بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

بسمه تعالی

دانشکده علوم ریاضی

تأییدیه اعضای هیأت داوران حاضر در جلسه دفاع از پایان‌نامه کارشناسی‌ارشد

اعضای هیأت داوران نسخهٔ نهایی پایان‌نامه آقای هادی خان‌محمدی رشته ریاضی‌کاربردی به شماره دانشجویی ۹۰۵۲۰۴۱۰۰۷ تحت عنوان: «تحلیل و ارزیابی امنیت چند طرح تسهیم راز پویا» را در تاریخ ۱۳۹۲/۶/۲۶ از نظر فرم و محتوا بررسی نموده و آن را برای اخذ درجهٔ کارشناسی‌ارشد مورد تأیید قرار دادند.

اعضای هیأت داوران	نام و نام‌خانوادگی	رتبه علمی	امضاء
۱- استاد راهنما	دکتر محمدحسام تدین	استادیار	
۲- استاد مشاور	دکتر علی رجایی	استادیار	
۳- استاد ناظر داخلی	دکتر مهدیه طهماسبی	استادیار	
۴- استاد ناظر خارجی	دکتر عبدالرسول میرقدری	دانشیار	
۵- نماینده تحصیلات تکمیلی	دکتر مهدیه طهماسبی	استادیار	

آیین نامه چاپ پایان‌نامه (رساله)های دانشجویان دانشگاه تربیت مدرس

نظر به اینکه چاپ و انتشار پایان نامه (رساله)های تحصیلی دانشجویان دانشگاه تربیت مدرس، مبین بخشی از فعالیتهای علمی - پژوهشی دانشگاه است بنابراین به منظور آگاهی و رعایت حقوق دانشگاه،دانش آموختگان این دانشگاه نسبت به رعایت موارد ذیل متعهد می‌شوند:

ماده ۱: در صورت اقدام به چاپ پایان نامه (رساله)ی خود، مراتب را قبلا به طور کتبی به «دفتر نشر آثارعلمی» دانشگاه اطلاع دهد.

ماده ۲: در صفحه سوم کتاب (پس از برگ شناسنامه) عبارت ذیل را چاپ کند:

«کتاب حاضر، حاصل پایان نامه کارشناسی ارشد/ رساله دکتری نگارنده در رشته است که در سال در دانشکده دانشگاه تربیت مدرس به راهنمایی سرکار خانم/جناب آقای دکتر ، مشاوره سرکار خانم/جناب آقای دکتر و مشاوره سرکار خانم/جناب آقای دکتر از آن دفاع شده است.»

ماده ۳: به منظور جبران بخشی از هزینه‌های انتشارات دانشگاه، تعداد یک درصد شمارگان کتاب (در هر نوبت‌چاپ) را به «دفتر نشر آثارعلمی» دانشگاه اهدا کند. دانشگاه می‌تواند مازاد نیاز خود را به نفع مرکز نشر درمعرض فروش قرار دهد.

ماده ۴: در صورت عدم رعایت ماده ۳، ۵۰٪ بهای شمارگان چاپ شده را به عنوان خسارت به دانشگاه تربیت‌مدرس، تأدیه کند.

ماده ۵: دانشجو تعهد و قبول می کند در صورت خودداری از پرداخت بهای خسارت، دانشگاه می‌تواند خسارت مذکور را از طریق مراجع قضایی مطالبه و وصول کند؛ به علاوه به دانشگاه حق می‌دهد به منظور استیفای حقوق خود، از طریق دادگاه، معادل وجه مذکور در ماده ۴ را از محل توقیف کتابهای عرضه شده نگارنده برای فروش، تامین نماید.

ماده ۶: اینجانب هادی خان محمدی دانشجوی رشته ریاضی کاربردی مقطع کارشناسی ارشد تعهد فوق وضمانت اجرایی آن را قبول کرده، به آن ملتزم می شوم.

نام و نام خانوادگی: هادی خان محمدی

تاریخ و امضا: ۹۲/۱۰/۳

آیین‌نامه حق مالکیت مادی و معنوی در مورد نتایج پژوهشهای علمی دانشگاه تربیت مدرس

مقدمه: با عنایت به سیاست‌های پژوهشی و فناوری دانشگاه در راستای تحقق عدالت و کرامت انسانها که لازمه شکوفایی علمی و فنی است و رعایت حقوق مادی و معنوی دانشگاه و پژوهشگران، لازم است اعضای هیات علمی، دانشجویان، دانش‌آموختگان و دیگر همکاران طرح، در مورد نتایج پژوهشهای علمی که تحت عناوین پایان‌نامه، رساله و طرحهای تحقیقاتی با هماهنگی دانشگاه انجام شده است، موارد زیر را رعایت نمایند:

ماده ۱- حق نشر و تکثیر پایان نامه/ رساله و درامدهای حاصل از انها متعلق به دانشگاه می باشد ولی حقوق معنوی پدید اورندگان محفوظ خواهد بود.

ماده ۲- انتشار مقاله یا مقالات مستخرج از پایان‌نامه/ رساله به صورت چاپ در نشریات علمی و یا ارائه در مجامع علمی باید به نام دانشگاه بوده و با تایید استاد راهنمای اصلی، یکی از اساتید راهنما، مشاور و یا دانشجو مسئول مکاتبات مقاله باشد. ولی مسئولیت علمی مقاله مستخرج از پایان نامه و رساله به عهده اساتید راهنما و دانشجو می باشد.

تبصره: در مقالاتی که پس از دانش‌اموختگی بصورت ترکیبی از اطلاعات جدید و نتایج حاصل از پایان‌نامه/ رساله نیز منتشر می‌شود نیز باید نام دانشگاه درج شود.

ماده ۳- انتشار کتاب، نرم افزار و یا اثار ویژه (اثری هنری مانند فیلم، عکس، نقاشی و نمایشنامه) حاصل از نتایج پایان‌نامه/ رساله و تمامی طرحهای تحقیقاتی کلیه واحدهای دانشگاه اعم از دانشکده ها، مراکز تحقیقاتی، پژوهشکده ها، پارک علم و فناوری و دیگر واحدها باید با مجوز کتبی صادره از معاونت پژوهشی دانشگاه و براساس ائین نامه های مصوب انجام شود.

ماده ٤- ثبت اختراع و تدوین دانش فنی و یا ارائه یافته ها در جشنواره‌های ملی، منطقه‌ای و بین‌المللی که حاصل نتایج مستخرج از پایان‌نامه/ رساله و تمامی طرح‌های تحقیقاتی دانشگاه باید با هماهنگی استاد راهنما یا مجری طرح از طریق معاونت پژوهشی دانشگاه انجام گیرد.

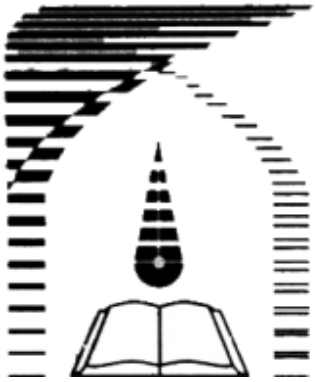
ماده ٥- این ایین‌نامه در ٥ ماده و یک تبصره در تاریخ۸۷/٤/۱ در شورای پژوهشی و در تاریخ ۸۷/٤/۲۳ در هیات رئیسه دانشگاه به تایید رسید و در جلسه مورخ ۸۷/۷/۱۵ شورای دانشگاه به تصویب رسیده و از تاریخ تصویب در شورای دانشگاه لازم‌الاجرا است.

اینجانب هادی خان محمدی دانشجوی رشته ریاضی کاربردی ورودی سال تحصیلی ۱۳۹۰

مقطع کارشناسی ارشد دانشکده علوم ریاضی متعهد می شوم کلیه نکات مندرج در ائین نامه حق مالکیت مادی و معنوی در مورد نتایج پژوهش های علمی دانشگاه تربیت مدرس را در انتشار یافته های علمی مستخرج از پایان نامه / رساله تحصیلی خود رعایت نمایم. در صورت تخلف از مفاد ائین نامه فوق الاشعار به دانشگاه وکالت و نمایندگی می دهم که از طرف اینجانب نسبت به لغو امتیاز اختراع بنام بنده و یا هر گونه امتیاز دیگر و تغییر ان به نام دانشگاه اقدام نماید ضمنا نسبت به جبران فوری ضرر و زیان حاصله بر اساس برآورد دانشگاه اقدام خواهم نمود و بدینوسیله حق هر گونه اعتراض را از خود سلب نمودم.

امضاء .....

تاریخ: ۹۲/۱۰/۳



دانشگاه تربیت مدرس

دانشکده علوم ریاضی

پایان نامه کارشناسی ارشد

تحلیل و ارزیابی امنیت چند طرح تسهیم راز پویا

نگارنده

هادی خان‌محمدی

استاد راهنما

دکتر محمدحسام تدین

استاد مشاور

دکتر علی رجایی

شهریور ۹۲

از استاد محترم آقای دکتر محمد حسام تدین که گام به گام در تهیه و تنظیم این پایان‌نامه به عنوان استاد راهنما و دوستی دلسوز بنده را یاری نمودند کمال تشکر و قدردانی را دارم.

از استاد ارجمند آقای دکتر علی رجایی که به عنوان استاد مشاور قبول زحمت کرده و به حق آنچه در توان داشتند برای یاری اینجانب دریغ نکردند بسیار سپاسگذارم.

از اساتید گرانقدر آقای دکتر عبدالرسول میرقدری و سرکار خانم دکتر مهدیه طهماسبی که زحمت داوری این پایان‌نامه را برعهده داشتند متشکرم.

از همه دوستانی که در طول این دوره دلسوزانه در کنار بنده بودند و بنده را از راهنمایی‌های خود بی نسیب نگذاشتند بسیار متشکرم.

در پایان از زحمات پدر و مادرم که به حق همه تلاش و توان خود را در جهت ارتقاء علم و فرهنگ بنده حقیر داشتند تشکر و قدردانی می‌کنم.

چکیده

تسهیم راز عبارت است از به اشتراک گذاشتن یک یا چند راز در میان افرادی به نام سهامدار، توسط فردی به نام مقسم؛ به نحوی که هرگاه زیر مجموعه‌های از پیش تعیین شده‌ای از مجموعه سهامداران جمع شوند و سهم‌های خصوصی خود را به اشتراک بگذارند، به همراه مقادیری که به صورت عمومی از پیش توسط مقسم انتشار یافته است، قادر باشند راز و یا رازها را بازیابی کنند.

یکی از بزرگترین چالش‌ها در این شاخه از رمزنگاری وجود تقلب سهامداران است. چرا که ممکن است سهامداری سهم خصوصی خود را تغییر داده و مقداری غیر از سهم اصلی خود را به اشتراک بگذارد. بنابراین طرح تسهیم رازی که این قابلیت را داشته باشد که در آن پیش از بازیابی راز درستی سهم‌های سهامداران بررسی شود، بسیار قابل توجه خواهد بود.

در این پایان‌نامه انواع طرح‌های تسهیم راز را به لحاظ امنیت و امکان وجود انواع تقلب بررسی می‌کنیم و در حد توان، با ایجاد تغییراتی در چند الگوی از پیش معرفی شده امنیت آن‌ها را افزایش می‌دهیم. در ضمن سعی می‌کنیم که ابزارهای ریاضی مورد نیاز جهت ایجاد امنیت در الگوهای تسهیم راز را مطرح کرده و نقش آن‌ها را در ایجاد امنیت بررسی کنیم. همچنین با استفاده از این ابزارها چند الگوی پیشنهادی معرفی میکنیم که دارای مزایای بسیاری از دیدگاه امنیت و کاهش هزینه‌های محاسباتی نسبت به الگوهای از پیش معرفی شده هستند.

در کنار امنیت، به موضوع پویایی طرح‌های تسهیم راز که باعث کاهش هزینه‌های راه‌اندازی الگو و کاهش پیچیدگی محاسباتی می‌شود نیز می‌پردازیم.

لغات کلیدی: تسهیم راز، مجموعه دسترسی، تقلب، کانال امن، امنیت محاسباتی، تأییدپذیری، پویایی، درونیابی چندجمله‌ای.

فهرست شکل ها و جدول ها

فهرست شکل ها

فهرست جدول ها

فهرست علائم و اختصارات

طرح تسهیم راز با امنیت محاسباتی	CSS
طرح تسهیم چند راز	MSS
طرح تسهیم چند راز چند مرحله‌ای	MSSS
طرح تسهیم راز با قابلیت تأیید همگانی	PVSS
طرح تسهیم راز تأییدپذیر	VSS
طرح تسهیم راز وزن‌دار	WSS
طرح تسهیم راز برای تسویر	ISS

فصل اول

مقدمه

مساله حفاظت از اطلاعات محرمانه از دیرباز مورد توجه بشر بوده است؛ به طوری که طی سال‌های متمادی روش‌های متفاوت زیادی جهت حفظ و نگهداری از اطلاعات محرمانه در مصارف گوناگون شخصی، اداری، نظامی و .... ارائه شده است.

مسأله تسهیم راز[1] نخستین بار با پرسش ساده زیر مطرح شد[۶]:

فرض کنید ۱۱ دانشمند بر روی یک پروژه محرمانه مشغول به کار هستند و می‌خواهند نتایج تحقیقات خود را در یک مکان امن نگهداری کنند، به طوری که درب این مکان تنها با حضور حداقل ۶ نفر از آن‌ها باز شود. اکنون سؤال این است که کمترین تعداد قفل‌ها ی مورد نیاز چقدر است؟ کمترین تعداد کلیدهای لازم برای هریک از دانشمندان چقدر است؟

در سال ۱۹۷۹ شامیر و بلاکلی، به طور مستقل از هم روشی جدید جهت پاسخ به این سؤال به نام تسهیم راز ارائه کردند[۱،۲] که به سرعت تبدیل به یکی از شاخه‌های رمزنگاری[2] مدرن شد.

تسهیم راز عبارت است از به اشتراک گذاشتن یک یا چند راز[3] (اطلاعات محرمانه) توسط فردی به نام مقسم[4] درمیان افرادی به نام سهادار[5] با اختصاص دادن مقادیری به آن ها تحت عنوان سهم[6] به نحوی که هرگاه

[1] Secret Sharing
[2] Cryptograghy
[3] secret
[4] Dealer
[5] Participant
[6] Share

زیرمجموعه‌های از پیش تعیین شده‌ای از این سهامداران جمع شده و سهم‌های خصوصی خود را به اشتراک بگذارند، قادر باشند که راز یا رازهای سیستم را بازیابی کنند و سایر زیر مجموعه‌ها قادر به بازیابی راز نباشند.

طرح های تسهیم راز کاربردهای فراوانی در زمینه های کنترل دسترسی به اطلاعات محرمانه، حفاظت از کلیدهای مخفی، دستگاه‌های بازیابی کلید، رأی‌گیری اینترنتی، توزیع یک سند رسمی، فروش اینترنتی و محاسبات چند بخشی (محاسباتی که هر بخش آن را یک نفر باید انجام دهد) و .... دار ند.

با ادامه مطاعات بر بروی طرح‌های تسهیم راز، چالش‌های بسیاری برای طرح‌های نخستین مطرح شد که از جمله آن‌ها می‌توان به امکان تقلب مقسم و تغییر در سهم‌های سهامداران به نحوی که امکان بازیابی راز را برای دسته‌ای از سهامدارن تسهیل نماید و یا امکان تقلب سهامداران به نحوی که در هنگام بازیابی راز تنها شخص متقلب از مقدار دقیق راز مطلع شود[۳]، عدم امکان به اشتراک گذاشتن چند راز[۴]، عدم امکان تغییر در پارامترهای سیستم از جمله مقدار راز، تعداد افرادی که جهت بازیابی راز حاضر می‌شوند و یا حذف و اضافه کردن سهامدار جدید به سیستم[۵] و ... را اشاره کرد. پژوهش‌های زیادی در سال‌های اخیر جهت رفع چالش-های مذکور انجام شده است به طوری که امروزه تقریباً تمام طرح‌های تسهیم رازی که مطرح می‌شوند فاقد مشکلات مذکور هستند.

بسته به محل استفاده از طرح تسهیم راز، امروزه مدل‌های زیادی از این الگوها مورد استفاده قرار می-گیرند. مثلاً فرض کنید راز مورد نظر بیش از حد بزرگ باشد برای این مورد راز را به قطعات کوچکتر می‌شکنند و توسط طرح‌های چند رازی (MSS) به اشتراک می‌گذارند؛ و یا ممکن است نیاز به بازیابی همه رازها نباشد و فقط در هر مرحله نیاز به بازیابی بخشی از رازها باشد که در این مورد نیز از طرح‌های چندگامی (MSSS) استفاده می‌شود؛ و یا حتی ممکن است بخواهیم توانایی یک یا چند سهامدار را به هنگام بازیابی راز تغییر دهیم به نحوی که شخص یا اشخاص مذکور نیاز به سهمامداران کمتری جهت بازیابی راز داشته باشند که در این مورد نیز از طرح‌های وزن دار (WSS) و یا طرح‌هایی با مجموعه‌های دسترسی عمومی[۷] استفاده می‌کنند که در آن ها مجموعه هایی از سهامدارن که قادر به بازیابی راز هستند دارای اندازه‌های متفاوت هستند. در این پایان‌نامه قصد داریم به ترتیب طرح های تسهیم راز ساده (طرح شامیر)؛ چندگانه (چند رازی)؛ چندگامی و در نهایت وزن دار مطرح تسهیم راز را از نقطه نظر چالش‌های مذکور به خصوص از نظر امنیت و پویایی بررسی کنیم و نیز جهت بررسی کارایی طرح‌های مطرح شده مقایسه‌ای بین این طرح‌ها انجام می‌دهیم. در ضمن یک طرح تسهیم

[7] General Access Structure

راز بر مبنای طرح شامیر ارائه خواهد شد که تقریبا تمام چالش‌های مذکور در آن برطرف شده است. همچنین یک طرح تسهیم راز چند رازی پیشنهادی نیز ارائه خواهیم داد که در راستای اثبات عدم وجود امنیت کامل در یکی از طرح‌های تسهیم راز و همچنین اثبات آسیب‌پذیری و رفع مشکلات امنیتی آن ارائه شده است.

ادامه پایان‌نامه به صورت زیر ارائه شده است:

در فصل دوم مبانی تسهیم راز و برخی تعاریف مهم که در تمام فصول پایان نامه مورد استفاده واقع خواهند شد. همچنین در این فصل به برخی از کاربردهای انواع الگو های تسهیم راز نیز اشاره‌ای مختصر شده است. در فصل سوم به تعمیم طرح تسهیم راز شامیر پرداخته و چند طرح جدید که با تغییرات جزئی در طرح شامیر امکانات جالبی به این الگوها اضاله کرده اند رامطرح می‌کنیم. در فصل چهارم به تحلیل امنیت چند الگوی تسهیم راز چندگانه مطرح، بر حسب روشی که جهت ایجاد امنیت به کار برده‌اند می‌پردازیم. در فصل پنجم چند الگوی تسهیم راز چندگامی و در نهایت در فصل ششم نیز چند الگوی وزن‌دار را مورد بررسی قرار می‌دهیم. در پایان نیز یک جمع بندی و نتیجه‌گیری کلی از تمام مباحث پایان نامه و در نهایت پیشنهادهایی جهت ادامه کار ارائه می‌شود.

فصل دوم

مبانی تسهیم راز

۲-۱ مقدمه

در سال ۱۹۶۸، لیو مسأله زیر را مطرح کرد[۶]:

فرض کنید ۱۱ دانشمند بر روی یک پروژه محرمانه مشغول به کار هستند و می‌خواهند نتایج تحقیقات خود را در یک مکان امن نگهداری کنند، به طوری که درب این مکان تنها با حضور حداقل ۶ نفر از آن ها باز شود. اکنون سؤال این است که کمترین تعداد قفل‌های مورد نیاز چقدر است؟ کمترین تعداد کلیدهای لازم برای هریک از دانشمندان چقدر است؟

می‌توان نشان داد که حداقل تعداد قفل‌های مورد نیاز ۴۶۲ و حداقل تعداد کلیدها نیز برای هر یک از دانشمندان ۲۵۲ عدد است. کاملاً مشخص است که نگهداری این تعداد قفل و کلید برای دانشمندان غیر عملی است به ویژه وقتی تعداد دانشمندان زیاد شود عملاً تعداد قفل‌ها و کلیدها نیز بسیار زیاد خواهد شد.

در سال ۱۹۷۹ شامیر[۱] و بلاکلی[۲] با ارائه طرحی به نام تسهیم راز، پاسخی عملی به پرسش مذکور دادند. تسهیم راز به زبان ساده یعنی به اشتراک گذاشتن مقداری تحت عنوان راز (اطلاعات محرمانه) در میان افرادی به نام سهامدار به نحوی که هرگاه زیرمجموعه‌های معینی از آن ها جمع شده و سهم‌های خود را به اشتراک بگذارند قادر به یافتن راز باشند اما سایر زیر مجموعه‌ها این توانایی را نداشته باشند.

در این فصل ابتدا تعاریف دقیق ریاضی جهت درک مفهوم تسهیم راز را ارائه می‌شود. سپس تسهیم راز شامیر را به طور کامل تشریح کرده و به با کمک آن چالش‌های وارد بر طرح‌های تسهیم راز را به ترتیب مطرح می‌کنیم.

۲-۲ تعاریف اولیه

۲-۲-۱ تسهیم راز

فرض کنید $P = \{P_i : 1 \le i \le n\}$ مجموعه‌ای متشکل از n سهامدار، S فضای راز (مجموعه تمام رازهای ممکن) و S_i فضای سهم (مجموعه‌ای از تمام سهم‌های ممکن) سهامدار P_i باشد. یک طرح تسهیم راز عبارت است از روشی جهت به اشتراک گذاشتن مقدار محرمانه (راز) $s \in S$ در میان اعضای مجموعه P. در این روش هر سهامدار $P_i \in P$ یک سهم $s_i \in S_i$ را از شخصی به عنوان مقسم که خود عضو مجموعه P نیست به صورت محرمانه دریافت می‌کند به نحوی که تنها زیر مجموعه‌های معینی از سهامداران که زیر مجموعه‌های مجاز[۸] یا مجموعه‌های دسترسی نامیده می‌شوند؛ قادر باشند با به اشتراک گذاشتن سهم‌های خصوصی خود راز S را بازیابی کنند[۷].

همان‌طور که از تعریف مشخص است هر طرح تسهیم راز از دو الگوریتم اساسی تشکیل شده است که الگوریتم اول مربوط به نحوه رساندن سهم‌ها به سهامداران توسط مقسم است و الگوریتم بعدی مربوط به نحوه بازیابی رازها توسط سهامدارانی است که جهت بازیابی راز سهم‌های خود را به اشتراک گذاشته‌اند. در بسیاری از طرح‌های تسهیم راز فرض بر این است که به هنگام بازیابی راز، اعضای یک مجموعه مجاز سهم‌های خود را برای شخصی به نام ترکیب کننده[۹] ارسال می‌کنند و او با توجه به پروتکلی که مقسم قبلا جهت انجام تسهیم راز اتخاذ کرده بود، به وسیله سهم‌های سهامداران، ساختار ریاضی که راز در آن قرار دارد را بازیابی کرده و راز الگو را از آن استخراج می‌کند.

۲-۲-۲ ساختار دسترسی

مجموعه تمام زیر مجموعه‌های مجاز جهت بازیابی راز ساختار دسترسی[۱۰] نامیده می‌شود و با Γ نمایش داده می‌شود. درواقع مجموعه Γ یک زیر مجموعه از مجموعه توانی مجموعه P است ($\Gamma \subseteq 2^P$). حال اگر یک ابر مجموعه از یک زیرمجموعه مجاز از سهامداران خود دوباره یک زیر مجموعه مجاز باشد؛ به ساختار دسترسی موجود یک ساختار دسترسی یکنوا می‌گویند. به عبارت دیگر برای ساختار دسترسی یکنوا داریم[۷]:

[8] Authorized Subset
[9] Combiner
[10] Access Structure

$$A \in \Gamma, A \subseteq B \Rightarrow B \in \Gamma \qquad (۱-۲)$$

۳-۲-۲ تسهیم راز آستانه‌ای و ساختار دسترسی عمومی

در طرح‌های تسهیم راز آستانه‌ای[11]، همه مجموعه‌های مجاز دارای اندازه حداقل یک مقدار ثابت t هستند. به عبارت دیگر تنها زیر مجموعه‌های شامل حداقل t عضو قادر به بازیابی راز الگو هستند. این طرح‌ها به طرح‌های آستانه‌ای (t,n) معروف هستند. به عبارت دیگر برای طرح‌های تسهیم راز آستانه‌ای داریم :

$$\Gamma = \{A \subseteq P : |A| \geq t\} \qquad (۲-۲)$$

در مقابل طرح‌های تسهیم راز آستانه‌ای طرح‌های با ساختار دسترسی عمومی[12] هستند که در این طرح‌ها برای مجموعه‌های دسترسی اندازه خاصی تعیین نمی‌شود بلکه بنا به ساختار طراحی شده الگو این مجموعه‌ها دارای اندازه‌های متفاوتی هستند.

به عنوان مثال از یکی از طرح‌های تسهیم راز آستانه‌ای ساده می‌توان طرح شامیر را مثال زد. این طرح بر پایه درونیابی لاگرانژ[13] است (ضمیمه۱). بر پایه این قاعده که با فرض وجود t نقطه (x_1, y_1)، (x_2, y_2) ... و (x_t, y_t) به نحوی که $x_i \neq x_j$ برای $i \& j = 1,...,t$ فقط و فقط یک چندجمله‌ای $f(x)$ از درجه حداکثر $t-1$ موجود است که $f(x_i) = y_i$ برای $i = 1,...,n$.

از آنجایی که در بیان مباحث آتی این پایان نامه، الگوی شامیر نقش مهمی را ایفا می‌کند؛ لذا قصد داریم اندکی بیشتر وارد جزئیات این الگو شویم به همین منظور در بخش بعد این الگو را به طور کامل مطرح می‌کنیم.

۳-۲ الگوی شامیر

این الگو بر مبنای درونیابی چندجمله ای[14] بر روی میدان‌های متناهی[15] بنا شده است. فرض کنید p یک عدد اول بزرگ باشد. ما قصد داریم راز $s \in Z_p$ را میان n سهامدار P_1، P_2،...، P_n به نحوی به اشتراک بگذاریم که

[11] Threshoud Scheme
[12] General Access Structure
[13] Lagrang Interpolation
[14] Polynomial Interpolation