با به اشتراک گذاشتن سهم‌های خود به راز برسند. این زیرمجموعه‌های خاص را زیرمجموعه‌های مجاز می‌نامیم. تعداد اعضای همه زیرمجموعه‌های مجاز می‌توانند یکسان یا متفاوت باشند. اگر n تعداد کل سهام‌داران و تعداد اعضای تمام زیرمجموعه‌های مجاز، یکسان و برابر با عدد ثابت t باشد، طرح تسهیم راز را آستانه‌ای[7] (t,n) می‌گوییم. به عبارت دیگر در یک طرح تسهیم راز آستانه‌ای (t,n) ، هر t سهام‌دار می‌توانند با به اشتراک گذاشتن سهم‌های خود به راز دست یابند ولی هیچ $t-1$ سهام‌دار یا کمتر قادر به انجام این کار نخواهند بود. از مهم‌ترین طرح‌های تسهیم راز آستانه‌ای ارائه شده می‌توان به طرح شمیر[8] [۹] و طرح بلکلی[9] [۲] اشاره کرد. طرح بلکلی از روش هندسی و طرح شمیر از روش درون‌یابی چندجمله‌ای استفاده می‌کند. در این بخش با توجه به موضوع مقاله که در مورد درون‌یابی ها است، ابتدا به معرفی اجمالی روش بلکلی پرداخته، سپس روش شمیر را مورد بررسی بیشتر قرار خواهیم داد.

۲-۲- طرح تسهیم راز بلکلی

ایده اصلی طرح تسهیم راز بلکلی بر اساس این واقعیت هندسی است که در یک فضای t بُعدی، تقاطع هر t ابرصفحه $t-1$ بُعدی و دوبه‌دو ناموازی، یک نقطه را به طور یکتا مشخص می‌نمایند. در این طرح، نقطه‌ای در فضای t بُعدی به عنوان راز فرض می‌شود. سپس n ابرصفحه متمایز و دوبه‌دو ناموازی $t-1$ بُعدی را به نحوی انتخاب می‌کنند که محل تقاطع آن‌ها نقطه راز باشد. هر ابرصفحه را به عنوان سهم به یک سهام‌دار می‌سپارند. در این صورت هر t سهام‌دار با قطع دادن ابرصفحه-های خود، به نقطه راز و در نتیجه به مقدار راز دست می‌یابند. از طرف دیگر، به ازای هر $t-1$ نفر یا کمتر، بی‌نهایت نقطه تقاطع وجود دارد و راز مخفی می‌ماند. لذا هر t نفر از n نفر سهام‌دار قادر به بازیابی راز خواهند بود ولی هیچ $t-1$ نفر یا کمتر نمی‌توانند به راز دست یابند.

۲-۳- طرح تسهیم راز شمیر

این طرح از نوع آستانه‌ای و بر اساس درون‌یابی لاگرانژ بوده و شامل دو پروتکل تسهیم راز و بازسازی راز می‌باشد که نحوه عملکرد آنها در جدول شماره ۲-۱ در زیر بیان شده است. البته قابل ذکر است که در طرح‌های تسهیم راز از چندجمله‌ای‌ها در حساب پیمانه‌ای استفاده می‌شود.

جدول ۲-۱: مراحل طرح تسهیم راز شمیر [۹]

پروتکل تسهیم: فرض کنید $GF(q)$ میدانی از مرتبه عدد اول q می‌باشد، توزیع‌کننده برای توزیع راز $S \in GF(q)$ به صورت زیر عمل می‌کند:

۱- ابتدا چندجمله‌ای $f(x)=S+a_1x+a_2x^2+\ldots+a_{t-1}x^{t-1}$ را روی میدان $GF(q)$ با مقادیر تصادفی $\{a_i\}_{i=1}^{t-1}$ تولید می‌کند.

۲- اگر U مجموعه شرکت کنندگان باشد. توزیع‌کننده، سهم متناظر با هر شرکت‌کننده $P_i \epsilon U$ را به صورت $sh_i = f(ID_i)$ در میدان متناهی $GF(q)$ تولید می‌کند که ID_i شناسه اختصاص‌یافته به P_i است.

پروتکل بازسازی: فرض کنید $Autsub=\{P_{\alpha_1},P_{\alpha_2},\ldots,P_{\alpha_t}\}$ یک زیرمجموعه‌ی مجاز از شرکت کنندگان باشد. در این صورت یک شخص معتمد با در اختیار داشتن سهام متناظر با اعضای $Autsub$، راز را به صورت زیر بازسازی می‌کند:

۱- مسأله درون‌یابی لاگرانژ را با ورودی زوج‌های $\{(ID_{\alpha_i}, sh_{\alpha_i})\}_{i=1}^{t}$ حل کرده و چندجمله‌ای $f(.)$ را بازسازی می‌کند.

۲- راز را به عنوان جمله ثابت این چندجمله‌ای در نظر می‌گیرد.

۲-۴- طرح تسهیم راز چندبخشی

در طرح‌های تسهیم راز آستانه‌ای فرض بر این است که صلاحیت شرکت‌کنندگان با یکدیگر برابر بوده و در نتیجه به آن‌ها سهم‌هایی با ارزش یکسان اختصاص داده می‌شود. در محیط واقعی، در اکثر مواقع این فرض برقرار نیست و شرکت‌کنندگان بر اساس موقعیت خود در اجتماع و میزان اعتماد به آن‌ها دارای صلاحیت‌های متفاوتی هستند. در نتیجه، وجود طرح‌های تسهیم رازی که قادر به در نظر گرفتن صلاحیت‌های متفاوت افراد باشند، ضروری است. تسهیم راز چندبخشی[10]، مفهومی است که این هدف را برآورده می‌نماید و ساختار دسترسی در نظر گرفته شده در این گونه طرح‌های تسهیم راز تعمیم‌های طبیعی ساختار دسترسی آستانه‌ای هستند که در نظر گرفتن صلاحیت‌های متفاوت را به روش‌های مختلف ممکن می‌سازند. در این طرح‌ها، فرض بر این است که مجموعه شرکت‌کنندگان U به $m+1$ زیرمجموعه مجزای $U_0,U_1,\ldots,U_m$ تقسیم شده بنحوی که شرکت‌کنندگان موجود در یک زیرمجموعه دارای صلاحیت‌های یکسانی هستند و شرکت‌کنندگانی که در سایر زیرمجموعه‌های

[7] Threshold secret sharing
[8] Shamir Scheme
[9] Blakley
[10] Multipartite secret sharing

مختلف قرار دارند دارای صلاحیت‌های متفاوت (از پیش تعیین شده) هستند. از جمله طرح‌های تسهیم راز چندبخشی مطرح، می‌توان به موارد زیر اشاره کرد:

تسهیم راز آستانه‌ای سلسله‌مراتبی[11]: فرض کنیم Γ یک ساختار دسترسی باشد. شرکت کننده P را در این ساختار دسترسی به صورت سلسله‌مراتبی بالا دستی عضوی مانند P' گویند هرگاه برای هر مجموعه دلخواه $A \subseteq U \setminus \{P,P'\}$ داشته باشیم: اگر $A \cup \{P\} \in \Gamma$، آن‌گاه $A \cup \{P'\} \in \Gamma$. حال با توجه به این تعریف، یک ساختار دسترسی را سلسله‌مراتبی گویند هرگاه هر دو شرکت‌کننده دلخواه در آن به صورت سلسله‌مراتبی با یکدیگر وابسته باشند [۱۰]. طرح‌های تسهیم راز آستانه‌ای وزن‌دار نمونه‌های خاصی از طرح‌های تسهیم راز سلسله‌مراتبی هستند. در ادامه خانواده مهمی از این ساختارها که طرح‌هایی کارا برای آن ارائه شده را معرفی می‌کنیم.

تسهیم راز آستانه‌ای سلسله‌مراتبی فصلی[12]: ساختار دسترسی یک طرح تسهیم راز آستانه‌ای سلسله‌مراتبی فصلی با یک دنباله صعودی از مقادیر آستانه‌ای $(\langle t_0,t_1\ldots,t_m\rangle)$ مشخص می‌شود. در این طرح‌ها یک مجموعه دلخواه (A) از شرکت‌کنندگان، مجاز به بازسازی راز است اگر $(0 \le j \le m-1)$ وجود داشته باشد که $\left|A \cap \left(\cup_{i=0}^{j} U_{m-i}\right)\right| \ge t_{m-j}$. تسهیم راز آستانه‌ای سلسله‌مراتبی فصلی برای اولین بار توسط سایمونز[13] و بریکل[14] [۱۱] مورد بررسی قرار گرفته است. سایمونز با استفاده از ساختارهای هندسی[15] استفاده شده در طرح تسهیم راز بلک‌لی [۲]، یک طرح تسهیم راز آستانه‌ای سلسله‌مراتبی فصلی ارائه کرده است. طرح ارائه شده توسط سایمونز ایده‌آل نیست اما قادر به تسهیم هم‌زمان چندین راز می‌باشد. بریکل [۱۲] دو طرح ایده‌آل برای این نوع ساختار دسترسی ارائه کرده است اما، هر دو طرح ارائه شده از نقطه نظر کارایی غیرعملی هستند. تاسا [۱۳] از درون‌یابی برکهف استفاده کرده و یک طرح کارا، ایده‌آل و کاملاً امن برای این ساختار دسترسی ارائه کرده است. ایده استفاده شده در طرح تاسا به این صورت است که راز را به عنوان ضریب انتهایی یک چندجمله‌ای قرار داده و پس از محاسبه مشتقات این چندجمله‌ای از مرتبه‌های مناسب، به هر شرکت‌کننده مقدار یکی از این مشتقات (انتخاب مرتبه مشتق مناسب بر اساس سطحی است که این شرکت‌کننده به آن تعلق دارد) در یک نقطه اختصاص داده می‌شود. برای بازسازی راز، یک مجموعه مجاز با انجام درون‌یابی برکهف روی سهام خود، مشتقی از چندجمله‌ای تسهیم شده را بازیابی کرده و ضریب انتهایی استفاده شده در تسهیم راز را به عنوان راز بازسازی شده در نظر می‌گیرند. با توجه به استفاده از طرح تسهیم راز آستانه‌ای سلسله‌مراتبی فصلی تاسا به عنوان مؤلفه اصلی طرح تسهیم چندراز اجتماعی، جزئیات این طرح در جدول ۳-۱ آورده شده است.

جدول ۳-۱: طرح تسهیم راز آستانه‌ای سلسله‌مراتبی فصلی تاسا [۱۴]

الف) پروتکل تسهیم:

فرض کنید n تعداد شرکت‌کنندگان و $\langle t_0,t_1\ldots,t_m\rangle$ دنباله‌ی مقادیر آستانه‌ای باشد. توزیع کننده برای تسهیم راز $S \in GF(q)$، به صورت زیر عمل می‌کند:

۱. چندجمله‌ای $f(x)=a_0+a_1x+a_2x^2+\ldots+a_{t-2}x^{t-2}+S\,x^{t_1-1}$ را روی میدان $GF(q)$ تولید می‌کند که $\{a_i\}_{i=0}^{t_1-2}$ مقادیری تصادفی هستند.

۲. برای هر شرکت‌کننده $P_i \in U$، مقدار $sh_i = f^{(t_1-t_j)}(i)$ را به عنوان سهم این شرکت‌کننده از راز محاسبه کرده و از طریق یک کانال امن برای او می‌فرستد که $f^{(t_1-t_j)}(.)$ مشتق مرتبه (t_1-t_j)-ام چندجمله‌ای $f(.)$ است و j نمایشگر شماره سطحی است که P_i به آن تعلق دارد.

ب) پروتکل بازسازی:

فرض کنید $Autsub=\{P_{\alpha_0},P_{\alpha_1},\ldots,P_{\alpha_{t_j-1}}\}$ یک مجموعه مجاز از شرکت‌کنندگان باشند. با استفاده از سهام متناظر با اعضای مجموعه $Autsub$ ، یک شخص مورد اعتماد می‌تواند راز را به صورت زیر بازسازی کند:

۱. درون‌یابی برکهف را روی سهام فراهم شده اعمال کرده و مشتق مرتبه (t_1-t_j)- ام چندجمله‌ای $f(.)$ را بازسازی می‌کند(یعنی $f^{(t_1-t_j)}(.)$).

۲. فرض کنیم S' آخرین ضریب $f^{(t_1-t_j)}(.)$ باشد. راز را به‌صورت $S=\frac{(t_j-1)!}{(t_1-1)!}S'$ بازسازی می‌کند.

۴- درونیابی‌های مورد استفاده

[11] Hierarchical threshold secret sharing
[12] Disjunctive hierarchical threshold secret sharing
[13] Simmons
[14] Brickell
[15] Geometric constructions

درون‌یابی لاگرانژ[۱۶] : یکی از روش‌های تعیین یک چندجمله‌ای حداکثر از درجه n که در معادله

$$P(x_i)=f_i \quad i=0,...,n \qquad (۱-۴)$$

صدق کند روش لاگرانژ است. در این روش فرض می‌کنیم هر یک از $L_n(x), ..., L_1(x), L_0(x)$ ، یک چندجمله‌ای درجه n باشند و داشته باشیم

(۲-۴)

$$P(x)=L_0(x)f_0+L_1(x)f_1+...+L_j(x)f_j+...+L_n(x)f_n$$

و سعی می‌کنیم $L_j(x)$ها را چنان تعیین کنیم که معادله (۴-۱) برقرار باشد. برای این منظور می‌گوییم به ازای $i=0,1,...,n$ باید داشته باشیم:

$$P(x_i)=L_0(x_i)f_0+...+L_j(x_i)f_j+...+L_n(x_i)f_n$$

لذا، کافی است (و در صورت مستقل بودن $L_i(x)$ ها از یکدیگر لازم است $i \neq j$) داشته باشیم:

$$\begin{cases} L_j(x_i)=0 \\ L_j(x_j)=1 \end{cases} \qquad (۳-۴)$$

اما، تابع زیر

(۴-۴)

$$(x-x_0)...(x-x_{j-1})(x-x_{j+1})...(x-x_n)$$

به ازای $x_n, ..., x_{j+1}, x_{j-1}, ..., x_1, x_0$ صفر است، یعنی به ازای x_iهایی که $i \neq j$، کافی است کاری

کنیم که مقدار این تابع به ازای x_j یک شود و این کار با تقسیم تابع مندرج در (۴-۳) بر عدد

$$(x_j-x_0)(x_j-x_1)...(x_j-x_{j-1})(x_j-x_{j+1})...(x_j-x_n)$$

امکان‌پذیر است. به عبارت دیگر داریم:

(۵-۴)

$$L_j(x)=\frac{(x-x_0)(x-x_1)...(x-x_{j-1})(x-x_{j+1})...(x-x_n)}{(x_j-x_0)(x_j-x_1)...(x_j-x_{j-1})(x_j-x_{j+1})...(x_j-x_n)}$$

این چندجمله‌ای‌های درجه n که به وسیله (۴-۵) بیان شده‌اند به چندجمله‌ای‌های لاگرانژ معروف هستند.

درون‌یابی هرمیت[۱۷]:

در این قسمت یک نوع درون‌یابی را معرفی می‌کنیم که با درون‌یابی لاگرانژ متفاوت است. در این درونیاب فرض می‌کنیم که در نقاط درون‌یابی، نه تنها خود تابع اصلی با تابع درونیاب هم عرض است، بلکه مشتقات متناهی تابع اصلی با مشتقات متناهی تابع درونیاب نیز هم عرض است. بدیهی است که داشتن چنین ویژگی، باعث همواری و دقیق بودن درونیاب خواهد بود.

فرض کنید x_i به ازای $i=0,1,...,m$ اعداد حقیقی باشند که $x_0<x_1<....<x_m$. نقاط درون‌یابی را به صورت زیر معرفی می‌کنیم:

(۶-۴)

$$\left(x_i, y_i^{(k)}\right) \quad , \quad i=0,1,...,m \quad , \quad k=0,1,...n_i-1$$

که در آن به ازای هر i، n_i عددی طبیعی است. چندجمله‌ای حداکثر از درجه n، P را چندجمله‌ای درونیاب هرمیت گوییم، هرگاه در شرایط زیر صدق کند:

(۷-۴)

$$P^{(k)}(x_i)=y_i^{(k)}, \qquad i=0,1,...,m, \qquad k=0,1,...,n_i-1$$

که در آن:

$$\sum_{i=0}^{m} n_i = n+1 \qquad (۸-۴)$$

که (۴-۷) را شرایط درون‌یابی گوییم.

درون‌یابی برکهف:

برکهف مسئله درون‌یابی خود را به‌صورت زیر مطرح کرد: برای داده‌های $C_{i,j}$ و x_i چندجمله‌ای درونیاب $P_n(x)$ از درجه حداکثر n را پیدا کنید که در شرط

(۹-۴)

$$P_n^{(j)}(x_i)=C_{i,j} \qquad (\text{معادله } n+1)$$

صدق کند.

در این بخش برخی از تعاریف و قضایای مرتبط با درون‌یابی برکهف را بیان خواهیم کرد.

تعریف ۴-۱-۱ درون‌یابی برکهف[۱۸]: فرض کنید:

[17] Lagrange interpolation

[18] Hermit

[19] Birkhoff interpolation

$X=\{x_1,x_2,....,x_k : x_1<x_2<....<x_k\}$ مجموعه‌ای از اعداد حقیقی باشد.

$E=(e_{i,j})\quad 1\le i\le k, 0\le j\le l$ ماتریسی با درایه‌های دودویی باشد که آخرین ستون آن مخالف صفر باشد $I(E)=\{(i,j):e_{i,j}=1\}$

$C=\{c_{i,j}:(i,j)\in I(E)\}$ مجموعه‌ای شامل N عدد حقیقی باشد.

مساله درون‌یابی برکهف متناظر با سه‌تایی $\langle X,E,C\rangle$ مساله یافتن چندجمله‌ای $P(x)\in R_{N-1}[x]$ است که در معادله زیر صدق کند:

(۱۰-۴)
$$P^{(j)}(x_i)=c_{i,j},(i,j)\in I(E).$$

در رابطه فوق $P^{(j)}(.)$ مشتق مرتبه (j)-ام $P(x)$ و $R_{N-1}[x]$ مجموعه تمام چندجمله‌ای‌های ممکن از درجه حداکثر $N-1$ است. ماتریس E ماتریس درون‌یابی نامیده می‌شود [۱۴].

برعکس مسائل درون‌یابی‌های لاگرانژ و هرمیت که بدون قید و شرط جواب یکتا دارند، مساله درون‌یابی برکهف ممکن است جواب یکتا نداشته باشند. در ادامه شرایط لازم و کافی برای یکتایی جواب مساله درون‌یابی برکهف را ذکر می‌کنیم.

۴-۱-۲ شرط پولیا[۱۹]: فرض کنیم مساله درون‌یابی برکهف متناظر با سه‌تایی $\langle X,E,C\rangle$ دارای جواب یکتا باشد. در این صورت، درایه‌های ماتریس درون‌یابی E در شرط پولیا صدق می‌کنند:

(۱۱-۴)
$$\forall t\ (0\le t\le l):\sum_{j=0}^{t}\sum_{i=1}^{k}e_{i,j}\ge(t+1)$$

در رابطه فوق l بزرگترین مرتبه مشتق موجود در داده‌های مساله و k تعداد نقاط درون‌یابی است.

شرط ۴-۱-۲ بیانگر یک شرط لازم برای یکتایی جواب مساله درون‌یابی برکهف است. برای به‌دست آوردن شروط کافی برای یکتایی جواب این مساله، در ابتدا تعریف زیر را در نظر بگیرید:

تعریف ۴-۱-۳: یک ۱-دنباله[۲۰] در یک ماتریس درون‌یابی E به محل حضور بیشترین ۱های متوالی در یک سطر از ماتریس E گفته می‌شود. به عبارت دیگر، یک ۱-دنباله، سه‌تایی به شکل (i,j_0,j_1) است $(0\le j_0\le j_1\le l\ ,\ 1\le i\le k)$؛ که به ازای هر $j_0\le j\le j_1$ داشته باشیم $e_{i,j}=1$ و (برای درستی تعریف، فرض می‌کنیم $e_{i,-1}=e_{i,l+1}=0$). یک ۱-دنباله (i,j_0,j_1) را پشتیبانی‌شده[۲۱] گوییم هرگاه اندیس‌های nw و sw $(j_{nw},j_{sw}<j_0,i_{nw}<i<i_{sw})$ موجود باشند که $e_{i_{nw},j_{nw}}=e_{i_{sw},j_{sw}}=1$. [۱۴].

قضیه زیر با استفاده از تعریف بالا شرط کافی برای یکتایی جواب مساله درون‌یابی برکهف را بیان می‌کند:

قضیه ۴-۱-۴: مساله درون‌یابی بیان شده در تعریف ۴-۱-۱ دارای جواب یکتا است هرگاه ماتریس درون‌یابی E در شرط پولیا صدق کند و شامل ۱-دنباله پشتیبانی شده‌ای با طول فرد نباشد [۱۵].

قضیه فوق یکتایی جواب مساله درون‌یابی برکهف در زمان انجام محاسبات روی مجموعه اعداد حقیقی را بیان می‌کند. در این مقاله درون‌یابی برکهف را در میدان‌های متناهی[۲۲] استفاده می‌کنیم. از آن‌جایی که تقسیم بر صفر در میدان‌های متناهی با تقسیم بر صفر در میدان اعداد حقیقی متفاوت است (در یک میدان متناهی هر مضربی از اندازه میدان با صفر برابر است)، ممکن است که یک مساله درون‌یابی که در میدان اعداد حقیقی جوابی یکتا دارد، در میدان‌های متناهی این ویژگی را از دست بدهد. قضیه زیر شرایط کافی برای یکتایی جواب مساله درون‌یابی برکهف در میدان‌های متناهی را بیان می‌کند [۱۵].

قضیه ۴-۱-۵ : مساله درون‌یابی برکهف بیان شده در تعریف ۴-۱-۱ روی میدان متناهی $GF(q)$ دارای جواب یکتا است اگر داده‌های مسئله علاوه بر صدق کردن در شرایط بیان شده در قضیه ۴-۱-۴ ، در شرط زیر نیز صدق کنند:

(۱۲-۴)
$$q>2^{-l+2}.(l-1)^{(l-1)/2}.(l-1)!\ .\ x_k^{(l-1)(l-2)/2}$$

که l بزرگترین مرتبه مشتق موجود در داده‌های مساله است.

در ادامه نحوه محاسبه جواب یک مساله درون‌یابی برکهف را بیان خواهیم کرد. فرض کنید $\varphi=\{g_0, g_1, \dots, g_{N-1}\}$ مجموعه‌ای از توابع حقیقی-مقدار $N-1$ بار مشتق‌پذیر و مستقل خطی باشند. همچنین فرض کنید $I'(E)=\{\alpha_i : i=1,\cdots,N-1\}$ برداری باشد که از

[20] Polya's condition
[21] 1-sequence
[22] Supported 1-sequence
[23] Finite field

مرتب‌سازی $I(E)$ به صورت لغت‌نامه‌ای به‌دست آمده باشد. (در $I'(E)$، زوج (i,k) قبل از زوج (i',k')می‌آید اگر و تنها اگر $i<i'$ یا $i=i'$ و $k<k'$). مقادیر $\alpha_i(1)$ و $\alpha_i(2)$ را به عنوان مولفه‌های اول و دوم $\alpha_i \in I'(E)$ و $C'=\{c'_i : i = 1,\cdots, N\text{-}1\}$ را به عنوان بردار حاصل از مرتب‌سازی لغت‌نامه‌ای C در نظر بگیرید(مرتب‌سازی بر اساس اندیس عناصر موجود در C انجام می‌گیرد).

حال، با استفاده از بردارهای حاصل از مرتب‌سازی E, X و φ می‌توانیم جواب مساله درون‌یابی برکهف را به صورت زیر بدست آوریم:

(۴-۱۳)

$$P(x) = \sum_{j=0}^{N-1} \frac{|A(E, X, \varphi_j)|}{|A(E, X, \varphi)|} g_j(x),$$

که:

(۴-۱۴)

$$A(E, X, \varphi) = \begin{bmatrix} g_0^{(a_0(2))}(x_{a_0(1)}) & g_1^{(a_0(2))}(x_{a_0(1)}) & \cdots & g_{N-1}^{(a_0(2))}(x_{a_0(1)}) \\ g_0^{(a_1(2))}(x_{a_1(1)}) & g_1^{(a_1(2))}(x_{a_1(1)}) & \cdots & g_{N-1}^{(a_1(2))}(x_{a_1(1)}) \\ \vdots & \vdots & \ddots & \vdots \\ g_0^{(a_{N-1}(2))}(x_{a_{N-1}(1)}) & g_1^{(a_{N-1}(2))}(x_{a_{N-1}(1)}) & \cdots & g_{N-1}^{(a_{N-1}(2))}(x_{a_{N-1}(1)}) \end{bmatrix}$$

$|.|$عملگر محاسبه دترمینان است و $A(E, X, \varphi_j)$ را می‌توان با جایگزینی $(j+1)$-امین ستون ماتریس (۴-۱۴) با C' به‌دست آورد.

در صورت بازنویسی معادله (۴-۱۳) با استفاده از باز کردن فرمول محاسبه دترمینان ماتریس $\left|A\left(E, X, \varphi_j\right)\right|$ حول $(j+1)$-امین ستون آن، فرمول زیر برای محاسبه جواب مساله درون‌یابی برکهف(معادله (۴-۱۰)) به‌دست می‌آید:

(۴-۱۵)

$$P(x) = \sum_{j=0}^{N-1}\sum_{i=0}^{N-1} (-1)^{(i+j)} c'_{i+1} \frac{|A_i(E, X, \varphi_j)|}{|A(E, X, \varphi)|} g_j(x)$$

که $A_i\left(E, X, \varphi_j\right)$ ماتریس حاصل از حذف $(i+1)$-امین سطر و $(j+1)$-امین ستون ماتریس $A\left(E, X, \varphi_j\right)$ است.

با توجه به معادله (۴-۱۵) ، به سادگی دیده می‌شود که:

(۴-۱۶)

$$P(0) = \sum_{j=0}^{N-1}\sum_{i=0}^{N-1} (-1)^{(i+j)} c'_{i+1} \frac{|A_i(E, X, \varphi_j)|}{|A(E, X, \varphi)|} g_j(0)$$

به‌طور مشخص، فرض کنید که

$$\varphi = \left\{g_0(x)=1, g_1(x)=x, \ldots, g_{N-1}(x)=x^{N-1}\right\},$$

در نتیجه داریم که $g_0(0)=1$ و $g_j(0)=0$ برای $1 \le j \le N-1$. بنابراین، در مساله درون‌یابی برکهف مورد نظر $P(0)$ را می‌توانیم به صورت زیر محاسبه کنیم:

(۴-۱۷)

$$P(0) = \sum_{i=0}^{N-1} (-1)^{(i)} c'_{i+1} \frac{|A_i(E, X, \varphi_0)|}{|A(E, X, \varphi)|} = \sum_{i=0}^{N-1} c'_{i+1} \left[(-1)^{(i)} \frac{|A_i(E, X, \varphi_0)|}{|A(E, X, \varphi)|} \right]$$

در ادامه به معرفی ضرایب درون‌یابی برکهف خواهیم پرداخت.

تعریف ۴-۱-۶ ضرایب درون‌یابی برکهف: همانند شرایط موجود در یک مساله درون‌یابی لاگرانژ، اگر یک مساله درون‌یابی برکهف حل‌پذیر باشد، خواهیم داشت:

$$\left[c'_1,\ldots,c'_N\right]^T = A\left(E,X,\varphi\right)\left[a_0,\ldots,a_{N-1}\right]^T$$

با توجه به وارون‌پذیری ماتریس $A\left(E,X,\varphi\right)$ (که توسط حل‌پذیری مساله درون‌یابی برکهف مورد نظر به‌دست آمده است)، داریم:

$$\left[a_0,\ldots,a_{N-1}\right]^T = A\left(E,X,\varphi\right)^{-1}\left[c'_1,\ldots,c'_N\right]^T$$

درایه‌های ماتریس $A\left(E,X,\varphi\right)^{-1}$ضرایب درون‌یابی برکهف متناظر با مجموعه X و ماتریس درون‌یابی E نامیده می‌شوند.

مثال ۴-۱-۹ : مساله درون‌یابی برکهف متناظر با داده‌های زیر را در نظر بگیرید:

$$X = \{1,2,3,4\},$$

$$C = C' = \{c_1=10, c_2=28, c_3=24, c_4=6\},$$

$$E = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

•

با توجه به داده‌های مساله داریم $I'(E)=\{\alpha_1=(1,1), \alpha_2=(2,1), \alpha_3=(3,3), \alpha_4=(4,4)\}$ و $N=3$. به راحتی می‌توان بررسی کرد که مساله داده شده در

شرایط قضیه ۴-۱-۵ صدق می‌کند و در نتیجه این مساله دارای جواب یکتا است. فرض کنید $\varphi=\{1,x,x^2,x^3\}$. با استفاده از داده‌های فوق خواهیم داشت:

$$|A(E,X,\varphi)|=\begin{vmatrix} g_0^{(1)}(x_1) & g_1^{(1)}(x_1) & g_2^{(1)}(x_1) & g_3^{(1)}(x_1)\\ g_0^{(1)}(x_2) & g_1^{(1)}(x_2) & g_2^{(1)}(x_2) & g_3^{(1)}(x_2)\\ g_0^{(3)}(x_3) & g_1^{(3)}(x_3) & g_2^{(3)}(x_3) & g_3^{(3)}(x_3)\\ g_0^{(4)}(x_4) & g_1^{(4)}(x_4) & g_2^{(4)}(x_4) & g_3^{(4)}(x_4) \end{vmatrix}=\begin{vmatrix} 1 & 1 & 1 & 1\\ 1 & 2 & 4 & 8\\ 0 & 0 & 2 & 18\\ 0 & 0 & 0 & 6 \end{vmatrix}=12$$

حال با جایگزینی C' در $(j+1)$-امین ستون ماتریس فوق، متناظر با آن به‌دست خواهد آمد و خواهیم داشت:

$$,|A(E,X,\varphi_0)|=\begin{vmatrix} 10 & 1 & 1 & 1\\ 28 & 2 & 4 & 8\\ 24 & 0 & 2 & 18\\ 6 & 0 & 0 & 6 \end{vmatrix}=48$$

$$,|A(E,X,\varphi_1)|=\begin{vmatrix} 1 & 10 & 1 & 1\\ 1 & 28 & 4 & 8\\ 0 & 24 & 2 & 18\\ 0 & 6 & 0 & 6 \end{vmatrix}=24$$

$$|A(E,X,\varphi_2)|=\begin{vmatrix} 1 & 1 & 10 & 1\\ 1 & 2 & 28 & 8\\ 0 & 0 & 24 & 18\\ 0 & 0 & 6 & 6 \end{vmatrix}=36$$

اکنون با استفاده از معادله (۴-۹)، جواب مساله درون‌یابی خواسته شده به صورت زیر محاسبه خواهد شد:

$$P(x)=\sum_{j=0}^{3}\frac{|A(E,X,\varphi_j)|}{|A(E,X,\varphi)|}g_j(x)=\frac{48(1)+24(x)+36(x^2)+12(x^3)}{12}$$

$$=4+2x+3x^2+x^3.$$

۵-تحلیل کارایی طرح‌های تسهیم راز

درون‌یابی توابع به‌وسیله چندجمله‌ای‌ها یکی از مباحث اساسی ریاضیات است. به نظر می‌رسد اولین کار در این زمینه در قرن هفدهم توسط نیوتن انجام شد. کمی بعد لاگرانژ فرمول نیوتن را گسترش داد. در سال ۱۸۷۸، هرمیت درونیاب معروف خود را ارائه داد. در سال ۱۹۰۶ برکهف اولین مقاله در زمینه درون‌یابی حفره‌ای[۲۳] یا درون‌یابی برکهف را ارائه داد. در این نوع درون‌یابی اطلاعاتی که از تابع اولیه در دست است شامل مقادیر تابع و مقادیر مشتقات مرتبه بالاتر تابع در برخی نقاط دیگر است که نظم و ترتیب خاصی ندارند. اگر به‌ازای هر i، مرتبه‌های مشتق j که $(j=0,1,2,...,j_i)$، در (۴-۹) دنباله‌ای باشد که شکستگی نداشته باشد، یعنی در تمام نقاط مذکور مشتق‌پذیر باشد و مشتق آن در همه این نقاط داده شده باشد، آنگاه نوع درونیابی که حاصل خواهد شد درونیاب هرمیت است. در حالت خاص وقتی که همه j_i ها صفر باشند، درونیاب لاگرانژ به‌دست می‌آید. این دنباله همیشه موجود و یکتاست و فرم صریح آن نیز در حالت کلی درست است. اما سوالی که مطرح می‌شود این است که اگر در مرتبه مشتقات، مثلا برای گره x_j ، به دنباله‌ای نامتوالی برخورد کنیم، (یعنی در بعضی از مراتب، مشتق وجود نداشته باشد و یا در اختیار ما نباشد) در این حالت آیا درون‌یابی هرمیت برای حل مسئله کارساز خواهد بود؟ جواب منفی است و برای حل این مسئله، برکهف، درون‌یابی جدیدی مطرح کرد که تا حدودی پاسخ‌گوی حل این مشکل می‌باشد. در برخی از مراجع درونیاب هرمیت را حالت خاصی از درونیاب برکهف در نظر می‌گیرند. اما اگر برخی از دنباله‌ها شکسته شوند، درونیاب برکهف را خواهیم داشت. تفاوت این دو درونیاب مثل تفاوت دو نظریه معادلات دیفرانسیل خطی و غیرخطی است [۱۶]. با توجه به مطالب فوق و مطالعه طرح‌های مختلف تسهیم راز ارائه شده در مقاله‌های [۱و ۱۷ و ۱۸] می‌توان گفت درون‌یابی لاگرانژ در طرح‌های تسهیم راز برای افراد دارای صلاحیت یکسان کاربرد دارد. در بسیاری از کاربردها، در نظر گرفتن صلاحیت یکسان برای تمام افراد، فرضی غیرمعقول است. همچنین ممکن است در موقعیت‌هایی نیاز باشد تا راز مابین شرکت‌کنندگان با سهامی با ارزش متفاوت در طول زمان تسهیم شود، در این صورت طرح‌های تسهیم راز معمولی از کارایی لازم برخوردار نیستند. برای برطرف شدن این مشکل طرح‌های مختلفی مانند طرح تسهیم راز اجتماعی ارائه شده است که در آن از درون‌یابی برکهف استفاده شده است. تسهیم راز اجتماعی امکان تسهیم یک راز مابین مجموعه‌ای از شرکت‌کنندگان را به‌گونه‌ای فراهم می‌کند که امکان تغییر ارزش سهام شرکت‌کنندگان در طول زمان وجود داشته باشد. با توجه به این مساله، از درون‌یابی برکهف و در حقیقت از مشتقات یک چندجمله‌ای استفاده شده است.

شاید این پرسش مطرح شود که آیا در طرح تسهیم راز اجتماعی می‌توان از درون‌یابی هرمیت که از برکهف ساده‌تر است استفاده نمود، که در پاسخ باید به این نکته اشاره کرد که اگر از درون‌یابی

[24] Lacunary Interpolution

هرمیت استفاده شود باید تمام مقادیر مشتق‌ها را به یک نفر خاص اختصاص دهیم و اگر قرار باشد مشتق‌ها را به افراد مختلف بدهیم ساختار دسترسی مسئله محدود می‌شود. یعنی اگر قرار باشد تا رازی را بازسازی کنیم، باید همه افراد در این کار مشارکت کنند تا راز بازسازی شود. مزیت دیگری که درون‌یابی برکهف نسبت به لاگرانژ دارد این است که با استفاده از درون‌یابی برکهف می‌توانیم به هر فرد سهام کمتری(در حقیقت تنها یک سهم) تخصیص دهیم. یعنی زمانی که از این درون‌یابی در طرح‌های تسهیم راز استفاده می‌شود، وجود مشتق مرتبه بالاتر در سهم فرد، نشان‌دهنده با ارزش‌تر بودن سهام فرد است. در حالی که اگر از درون‌یابی لاگرانژ استفاده شود باید برای افراد با صلاحیت بیشتر تعداد سهام بیشتر ارائه دهیم، که باعث کاهش کارایی طرح می‌شود.

۶- مقایسه طرح‌های تسهیم راز

نویسندگان این مقاله دو طرح در این زمینه با نام‌های طرح تسهیم چندراز پیش‌نگر با استفاده از درون‌یابی لاگرانژ و قضیه باقی‌مانده چینی [۱۹] در سال ۲۰۲۱ و طرح تسهیم چندراز اجتماعی با استفاده از درون‌یابی برکهف و قضیه باقی‌مانده چینی [۲۰] در سال ۲۰۲۲ به چاپ رسانده‌اند. در ادامه این بخش طرح‌های پیشنهادی فوق با سه طرح تسهیم راز دیگر از نظر کارایی، پیچیدگی محاسباتی و نوع درون‌یابی‌های مورد استفاده در آن با هم مقایسه شده‌اند. نتایج مقایسه طرح‌های تسهیم راز در جدول ۶-۱ آورده شده است. مشاهده می‌شود که دو طرح ارائه شده در [۱۹] و [۲۰] علاوه بر این‌که از اندازه سهام کوچکی برخوردارند و قابلیت تسهیم همزمان چند راز را پشتیبانی می‌کنند، لذا دارای قابلیت تسهیم تدریجی و ترتیبی رازها (تدریجی بودن یعنی رازها به صورت یکجا بازیابی نشوند و ترتیبی بودن یعنی رازها طبق ترتیب خاصی بازیابی می‌شوند) نیز هستند ولی سه طرح دیگر این قابلیت‌ها را ندارند. به طور مثال طرح پاک‌نیت و همکاران [۲۲] که از درون‌یابی لاگرانژ برای طرح خود استفاده نموده است، با وجود اندازه سهام به مراتب بزرگتر از طرح‌های [۱۹] و[۲۰]، قابلیت تسهیم تدریجی و ترتیبی رازها را ندارد. وجود ستاره (*) در دو سطر اول ستون ۶ جدول ۶-۱ به این خاطر می‌باشد که طرح‌های مذکور قابلیت تسهیم تنها یک راز را دارند و لذا به طور طبیعی قابلیت تسهیم ترتیبی و تدریجی رازها برای آن‌ها معنی ندارد.

جدول۶-۱: مقایسه چند طرح تسهیم راز از لحاظ کارایی و سایر ویژگی‌ها

طرح	نوع درون‌یا بی به کار رفته	پیچیدگی محاسباتی درون‌یابی	اندازه سهام	قابلیت تسهیم چند راز	قابلیت تسهیم تدریجی و ترتیبی رازها
طرح نجومیان [۸]	لاگرانژ	$o(t\log t)$	$t\lvert q\rvert$	خیر	*
طرح اسلامی و همکاران [۲۱]	برکهف	$o(t^{3.373})$	$\lvert q\rvert$	خیر	*
طرح پاک‌نیت و همکاران [۲۲]	لاگرانژ	$o(t\log t)$	$t\lvert q\rvert$	بلی	خیر
طرح تسهیم چند راز پیش‌نگر [۱۹]	لاگرانژ	$o(t\log t)$	$2\lvert q\rvert$	بلی	بلی
طرح تسهیم چند راز اجتماعی [۲۰]	برکهف	$o(t^{3.373})$	$2\lvert q\rvert$	بلی	بلی

۷- نتیجه‌گیری

در این تحقیق پنج طرح تسهیم چندراز بر اساس درون‌یابی لاگرانژ و برکهف معرفی شده و مورد تحلیل و مقایسه قرار گرفتند. شاخص‌های مورد تحلیل شامل نوع درون‌یابی مورد استفاده، پیچیدگی محاسباتی، اندازه سهام، قابلیت تسهیم چندراز و قابلیت تسهیم تدریجی و ترتیبی رازها می‌باشند. بر اساس نتایج حاصل از مقایسه شاخص های مورد نظر طرح‌های معرفی شده، مشاهده می‌شود که طرح‌های ارائه شده توسط نویسندگان مقاله علاوه بر این‌که از اندازه سهام کوچکی برخوردارند و قابلیت تسهیم همزمان چند راز را پشتیبانی می‌کنند، لذا دارای قابلیت تسهیم تدریجی و ترتیبی رازها نیز هستند ولی سه طرح دیگر دارای این قابلیت‌ها نیستند.

۸- مراجع

[1] A. Shamir, “ How to share a secret”, Communications of the ACM, 22(11), pp. 612-613, 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys", In Proceedings of the National Computer Conference, Vol. 48. No. 313, 1979.
[3] A. Shamir, "How to share a secret", Communications of the ACM, 22(11): 612-613, 1979.
[4] L. Harn, "Efficient sharing (broadcasting) of multiple secrets", IEE Proceedings Computers and Digital Techniques, 142(3): 237-240, 1995.
[5] V. Nikov, S. Nikov, B. Preneel, and J. Vandewalle., "Applying general access structure to proactive secret sharing schemes", IACR Cryptology ePrint Archive, 141, 2002.
[6] J. He, and E. Dawson,"Multistage secret sharing based on one-way function". Electronics Letters, 30(19): 1591–1592, 1994.
[7] H., Pilaram and T. Eghlidos, "An efficient lattice based multi-stage secret sharing scheme", IEEE Transactions on Dependable and Secure Computing, 14(1): 2–8, 2017.
[8] M. Nojoumian, D. R. Stinson, and M. Grainger, "Unconditionally secure social secret sharing scheme", IET Information Security, 4(4): 202–211, 2010.
[9] A. Shamir, "How to share a secret", Communications of the ACM, 22(11): 612-613, 1979.
[10] O. Farras, and C. Padro, "Ideal hierarchical secret sharing schemes", Information Theory, IEEE Transactions on, 58(5):3273–3286, 2012.
[11] G. J. Simmons, "How to (really) share a secret", In Proceedings on Advances in Cryptology, CRYPTO '88: 390–448, 1990.
[12] E. F. Brickell, "Some ideal secret sharing schemes", In Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology, EUROCRYPT'89: 468–475, 1990.
[13] T. Tassa, and N. Dyn, " Multi partite Secret Sharing by bivariate interpolation", Journal of, Cryptology, 22(2): 227–258, 2009.
[14] T. Tassa, "Hierarchical threshold secret sharing", Journal of Cryptology, 20(2): 237–264, 2007.
[15] K. Atkinson, and A. Sharma, "A partial characterization of poised hermite–birkhoff interpolation problems", SIAM Journal on Numerical Analysis, 6: 230–235, 1969.
[16] G. Lorentz, K. Jetter, S. D. Riemenschneider, "Birkhoff Interpolation.Encyclopedia of Mathematics and its Applications", Vol.19. ISBN: 0-201-13518-3, 1984.
[17] A. Beimel, T. Tassa, and E. Weinreb, " Characterizing ideal weighted threshold secret sharing", In Second Theory of Cryptography Conference, TCC 2005. Lecture Notes in Computer Sci. 3378: 600–619, 2005.
[18] P. Morillo, C. Padro, G. Saez, and J. L. Villar,"Weighted threshold secret sharing schemes", Information Processing Letters, 70(5): 211 – 216, 1999.
[19] M. E. Ebrahimi Kiasari, A. Mirghadri, N. Pakniat, and M. Nazari, "Proactive multi-secret sharing scheme based on lagrange interpolation and chinese remainder theorem", Journal of New Researches in Mathematics, 28:145-156, 2021.
[20] M. E. Ebrahimi Kiasari, A. Mirghadri, N. Pakniat, and M. Nazari, "A new social multi-secret sharing scheme using Birkhoff interpolation and Chinese remainder theorem", The ISC Int'l Journal of Information Security, Volume 15, Number 1, pp. 125–135, 2022.
[21] Z. Eslami, N. Pakniat, and M. Nojoumian, "Ideal social secret sharing using Birkhoff interpolation method", Security and Communication Networks, 9(18):4973–4982, 2016.
[22] N. Pakniat, and Z. Eslami, "Verifiable social multi-secret sharing secure in active adversarial model. Journal of Computing and Security, 4(1): 3–12, 2017.