



Survey and analysis of several secret sharing schemes based on interpolation methods

M.E. Ebrahimi Kiasari ¹, A.R. Mir GHadri ^{2*}, M.Nazari ³, N. Paknit ⁴

* Associate Professor, Faculty and Research Institute of Information and Communication Technology, Imam Hossein University (AS), Tehran, Iran

(Received: 2023/06/26, Revised: 2023/09/12, Accepted: 2023/10/11, Published: 2024/06/02)

DOR: <https://dorl.net/dor/20.1001.1.23224347.1403.12.1.2.0>

ABSTRACT

Secret sharing is one of the fascinating topics of cryptography, which is widely used in information security. The problem of secret sharing is a process in which one or more secrets are shared between a number of qualified participants or with different credentials. In times when there is a need to recover a secret, a number of people, whom we call authorized people, collect their shares to recover the desired secret. So far, various types of secret sharing schemes based on interpolation have been proposed. In these secret sharing plans, different interpolations have been used, depending on the structural needs of the plan. In this article, some secret sharing schemes based on interpolation are studied and analyzed. Then, by analyzing and comparing the basic features of these schemes, it can be seen that the two secret sharing plans based on Birkhoff interpolation have better efficiency than the other reviewed plans.

Keywords: Cryptography, secret sharing scheme, threshold secret sharing, Lagrange interpolation, Birkhoff interpolation

This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

Publisher: Imam Hussein University

 Authors



* Corresponding Author Email: Amrghdri@ihu.ac.ir



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 خرم‌آباد، دانشگاه آزاد اسلامی، خرم‌آباد، ایران ۲. دانشیار، دانشکده و پژوهشکده فناوری اطلاعات و

ارتباطات، دانشگاه جامع امام حسین (ع)، تهران، ایران ۳. استادیار، گروه ریاضی، واحد خرم‌آباد، 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)

DOR: <https://dorl.net/dor/20.1001.1.23224347.1403.12.1.2.0>



* این مقاله یک مقاله با دسترسی آزاد است که تحت شرایط و ضوابط مجوز Creative Commons Attribution (CC BY) توزیع شده است.

نویسندگان

ناشر: دانشگاه جامع امام حسین (ع)

چکیده

تسهیم راز یکی از مباحث جذاب علم رمزنگاری است که در امنیت اطلاعات کاربرد زیادی دارد. مسئله تسهیم راز به فرایندی گفته می‌شود که در آن یک یا چند راز بین تعدادی از شرکت‌کنندگان صلاحیت‌دار و 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 موردنظر 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 برکھف نسبت به سایر طرح‌های بررسی شده دارای کارایی بهتری هستند.

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

۱-مقدمه

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 سلسله‌مراتبی موجود در این مثال، منطقی و منصفانه نیست که از یک سامانه امضای آستانه‌ای

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

¹Shamir

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

که در این حالت یک متخصص 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^۴ 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 موردنیاز است و متخصص 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 قابل‌استفاده 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 آستانه‌ای 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 طرح‌های 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 می‌شوند. همان‌طوری که در بخش قبل ذکر شد، در یک طرح تسهیم راز، تعدادی سهام بین سهام‌داران توزیع می‌شود، به‌گونه‌ای که زیرمجموعه‌های خاصی از سهام‌داران بتوانند با به اشتراک گذاشتن سهم‌های خود به راز برسند. این زیرمجموعه‌های خاص را زیرمجموعه‌های مجاز می‌نامیم. طرح‌های تسهیم راز آستانه‌ای و بلک‌لی به شرح ذیل معرفی می‌گردند.

معمولی (برای مثال (۴ و ۹)) 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^۱ و بریکل^۲ [۲] مورد بررسی قرار گرفته است.

در سال ۲۰۰۹ تا سا^۳ [۳] با استفاده از درون‌یابی برکف، یک طرح کارآمد، ایده‌آل و کاملاً امن برای این ساختار دسترسی ارائه کرد. ایده استفاده شده در طرح تا سا 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 برکف روی سهام خود، مشتقی از چندجمله‌ای تسهیم شده 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 ۲ و ۳. اما، در بسیاری از کاربردها تسهیم هم‌زمان چندین راز موردنیاز است. اجرای مکرر یک طرح تسهیم راز معمولی برای تسهیم جداگانه هر یک از رازها راه‌حلی بدیهی، اما ناکارآمد برای این مسئله است. در صورت استفاده از این رویکرد، هر کاربر به‌ازای 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 باهدف کاهش میزان سهم نهایی دریافتی هر کاربر ابداع شده‌اند.

مفهوم تسهیم چند راز برای اولین بار توسط هارن^۴ [۴] ارائه شده است. در این طرح، سهام شرکت‌کنندگان در طول زمان ثابت است. این مسئله برای رازهای با طول عمر زیاد مناسب نیست چرا

^۱Simmon

^۲Brickel

^۳Tasa

^۴Nikov

۱-۲- طرح تسهیم راز آستانه‌ای

همان‌طوری که در بخش قبل ذکر شد، در یک طرح تسهیم راز، تعدادی سهم بین سهام‌داران توزیع می‌شود. به‌گونه‌ای 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^۱ (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^۲ [۹] و طرح بلکلی^۳ [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 درون‌یابی‌ها 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 دوبعدی 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 دوبعدی 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 ابرصفحه‌های 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.

۳-۲- طرح تسهیم راز شمیر

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

جدول (۱-۲): 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:

$$f(x) = S + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1}$$

۱- ابتدا چندجمله‌ای $f(x)$ با مقادیر تصادفی $\{a_i\}_{i=1}^{t-1}$ تولید می‌کند.

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

پروتکل بازسازی: فرض کنید $Autsub = \{P_{\alpha_1}, P_{\alpha_2}, \dots, P_{\alpha_t}\}$ یک زیرمجموعه مجاز از شرکت کنندگان باشد. در این صورت یک شخص معتمد با در اختیار داشتن سهم 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 $f(\cdot)$ را بازسازی می‌کند.

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

۴-۲- 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^۴، 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, \dots, U_m تقسیم شده بنحوی که شرکت‌کنندگان موجود در یک زیرمجموعه دارای صلاحیت‌های یکسانی هستند و شرکت‌کنندگانی که در سایر زیرمجموعه‌های 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^۵: فرض کنیم Γ یک ساختار دسترسی باشد. شرکت‌کننده P را در این ساختار دسترسی به

^۱ Threshold secret sharing

^۲ Shamir Scheme

^۳ Blakley

^۴ Multipartite secret sharing

^۵ Hierarchical threshold secret sharing

به عنوان مؤلفه اصلی طرح تسهیم چندراز اجتماعی، جزئیات این طرح در جدول ۱-۳ آورده شده است.

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

الف) پروتکل تسهیم:

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

۱. چندجمله‌ای

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{t-2}x^{t-2} + Sx^{t-1}$$

روی میدان $GF(q)$ تولید می‌کند که $\{a_i\}_{i=0}^{t-2}$ مقادیری تصادفی هستند.

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

ب) پروتکل بازسازی:

فرض کنید $Autsub = \{P_{\alpha_0}, P_{\alpha_1}, \dots, P_{\alpha_{j-1}}\}$ 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 برکف را روی سهام فراهم شده اعمال کرده و مشتق مرتبه $(t_1 - t_j)$ -ام چندجمله‌ای $f(\cdot)$ را بازسازی می‌کند (یعنی $f^{(t_1-t_j)}(\cdot)$).

۲. فرض کنیم S' آخرین ضریب $f^{(t_1-t_j)}(\cdot)$ باشد. راز را به صورت

$$S = \frac{(t_j - 1)!}{(t_1 - 1)!} S'$$

۴- درونیابی‌های مورد استفاده

درون‌یابی لاگرانژ^۵: یکی از روش‌های تعیین یک چندجمله‌ای حداکثر از درجه n که در معادله

$$P(x_i) = f_i \quad i = 0, \dots, n \quad (1-4)$$

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

صورت سلسله‌مراتبی بالا دستی عضو 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^۱: ساختار دسترسی یک طرح تسهیم راز آستانه‌ای سلسله‌مراتبی فصلی با یک دنباله صعودی از مقادیر آستانه‌ای $\langle t_0, t_1, \dots, t_m \rangle$ مشخص می‌شود. در این طرح‌ها یک مجموعه دلخواه (A) از شرکت‌کنندگان، مجاز به بازسازی راز است اگر $(0 \leq j \leq m-1)$ وجود داشته باشد که $|A \cap (U_{i=0}^{m-i})| \geq t_{m-j}$. تسهیم راز آستانه‌ای سلسله‌مراتبی فصلی برای اولین بار توسط سایمونز^۲ و بریکل^۳ [۱۱] مورد بررسی قرار گرفته است. سایمونز با استفاده از ساختارهای هندسی^۴ استفاده شده در طرح تسهیم راز بلکالی [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 برکف 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 برکف 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

^۱ Disjunctive hierarchical threshold secret sharing

^۲ Simmons

^۳ Brickell

^۴ Geometric constructions

^۵ Lagrange interpolation

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

$$(۶-۴)$$

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

که در آن به ازای هر i, n_i عددی طبیعی است. چندجمله‌ای حداکثر از درجه n ، P را چندجمله‌ای درونیاب هرمتی^۱ گوییم، هرگاه در شرایط زیر صدق کند:

$$(۷-۴)$$

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

که در آن:

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

که (۷-۴) را شرایط درون‌یابی گوییم.

درون‌یابی برکف:

برکف مسئله درون‌یابی خود را به صورت 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

$$P_n^{(j)}(x_i) = C_{i,j} \quad (۹-۴) \quad (n+1 \text{ معادله})$$

صدق کند.

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

تعریف ۴-۱-۱ درون‌یابی برکف^۲: فرض کنید:

$$X = \{x_1, x_2, \dots, x_k : x_1 < x_2 < \dots < x_k\}$$

مجموعه‌ای از اعداد حقیقی باشد.

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

$$I(E) = \{(i, j) : e_{i,j} = 1\}$$

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

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

$$(۲-۴)$$

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

و سعی می‌کنیم $L_j(x)$ ها را چنان تعیین کنیم که معادله (۴-۲) برقرار باشد. برای این منظور می‌گوییم به ازای $i = 0, 1, \dots, n$ باید داشته باشیم:

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

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

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

اما تابع زیر

$$(۴-۴)$$

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

به ازای $x_0, x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_n$ صفر است، یعنی به ازای x_i هایی 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

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

امکان پذیر است. به عبارت دیگر داریم:

$$(۵-۴)$$

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

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

درون‌یابی هرمتی^۱:

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.

² Birkhoff interpolation

¹ Hermit

پولیا صدق کند و شامل ۱- دنباله پشتیبانی شده‌ای با طول فرد نباشد [۱۵].

قضیه فوق یکتایی جواب مسئله درون‌یابی برکف در زمان انجام محاسبات روی مجموعه اعداد حقیقی را بیان می‌کند. در این مقاله درون‌یابی برکف را در میدان‌های متناهی^۴ 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 مسئله 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 مسئله درون‌یابی برکف در میدان‌های متناهی را بیان می‌کند [۱۵].

قضیه ۴-۱-۵: مساله درون‌یابی برکف 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:

$$(۱۲-۴)$$

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

که l بزرگ‌ترین مرتبه مشتق موجود در داده‌های مسئله است در ادامه نحوه محاسبه جواب یک مساله درون‌یابی برکف 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 $I'(E) = \{\alpha_i : i = 1, \dots, N-1\}$ برداری باشد که از مرتب‌سازی $I(E)$ به صورت لغت‌نامه‌ای به دست 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 $C' = \{c'_i : i = 1, \dots, N-1\}$ را به عنوان بردار حاصل از مرتب‌سازی لغت‌نامه‌ای C در نظر بگیریم (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 برکف را به صورت زیر بدست آوریم:

$$P(x) = \sum_{j=0}^{N-1} \frac{|A(E, X, \varphi_j)|}{|A(E, X, \varphi)|} g_j(x), \quad (۱۳-۴)$$

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

در رابطه فوق $P^{(j)}(\cdot)$ 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 هرمی‌ات که بدون قید و شرط جواب یکتا دارند، مسئله درون‌یابی برکف ممکن است جواب یکتا نداشته باشند. در ادامه شرایط لازم و کافی برای یکتایی جواب مسئله درون‌یابی برکف را ذکر می‌کنیم.

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

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

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 برکف است. برای به دست آوردن شروط کافی برای یکتایی جواب این مساله، در ابتدا تعریف زیر را در نظر بگیرید:

تعریف ۴-۱-۳: یک ۱-دنباله^۲ در یک ماتریس درون‌یابی E به محل حضور بیشترین اهای متوالی در یک سطر از ماتریس E گفته می‌شود. به عبارت دیگر، یک ۱-دنباله، سه‌تایی به شکل (i, j_0, j_1) است $(0 \leq j_0 \leq j_1 \leq l, 1 \leq i \leq k)$ ، که به ازای هر $j_0 \leq j \leq j_1$ داشته باشیم $e_{i,j} = 1$ (برای درستی تعریف، فرض می‌کنیم $e_{i,-1} = e_{i,l+1} = 0$). یک ۱-دنباله (i, j_0, j_1) را پشتیبانی شده^۳ گوئیم 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 مسئله درون‌یابی برکف 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

^۱ Polya's condition

^۲ sequence

^۳ Supported 1-sequence

^۴ Finite field

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

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

باتوجه به وارون‌پذیری ماتریس $A(E, X, \varphi)$ (که توسط حل‌پذیری مسئله درون‌یابی برکھف موردنظر به‌دست‌آمده است)، داریم:

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

درایه‌های ماتریس $A(E, X, \varphi)^{-1}$ ضرایب درون‌یابی برکھف متناظر با مجموعه X و ماتریس درون‌یابی E نامیده می‌شوند. مثال ۴-۱-۹: مساله درون‌یابی برکھف 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:

(۴-۱۴)

$$A(E, X, \varphi) = \begin{bmatrix} (a_0(z)) & (a_0(z)) & (a_0(z)) & (a_0(z)) \\ \xi_0^{(x)} & \xi_1^{(x)} & \xi_{N-1}^{(x)} & \xi_{N-1}^{(x)} \\ (a_1(z)) & (a_1(z)) & (a_1(z)) & (a_1(z)) \\ \xi_0^{(x)} & \xi_1^{(x)} & \xi_{N-1}^{(x)} & \xi_{N-1}^{(x)} \\ \vdots & \vdots & \vdots & \vdots \\ (a_{N-1}(z)) & (a_{N-1}(z)) & (a_{N-1}(z)) & (a_{N-1}(z)) \\ \xi_0^{(x)} & \xi_1^{(x)} & \xi_{N-1}^{(x)} & \xi_{N-1}^{(x)} \end{bmatrix}$$

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 $|A(E, X, \varphi_j)|$ حول $(j+1)$ -امین ستون آن، فرمول زیر برای محاسبه جواب مساله درون‌یابی برکھف (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 $A_i(E, X, \varphi_j)$ ماتریس حاصل از حذف $(i+1)$ -امین سطر و $(j+1)$ -امین ستون ماتریس $A(E, X, \varphi_j)$ 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

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

در نتیجه داریم که $g_0(0) = 1$ و $g_j(0) = 0$ برای $1 \leq j \leq N-1$. بنابراین، در مساله درون‌یابی برکھف مورد نظر

$P(0)$ را می‌توانیم به صورت زیر محاسبه کنیم:

(۴-۱۷)

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

در ادامه به معرفی ضرایب درون‌یابی برکھف خواهیم پرداخت.

خاص وقتی که همه j_i ها صفر باشند، درونیاب لاگرانژ به دست 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 هرمی‌ات برای حل مسئله کارساز خواهد بود؟ جواب منفی است و برای حل این مسئله، برکف، درونیابی جدیدی مطرح کرد که تا حدودی پاسخ‌گوی حل این مشکل می‌باشد. در برخی از مراجع درونیاب هرمی‌ات را حالت خاصی از درونیاب برکف در نظر می‌گیرند. اما اگر برخی از دنباله‌ها شکسته شوند، درونیاب برکف 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 [۱۷] و [۱۸] می‌توان گفت درونیابی لاگرانژ در طرح‌های تسهیم راز برای افراد دارای صلاحیت یکسان کاربرد دارد. در بسیاری از موارد، $|A(E, X, \varphi_0)| = 12$ نظر گرفتن صلاحیت یکسان برای تمام افراد، فوضوی غیرمعمول 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 برکف استفاده شده است. تسهیم راز اجتماعی امکان تسهیم یک راز مابین مجموعه‌ای از شرکت‌کنندگان را به گونه‌ای فراهم می‌کند که امکان تغییر ارزش سهام شرکت‌کنندگان در طول زمان وجود داشته باشد. با توجه به این مساله، از درونیابی برکف 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 هرمی‌ات که از برکف ساده‌تر است استفاده نمود که در پاسخ باید به این نکته اشاره کرد که اگر از درونیابی هرمی‌ات 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 برکف نسبت به لاگرانژ دارد این است که با استفاده از درونیابی برکف 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 بارزتر بودن سهم فرد است. درحالی‌که

$$|A(E, X, \varphi_3)| = \begin{vmatrix} 1 & 1 & 1 & 10 \\ 1 & 2 & 4 & 28 \\ 0 & 0 & 2 & 24 \\ 0 & 0 & 0 & 6 \end{vmatrix} = 12$$

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

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

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

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 به وسیله 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، هرمی‌ات درونیاب معروف خود را ارائه داد. در سال ۱۹۰۶ برکف اولین مقاله در زمینه درونیابی حفره‌ای^۱ یا درونیابی برکف 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 $(j = 0, 1, 2, \dots, j_i)$ ، در $(4-9)$ 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 هرمی‌ات است. در حالت

^۱ Lacunary Interpolation

بلی	بلی	$2 q $	$o(t^{3.373})$	برکھف	طرح تسهیم چند راز اجتماعی [۲۰]
-----	-----	--------	----------------	-------	--------------------------------

اگر از درون‌یابی لاگرانژ استفاده شود باید افراد باصلاحیت 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 چند راز پیش‌نگر با استفاده از درون‌یابی لاگرانژ و قضیه باقی‌مانده چینی [۱۹] در سال ۲۰۲۱ و طرح تسهیم چندراز اجتماعی با استفاده از درون‌یابی برکھف 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 ۱-۶ آورده شده است. مشاهده می‌شود که دو طرح ارائه شده در [۱۹] و [۲۰] علاوه بر این که 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 ۱-۶ 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.

جدول (۱-۶): مقایسه چند طرح تسهیم راز از لحاظ کارایی و سایر

ویژگی‌ها

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

۷- نتیجه‌گیری

در این تحقیق پنج طرح تسهیم چند راز بر اساس درون‌یابی لاگرانژ و برکھف معرفی شده و مورد تحلیل و مقایسه قرار گرفتند. شاخص‌های مورد تحلیل شامل نوع درون‌یابی مورد استفاده، پیچیدگی محاسباتی، اندازه سهام، قابلیت تسهیم چند راز و قابلیت تسهیم تدریجی و ترتیبی رازها هستند. بر اساس نتایج حاصل از مقایسه شاخص‌های مورد نظر طرح‌های معرفی شده، مشاهده می‌شود که طرح‌های ارائه شده توسط نویسندگان مقاله علاوه بر این که 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 Aryptographic 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., P. P. 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. Nojournian, 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

- 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 Mmulti-secret Sharing Scheme Bbased 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 Acheme 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. Nojournian, "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.
- 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 Aivariate Interpolation", *Journal of, Cryptology*, 22(2): 227–258, 2009.
- [14] T. Tassa, "Hierarchical Sthreshold secret Aharing", *Journal of Cryptology*, 20(2): 237–264, 2007.
- [15] K. Atkinson, and A. Sharma, "A partial Characterization of Poised Hermite–Birkhoff Interpolation Aproblems", *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*