مقدمه

بسمه تعالی

جلسه دفاع از پایان‌نامه کارشناسی ارشد

رابطه بین تسهیم راز و کدهای خطی

سخنران: محبوبه کاملی

زمان: سه‌شنبه ۲۴ /۱۰ /۹۲ ساعت ۳۰ : ۹ صبح

مکان: تالار خوارزمی

هیئت داوران

۱- پروفسور مرتضی اسماعیلی

۲- دکتر علی زاغیان

۳- دکتر محمدحسام تدین

۴- دکتر حمیدرضا مرزبان

چکیده

تسهیم راز یکی از موضوعات مهم رمزنگاری است که در امنیت اطلاعات کاربرد دارد. چندین روش برای ساخت طرح‌های تسهیم راز وجود دارد. یکی از این روش‌ها مبتنی بر نظریه کدگذاری است. هر کد خطی می‌تواند برای ساخت طرح‌های تسهیم راز مورد استفاده قرار بگیرد. ساختار دسترسی طرح تسهیم راز مبتنی بر یک کد، کدکلمه‌های کمینه دوگان آن کد است. در این پایان‌نامه ابتدا چند ساختار از کدهایی که مسأله پوشش تحت شرایط خاص برای آن‌ها حل شده است معرفی می‌شود. مسأله پوشش در نظریه کدگذاری به مسأله مشخص کردن کدکلمه‌های کمینه یک کد معروف است. در قسمت دوم این پایان‌نامه، علاوه بر ساختار کدهای معرفی شده در قسمت قبل، از کدهای خوددوگان برای ساخت طرح‌های تسهیم راز استفاده شده است. به‌منظور تعیین ساختارهای دسترسی در طرح تسهیم راز مبتنی بر کدهای خوددوگان، خصوصیات ترکیبیاتی از جمله خصوصیت طرح‌ها و وزن‌شمار ژاکوبی مورد استفاده قرار می‌گیرند. در پایان با توجه به آن‌که تعیین ساختارهای دسترسی کمینه کار دشواری است و تنها برای کلاس خاصی از کدهای باینری صورت گرفته است الگوریتمی ارائه می‌شود که می‌تواند برای هر کد خطی باینری کدکلمه‌های کمینه را مشخص کند و به این ترتیب ساختار دسترسی کمینه در طرح تسهیم راز مبتنی بر هر کد خطی باینری را مشخص نماید.

کلمات کلیدی: طرح تسهیم راز، کدهای خطی، ساختار دسترسی، کدکلمه‌های کمینه، کدهای خوددوگان، خصوصیات طرح‌ها، وزن‌شمار ژاکوبی

دانشگاه صنعتی اصفهان
دانشکده علوم ریاضی

رابطه بین تسهیم راز و کدهای خطی

پایان‌نامه کارشناسی‌ارشد ریاضی کاربردی

محبوبه کاملی

استاد راهنما

پروفسور مرتضی اسماعیلی

دی ۱۳۹۲

دانشگاه صنعتی اصفهان
دانشکده علوم ریاضی

پایان‌نامه کارشناسی‌ارشد ریاضی کاربردی خانم محبوبه کاملی
تحت عنوان

رابطه بین تسهیم راز و کدهای خطی

در تاریخ ۲۴ /۱۰ /۹۲ توسط کمیته تخصصی زیر مورد بررسی و تأیید نهایی قرار گرفت.

۱– استاد راهنما	پروفسور مرتضی اسماعیلی
۲– استاد مشاور	دکتر علی زاغیان
۳– استاد داور۱	دکتر محمدحسام تدین
۴– استاد داور۲	دکتر حمیدرضا مرزبان

سرپرست تحصیلات تکمیلی دانشکده دکتر ظهوری زنگنه

سپاس شایان نثار ایزد متعال که توفیق علم آموزی را رفیق راهم ساخت و در مرحله دیگری از زندگی همراهم بود.

از استاد راهنمای ارجمندم جناب آقای پروفسور مرتضی اسماعیلی که در راه کسب علم مرا یاری نمودند کمال قدردانی را دارم.

هم چنین از زحمات استاد مشاور گرامی جناب آقای دکتر علی زاغیان بسیار سپاس گزارم.

با درود فراوان به روح پدر بزرگوارم که با مهربانی، چگونه زیستن را به من آموخت و

امتنان بیکران بر همدلی، همراهی و همگامی مادر دلسوز و فداکارم که از دامان گهربارش انسانیت و مهربانی را آموختم.

با سپاس بیکران به همسر مهربانم که با قلبی آکنده از عشق و معرفت، محیطی سرشار از سلامت، امنیت و آرامش برای من فراهم آورده است و مرا در راه رسیدن به اهداف عالی یاری می رساند.

و با تشکر خالصانه به آنان که نفس خیرشان بدرقه راهم بود و همه کسانی که به نوعی مرا در به انجام رساندن این مهم یاری نموده اند.

تقدیم به

همسر بی نظیر و مهربانم

مادر عزیز و فداکارم

"به یاد پدر دلسوز و بزرگوارم"

فهرست مطالب

چکیده

تسهیم راز یکی از موضوعات مهم رمزنگاری است که در امنیت اطلاعات کاربرد دارد. چندین روش برای ساخت طرح‌های تسهیم راز وجود دارد. یکی از این روش‌ها مبتنی بر نظریه کدگذاری است. هر کد خطی می‌تواند برای ساخت طرح‌های تسهیم راز مورد استفاده قرار بگیرد. ساختار دسترسی طرح تسهیم راز مبتنی بر یک کد، کدکلمه‌های کمینه دوگان آن کد است. در این پایان‌نامه ابتدا چند ساختار از کدهایی که مسأله پوشش تحت شرایط خاص برای آن‌ها حل شده است معرفی می‌شود. مسأله پوشش در نظریه کدگذاری به مسأله مشخص کردن کدکلمه‌های کمینه یک کد معروف است. در قسمت دوم این پایان‌نامه، علاوه بر ساختار کدهای معرفی شده در قسمت قبل، از کدهای خوددوگان برای ساخت طرح‌های تسهیم راز استفاده شده است. به‌منظور تعیین ساختارهای دسترسی در طرح تسهیم راز مبتنی بر کدهای خوددوگان، خصوصیات ترکیبیاتی از جمله خصوصیت طرح‌ها و وزن‌شمار ژاکوبی مورد استفاده قرار می‌گیرند. در پایان با توجه به آن‌که تعیین ساختارهای دسترسی کمینه کار دشواری است و تنها برای کلاس خاصی از کدهای باینری صورت گرفته است الگوریتمی ارائه می‌شود که می‌تواند برای هر کد خطی باینری کدکلمه‌های کمینه را مشخص کند و به این ترتیب ساختار دسترسی کمینه در طرح تسهیم راز مبتنی بر هر کد خطی باینری را مشخص نماید.

کلمات کلیدی: طرح تسهیم راز، کدهای خطی، ساختار دسترسی، کدکلمه‌های کمینه، کدهای خوددوگان، خصوصیات طرح‌ها، وزن‌شمار ژاکوبی

فصل ۱

مقدمه

در عصر ارتباطات و توزیع اطلاعات، پیشرفت سریع و همه جانبه ارتباطات ماهواره‌ای، گسترش شبکه‌های مخابراتی، استفاده روز افزون از کارت هوشمند و . . . نیاز به حفاظت از اصل داده و محرمانه بودن داده‌های در حال پردازش را از ضروریات قرار داده است. ارتباطات سیاسی و نظامی ایجاب می‌کرد که پی‌بردن به یک پیام، فقط برای افراد خاصی مجاز باشد و دیگران در صورت دسترسی به آن امکان فهم پیام را نداشته باشند. برای نیل به این مقصود، نظامیان، نمایندگان سیاسی دولت‌ها و . . . پیام را معمولاً به‌صورت رمز شده به مقصد ارسال می‌کردند تا در صورتی که به هر دلیل پیام به‌دست دیگران می‌افتاد برای آن‌ها قابل فهم نمی‌بود. ازطرف دیگر، عده‌ای تلاش می‌کردند تا از طریق پیام رمز شده، به محتوای نامه پی‌ببرند. تلاش موازی این دو گروه، موجب پیشرفت هنر رمزنگاری شد، تا این که امروزه، با پیشرفت علمی و صنعتی، هنر رمزنگاری به علم رمزنگاری تبدیل شده است.

باپیدایش علم رمزنگاری در قرن بیستم میلادی، موضوعات بسیاری مطرح شدند که با رمزنگاری رایج متفاوت بوده، ولی در دسته موضوعی رمزنگاری قرار گرفتند. اکثر این مباحث در نگاه اول، صرفاً یک بازی هوشی به نظر می‌رسند. لیکن، امروزه با نظری شدن آن‌ها به زیرشاخه‌هایی ازعلم رمزنگاری تبدیل گشته است. یکی از این مباحث، تسهیم راز است که در سال ۱۹۷۹ با یک پرسش ساده آغاز شد:

فرض کنید ۱۱ دانشمند روی پروژه محرمانه‌ای کار می‌کنند و نتایج تحقیقات آن‌ها در گاوصندوقی قرار دارد. به منظور رعایت نکات امنیتی، می‌خواهیم کاری کنیم که باز شدن درب گاوصندوق تنها درصورت حضور دست‌کم ۶ دانشمند ممکن باشد. چند قفل برای گاوصندوق مورد نیاز است؟ هر دانشمند باید چند کلید به همراه داشته باشد؟ در این مسئله فرض شده که باز شدن تنها یک قفل برای باز شدن درب گاوصندوق کافی است و برای باز شدن هر قفل، دقیقا ۶ کلید مورد نیاز است.

برای پاسخ‌گوئی به سؤال باید توجه داشت که هر ۶ نفر از ۱۱ دانشمند، باید قادر به گشودن درب

گاوصندوق باشند. تعداد حالات انتخاب ۶ نفر از ۱۱ دانشمند برابر است با:

$$\binom{۱۱}{۶} = \frac{۱۱!}{۶! \times (۱۱-۶)!} = ۴۶۲.$$

پس ۴۶۲ قفل برای گاوصندوق نیاز است. از طرف دیگر، هر دانشمند باید بتواند با کمک هر ۵ نفر از ۱۰ دانشمند دیگر، درب گاوصندوق را باز کند. بنابراین لازم است هر دانشمند به

$$\binom{۱۰}{۵} = \frac{۱۰!}{۵! \times (۱۰-۵)!} = ۲۵۲$$

طریق مختلف، درب گاوصندوق را باز کند. به این منظور، هر دانشمند باید ۲۵۲ کلید به همراه داشته باشد. تعداد قفل‌ها و کلیدها با افزایش تعداد دانشمندان و افزایش تعداد آستانه به‌سرعت افزایش می‌یابد. این تعداد زیاد و غیرعملی قفل‌ها و کلیدها لزوم یافتن یک راه حل جایگزین و طراحی یک سیستم عملی را روشن می‌سازد. راه حل پیشنهادی، استفاده از روش‌های تسهیم راز است.

تسهیم راز عبارت است از به اشتراک گذاشتن یک راز میان چند نفر، به‌طوری‌که برای بازیابی راز به مشارکت زیرمجموعه‌های خاصی از آن‌ها نیاز باشد. به‌عنوان مثال، در مسئله دانشمندان، راز یا همان کلید گاوصندوق مشخص می‌شود اگر و تنها اگر ۶ نفر از ۱۱ نفر در این کار مشارکت داشته باشند.

تسهیم راز از دو منظر اهمیت دارد: یکی مسئله از بین رفتن اطلاعات و دیگری مسئله عدم اطمینان کامل به یک شخص. به‌عنوان مثال، اگر کلید گاوصندوق یک بانک تنها در اختیار رئیس بانک باشد در هنگام عدم حضور رئیس (از بین رفتن موقتی اطلاعات) هیچ کس قادر به گشودن درب گاوصندوق نخواهد بود. از سوی دیگر، نمی‌توان اطمینان داشت که رئیس بانک از اطلاعات خود به‌منظور برداشت غیرمجاز از گاوصندوق سوءاستفاده نمی‌کند. چنانچه کلید گاوصندوق میان رئیس بانک و دو تن از معاونان او به اشتراک گذارده شود که هر دو نفر از سه نفر آن‌ها بتوانند درب گاوصندوق را باز کنند احتمال باز نشدن درب گاوصندوق در مواقع لازم و نیز احتمال سوءاستفاده از آن کاهش می‌یابد.

طرح تسهیم راز ابتدا در سال ۱۹۷۹ توسط شامیر [۲۴] و بلکلی [۴]، برای نگهداری از یک راز به‌صورت امن معرفی شد. پس از آن میگنوت [۱۹] و اسموث-بلوم [۲]، طرح تسهیم راز آستانه را در سال ۱۹۸۳ ارائه دادند و در همان سال کارنین [۱۴]، طرح تسهیم راز کامل را معرفی کرد. ایتو، سایتو و نیشزکی [۱۳]، در سال ۱۹۸۷ و بنالو و لیختر [۳]، در سال ۱۹۹۰ یک طرح کلی‌تر تسهیم راز را معرفی کردند.

در سال ۱۹۸۱ برای نخستین بار رابطه بین طرح تسهیم راز و نظریه کدگذاری مطرح شد [۱۸]. در این سال مک-الیس و سارویت [۱۸]، به رابطه بین طرح تسهیم راز آستانه شامیر و کدهای رید-سولومون اشاره کردند و نشان دادند روش تسهیم راز آستانه شامیر بسیار شبیه به کد رید-سولومون است. مسی [۱۷]،

از کدهای خطی برای طرح تسهیم راز استفاده کرد و به رابطه بین ساختار دسترسی و کدکلمه‌های کمینه کد دوگان اشاره کرد. او نشان داد که مجموعه‌های دسترسی یک طرح تسهیم راز مبتنی بر کدهای خطی، دقیقاً به مجموعه کدکلمه‌های کمینه کد دوگان مربوط می‌شود.

فصل‌های بعدی این پایان‌نامه این‌گونه در نظر گرفته شده‌اند که در فصل دوم، مفاهیم ابتدایی طرح تسهیم راز و کدهای خطی معرفی می‌شود. در فصل سوم، رابطه بین تسهیم راز و کدهای خطی بیان می‌شود و ساختار دسترسی برای برخی از کدهای خطی مشخص می‌گردد. در فصل چهارم، طرح تسهیم راز برای کدهای خوددوگان ارائه می‌شود. در فصل پنجم، الگوریتمی ارائه می‌گردد که می‌تواند ساختار دسترسی کمینه در طرح تسهیم راز مبتنی بر هر کد خطی باینری را مشخص نماید.

فصل ۲

مبانی و مفاهیم اولیه

مبحث تسهیم راز که برای اولین بار در سال ۱۹۷۹ توسط شامیر و بلکلی مطرح شد امروزه جایگاه ویژه‌ای در علم رمزنگاری دارد. تسهیم راز کاربردهای فراوانی دارد ازجمله در مدیریت کلیدهای رمزنگاری و بازکردن گاوصندوق بانک و به‌طور کلی هر فرآیندی که نیاز به مشارکت هم‌زمان داشته باشد. در این فصل به معرفی مبانی طرح تسهیم راز پرداخته می‌شود و در ادامه مفاهیمی از کدهای خطی ارائه می‌گردد.

۱.۲ تسهیم راز

تسهیم راز عبارت است از به اشتراک گذاشتن یک راز بین n نفر، به‌طوری که تنها زیرمجموعه‌های از پیش تعریف شده‌ای از آن‌ها قادر به بازیابی راز باشند و سایر زیرمجموعه‌ها که زیرمجموعه‌های غیرمجاز نام دارند نتوانند به راز دست یابند. یک حالت از این کار، به اشتراک گذاشتن یک راز بین n نفر است به‌طوری که هر t، $t \leq n$، نفر از آن‌ها بتوانند راز را بازیابی نمایند ولی هیچ تعداد کمتری نتوانند به راز دست یابند [۲۴].

اصطلاحات زیر در حوزه تسهیم راز به‌کار می‌روند:

راز: عدد $s \in \mathbb{F}_q$ که باید بین سهام‌داران به اشتراک گذاشته شود راز نامیده می‌شود.

سهم: یک سهم، داده‌ای محرمانه است که از سهم‌بندی کردن راز به‌دست می‌آید و در اختیار هریک از سهام‌داران قرار می‌گیرد.

سهام‌دار: سهام‌دار، شخصی است که سهم را دریافت کرده و از آن حفاظت می‌کند.

توزیع کننده: شخص امینی که راز را انتخاب و سهم‌بندی کرده و آن را بین سهام‌داران توزیع می‌کند توزیع کننده نامیده می‌شود. توزیع کننده متعلق به مجموعه سهام‌داران نیست.

زیرمجموعه مجاز: زیرمجموعه‌های خاصی از سهام‌داران که قادر به احیای راز هستند زیرمجموعه‌های مجاز نامیده می‌شوند.

زیرمجموعه غیرمجاز: زیرمجموعه‌هایی از سهام‌داران که قادر به احیای راز نیستند زیرمجموعه‌های غیرمجاز نامیده می‌شوند.

به عبارت دیگر، طرح تسهیم راز از دو مرحله زیر تشکیل می‌شود.

- تولید و توزیع سهم از راز: در این مرحله توزیع کننده سهم‌ها را محاسبه کرده و بین سهام‌داران توزیع می‌کند. راز به‌گونه‌ای بین سهام‌داران توزیع می‌شود که اگر بعضی سهام‌داران، سهم خود را از دست دادند باز هم راز قابل کشف باشد.

- احیای راز: در این مرحله زیرمجموعه‌های خاصی از سهام‌داران با به اشتراک گذاشتن سهم‌های خود، راز را احیا می‌کنند. در این قسمت، توزیع کننده حضور ندارد و شخص دیگری به‌عنوان ترکیب کننده با ترکیب سهم‌های حاصل از زیرمجموعه‌ای از سهام‌داران راز را بازیابی می‌کند. حضور ترکیب کننده در این مرحله الزامی نیست و این مرحله می‌تواند توسط خود سهام‌داران صورت گیرد.

۱.۱.۲ ساختار دسترسی

تعریف ۱.۱.۲ مجموعه سهام‌داران $P = \{p_1, p_2, \ldots, p_n\}$ را درنظر بگیرید که p_i سهام‌دار شماره i-ام است. در حالت کلی یک ساختار دسترسی عبارت است از معین کردن زیرمجموعه‌هایی از P مانند زیر که مجاز و قادر به بازیابی راز هستند.

$$\Gamma = \{K_1, K_2, \ldots\}.$$

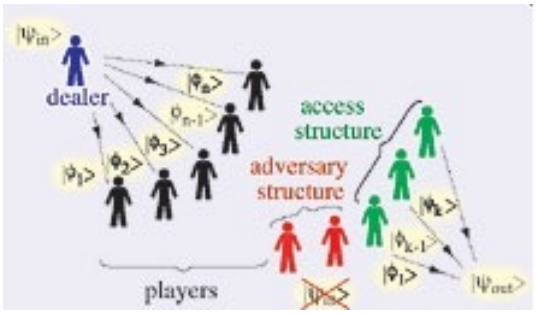
K_iها زیرمجموعه‌هایی از P هستند که می‌توانند راز را بازیابی کنند. اگر طرحی یافت شود که به K_iها اجازه بازیابی راز را بدهد و سایر زیرمجموعه‌های دیگر P را از دسترسی به راز باز دارد یک ساختار تسهیم راز پیدا می‌شود. K_iها مجموعه‌های دسترسی نامیده می‌شوند [۲۵]. به عبارت دیگر ساختار دسترسی Γ مجموعه تمام مجموعه‌های دسترسی است.

اگر A یک زیرمجموعه از P بوده و K_i یک زیرمجموعه مجاز از P، با شرط $K_i \subseteq A$، باشد آن‌گاه A نیز یک زیرمجموعه مجاز از P خواهد بود زیرا افراد مجموعه A، بدون نیاز به اطلاعات افراد مجموعه $A - K_i$، می‌توانند راز را بازیابی کنند. Γ معرف مجموعه تمام زیرمجموعه‌های مجاز P است. اگر $K_i \subseteq A \subseteq P$، آن‌گاه A نیز یک مجموعه دسترسی است.

یک مجموعه از سهام‌داران را مجموعه دسترسی کمینه گوییم هرگاه این مجموعه با ترکیب سهم‌هایشان بتوانند راز را بازیابی کنند ولی هیچ زیرمجموعه سره‌ای از آن‌ها نتوانند به راز دست یابند.

یک سهام‌دار را زاید گوییم هرگاه به هیچ مجموعه دسترسی کمینه تعلق نداشته باشد؛ به‌عبارتی این سهام‌دار، سهم تهی داشته باشد. بنابراین بدون از دست دادن کلیت مسئله فرض می‌کنیم که ساختار دسترسی شامل هیچ سهام‌دار زایدی نیست و اجتماع مجموعه‌های مجاز برابر با کل سهام‌داران است.

برای مثال در شکل ۱.۲ دیده می‌شود که توزیع کننده راز را میان ۵ سهام‌دار تقسیم می‌کند به‌طوری‌که فقط ۳ نفر از آن‌ها می‌توانند راز را بازیابی کنند. دو نفر دیگر به‌عنوان ساختار دشمن، سعی می‌کنند اطلاعاتی از راز را به‌دست آورند.



شکل ۱.۲: ساختار دسترسی طرح تسهیم راز [۲۴]

طرح‌های تسهیم راز با توجه به مقایسه تعداد سهام‌داران مجموعه‌های مجاز با یکدیگر به دو دسته به شرح زیر تقسیم می‌شوند.

۲.۲ تسهیم راز آستانه

تعریف ۱.۲.۲ یک طرح تسهیم راز که تعداد سهام‌داران مجموعه‌های مجاز آن با هم برابر باشند و هیچ زیرمجموعه‌ای از سهام‌داران که تعداد اعضایشان کمتر از تعداد سهام‌داران مجموعه‌های مجاز است نتوانند به راز دست یابند طرح تسهیم راز آستانه نامیده می‌شود.

اگر n وt اعداد صحیح مثبتی بوده و $t \leq n$، آنگاه یک (t, n) –طرح تسهیم راز آستانه یک روش تسهیم راز بین یک مجموعه n عضوی از سهام‌داران می‌باشد به‌طوری‌که هر t سهام‌دار بتوانند با اتحاد سهم‌هایشان راز را بازیابی کنند ولی هیچ $t-1$ سهام‌دار و یا کمتر نتوانند به راز دست یابند [۱۹].

۳.۲ طرح تسهیم راز با ساختار دسترسی

با توجه به تعریف طرح تسهیم راز آستانه هیچ سهام‌داری نسبت به دیگری امتیازی ندارد. در بعضی از مواقع، لازم به اولویت‌بندی سهام‌داران است که در طرح تسهیم راز آستانه قابل اجرا نیست. وقتی سهام‌داران در سطوح دسترسی متفاوتی قرار بگیرند به سهام‌داران با اولویت بالاتر، تعداد سهم بیشتری تعلق می‌گیرد و بازیابی راز به سطح اولویت سهام‌داران وابسته خواهد بود و دیگر نیازی به یک مجموعه $t-$ عضوی نیست. به عبارت دیگر، طرح تسهیم رازی که در آن تعداد سهام‌داران زیرمجموعه‌های مجاز با هم برابر نباشند طرح تسهیم راز با ساختار دسترسی نامیده می‌شود [۲۵].

همان‌طور که از تعریف طرح تسهیم راز آستانه برداشت می‌شود طرح تسهیم راز آستانه حالت خاصی از طرح تسهیم راز با ساختار دسترسی است که در آن تعداد سهام‌داران زیرمجموعه‌های مجاز باهم برابرند.

تعریف ۱.۳.۲ اگر X یک متغیر تصادفی باشد میزان ابهام این فرآیند تصادفی با $H(X)$ نمایش داده می‌شود و مقدار آن برابر است با:

$$H(X) = -\sum_{x \in X} p(x) log\ p(x).$$

$H(X)$ تابع آنتروپی شانون نامیده می‌شود.

۴.۲ تسهیم راز کامل

تعریف ۱.۴.۲ یک طرح تسهیم راز را کامل گوییم هرگاه هر زیرمجموعه مجاز آن قادر به بازسازی راز باشد ولی اطلاعات هر زیرمجموعه غیرمجاز نه تنها منجر به احیای راز نشود بلکه هیچ‌گونه اطلاعاتی بیش از اطلاعات یک سهام‌دار در مورد راز به‌دست ندهد [۱۴]. برای درک بهتر طرح تسهیم راز کامل مثال زیر آورده شده است.

مثال ۲.۴.۲ فرض کنید راز یک عدد ۹۶ بیتی است. چهار سهام‌دار برای این طرح تسهیم راز انتخاب می‌شوند و راز طوری میان این چهار سهام‌دار تقسیم می‌شود که مشارکت هر چهار سهام‌دار برای احیای راز الزامی باشد. دو راه حل زیر درنظر گرفته شده است:

حالت اول، راز به چهار قسمت ۲۴ بیتی تقسیم شده و بین سهام‌داران توزیع می‌شود. اطلاعات دو سهام‌دار دو برابر اطلاعات یک نفر به تنهایی است و هر سه سهام‌دار از سهام‌داران می‌توانند به بخش بزرگی

از راز دست یابند. اگر این راز کلید یک سیستم رمزنگاری باشد ممکن است با فاش شدن ۷۲ = ۲۴ × ۳ بیت از کلید، کل سیستم شکسته شود.

حالت دوم، راز به چهار عدد ۹۶ بیتی تقسیم می‌شود به‌طوری‌که حاصل جمع این اعداد در مبنای ۲ راز ۹۶ بیتی را احیا می‌کند. در این‌صورت از حاصل‌جمع سه عدد ۹۶ بیتی، بدون حضور عدد چهارم، هیچ اطلاعاتی در مورد راز به‌دست نمی‌آید. اگر این اعداد به‌طور کامل تصادفی انتخاب شده باشند هر بیت از راز به احتمال ۰.۵ برابر با ۰ و به احتمال ۰.۵ برابر با ۱ خواهد بود.

با توجه به توضیحات بالا مشاهده می‌شود که اگر s یک راز و B یک زیرمجموعه غیرمجاز باشد آن‌گاه:

$$H(s|B) = H(s),$$

و اگر A یک زیرمجموعه مجاز باشد آن‌گاه:

$$H(s|A) = ۰.$$

۱.۴.۲ تسهیم راز ایده‌آل

تعریف ۳.۴.۲ یک طرح تسهیم راز که در آن اندازه تمام سهم‌ها یکسان و برابر با اندازه راز باشد، به‌عبارت دیگر، سهم‌ها و راز هر دو از یک دامنه انتخاب شده باشند، طرح تسهیم راز ایده‌آل نامیده می‌شود.

۵.۲ طرح تسهیم راز بلکلی

جرج بلکلی در سال ۱۹۷۹ با استفاده از نقاط در فضا، یک طرح تسهیم راز آستانه ارائه داد. در طرح تسهیم راز بلکلی، راز به‌عنوان یک نقطه در فضای t-بعدی تعریف شد. هر سهم معادل یک صفحه $t-۱$ بعدی است که دربردارنده نقطه است. فصل مشترک هر t صفحه به‌طور دقیق نقطه را مشخص می‌کند. واسطه سهم‌های یک راز s را بین n عضو توزیع می‌کند و هر گروه شامل t عضو، با متحد کردن سهم‌هایشان می‌توانند s را احیا کنند [۴].

۶.۲ طرح تسهیم راز شامیر

می‌دانیم هر t نقطه مجزا در دستگاه مختصات دودویی، به‌طور یکتا یک چندجمله‌ای از درجه حداکثر $t-۱$ را مشخص می‌کنند حال آن‌که به‌ازای هر $t-۱$ نقطه متمایز، بی‌نهایت چندجمله‌ای از درجه $t-۱$ وجود دارد که از آن $t-۱$ نقطه عبور می‌کند. این ایده اصلی الگوریتم تسهیم راز شامیر است.

فرض کنید s یک راز باشد. در روش شامیر، توزیع کننده یک چندجمله‌ای از درجه $t-۱$ با ضرایب تصادفی $a_۱$، $a_۲$، ...، $a_{t-۱}$ و جمله ثابت $a_۰ = s$ را به‌صورت زیر تولید می‌کند.

$$f(x) = s + a_۱x + a_۲x^۲ + \ldots + a_{t-۱}x^{t-۱}.$$

سپس مقدار تابع f در n نقطه مختلف، $x = ۱, ۲, \ldots, n$، محاسبه شده و مقدار $f(i)$ برای سهام‌دار i-ام به‌عنوان سهم در نظر گرفته می‌شود. برای بازسازی راز کافی است هر t نقطه دلخواه، مقدار سهم خود را فاش کنند. حال با داشتن t زوج $(i, f(i))$ و تشکیل یک دستگاه t معادله و t مجهول، چندجمله‌ای f به‌دست می‌آید و راز به‌صورت $s = f(۰)$ بازسازی می‌شود [۲۴].

ازجمله خواص طرح تسهیم راز شامیر می‌توان به موارد زیر اشاره کرد.

کامل بودن: اگرچه هر t نفر دلخواه می‌توانند به‌راحتی راز را بازیابی کنند ولی هیچ $t-۱$ نفری قادر نیستند هیچ‌گونه اطلاعاتی بیش از اطلاعات یک نفر به تنهایی به‌دست آورند چون بی‌نهایت چندجمله‌ای از درجه $t-۱$ وجود دارد که از $t-۱$ نقطه داده شده عبور می‌کنند.

ایده‌آل بودن: هرسهم، عددی هم اندازه با راز است.

قابلیت توسعه: به‌راحتی با افزایش n و ایجاد نقاط بیشتر می‌توان افراد بیشتری را در طرح شرکت داد.

قابلیت انعطاف: دربرخی از کاربردها سهام‌داران ارزش برابر ندارند و لازم است که برخی از آن‌ها از امتیاز بیشتری در بازیابی راز برخوردار باشند. این کار با اختصاص دادن تعدادی سهم به هر سهام‌دار، متناسب با امتیاز او در بازیابی راز صورت می‌گیرد.

مثال ۱.۶.۲ یک $(۳, ۵)$-طرح تسهیم راز شامیر در نظر گرفته می‌شود (هر۳ سهام‌دار از ۵ سهام‌دار قادر به احیای راز هستند). راز عدد $s = ۷$ است و محاسبات به پیمانه $q = ۱۷$ انجام می‌شود و ضرایب $a_۱ = ۵$ و $a_۲ = ۱$ به‌طور محرمانه و مستقل از میدان $\mathbb{F}_{۱۷}$ انتخاب شده‌اند. توزیع کننده برای تولید و توزیع سهم‌ها چندجمله‌ای $f(x) = a_۰ + a_۱x + a_۲x^۲$ را درنظر می‌گیرد و با جایگذاری ضرایب، سهم‌ها به‌صورت زیر