

پیشنهاد و مقایسه دو طرح تسهیم چند راز تصدیق پذیر: یک طرح خطی با امنیت استاندارد و یک طرح شبکه مبنا

مسعود هادیان^{۱*}، سمانه مشهدی^۲، نیلوفر کیاماری^۳

۱- استاد، ۲- استادیار، ۳- دانشجوی دکتری دانشگاه علم و صنعت ایران

(دریافت: ۹۸/۰۷/۱۰، پذیرش: ۹۸/۱۱/۱۲)

چکیده

در این مقاله، دو طرح تسهیم چند راز با خاصیت تصدیق پذیری ارائه داده می‌شود که شامل یک طرح تسهیم چند راز خطی با ساختار دسترسی عمومی و یک طرح آستانه‌ای (t, n) بر اساس مسئله یادگیری با خطا (LWE) می‌باشد. طرح اول، یک تسهیم چند راز (MSS) خطی می‌باشد که در آن تعدادی راز از طریق واسطه، متناسب با ساختار دسترسی مربوط به هر راز، در میان گروهی از سهامداران توزیع می‌شود. این طرح مزیت‌های طرح‌های قبلی را دارد و در مقایسه با آن‌ها کاربردهای عملی بسیاری مانند تصدیق پذیری و ویژگی چند بار مصرفی را دارا می‌باشد. بازسازی رازها نیز بر اساس ترتیب از پیش تعیین شده توسط واسطه انجام می‌شود. به علاوه امنیت طرح نیز در مدل استاندارد ثابت شده است. این طرح بر پایه مسائل سخت نظریه اعدادی بوده و بنابراین در برابر حملات کوانتومی ایمن نیست. طرح دوم ارائه شده در این مقاله یک طرح تسهیم راز مبتنی بر شبکه‌ها می‌باشد. در این طرح که یک تسهیم چند راز آستانه‌ای (t, n) است، حضور هم‌زمان حداقل t شرکت کننده برای بازسازی راز الزامی است. امنیت این طرح بر مبنای سختی مسئله LWE است. این مسئله بسیار سخت بوده و در برابر الگوریتم‌های کوانتومی مقاوم می‌باشد.

کلید واژه‌ها: تسهیم راز، تصدیق پذیری، امنیت استاندارد، پساکوانتوم، شبکه، مسئله LWE

۱- مقدمه

نتیجه سهامداران توانایی یکسانی برای دستیابی به راز داشتند. اما در واقعیت، با موارد فراوانی مواجه می‌شوید که بازسازی رازها، با استفاده از این روش مطلوب نمی‌باشد.

مثلاً دو شرکت کننده با موقعیت‌های متفاوت که در یک طرح تسهیم راز شرکت می‌نمایند متناسب با موقعیتشان باید از حق دسترسی متفاوتی برای راز برخوردار باشند. همین امر موجب تعریف مدل کلی تر و انعطاف پذیرتری با عنوان طرح تسهیم راز با ساختار دسترسی عمومی شد [۳-۵].

طرح‌های تسهیم راز تصدیق پذیر (VSS)، نقش مهمی در پروتکل‌های رمزنگاری مختلف دارند [۶-۷]. این طرح‌ها به احتمال تقلب توسط واسطه و شرکت کنندگان می‌پردازند و چندین دسته‌بندی از آن‌ها مطرح شده است. در یک دسته‌بندی این طرح‌ها بر اساس قدرت محاسباتی مهاجم تقسیم بندی می‌شوند: دسته اول در این تقسیم بندی طرح‌هایی هستند که قدرت محاسباتی مهاجم محدود است [۸-۱۱] و دسته دوم طرح‌های تصدیق پذیری هستند که در آن‌ها امنیت کامل و قدرت محاسباتی نامحدود برای مهاجم در نظر گرفته می‌شود [۱۲-۱۳، ۵] به طور طبیعی، به علت پیچیدگی‌های موجود در تبادل پیام و ارتباطات، مهاجم دارای قدرت محاسباتی محدود

یک طرح تسهیم راز، توزیع یک راز در میان یک گروه از سهامداران است به طوری که شخصی به عنوان واسطه به هر کدام از سهامداران یک سهم اختصاص می‌دهد و هر زیرمجموعه مجاز از سهامداران قادر به بازسازی مقدار راز با به اشتراک گذاری سهم‌هایشان می‌باشند اما هیچ زیرمجموعه غیر مجازی از سهامداران قادر به دستیابی به هیچ اطلاعاتی راجع به راز نیست. خانواده زیرمجموعه‌های مجاز سهامداران ساختار دسترسی نامیده می‌شود.

تسهیم راز آستانه‌ای (t, n) اولین و نوع خاصی از طرح‌های تسهیم راز است که در سال ۱۹۷۹ توسط شامیر [۱] و بلکلی [۲] به طور مستقل ابداع شد. طرح اول بر اساس درونیایی لاگرانژ و دومی بر اساس هندسه تصویری خطی بود.

طرح‌های تسهیم راز آستانه‌ای تنها قسمتی از ایده کلی طرح‌های تسهیم راز را برآورده می‌کردند زیرا در این طرح‌ها، سهم تمامی سهامداران از ارزش یکسانی برخوردار بودند و در

* رایانامه نویسنده مسئول: mhadian@iust.ac.ir

۱. MSSST1: در این دسته رازها می‌توانند با هر ترتیب دلخواهی بازسازی شوند [۱۴، ۱۹].

۲. MSSST2: بازسازی رازها باید بر حسب یک ترتیب از پیش تعیین شده انجام شود [۱۴، ۲۰].

دسته دوم در دنیای واقعی بسیار کاربردی می‌باشند. به عنوان مثال، ممکن است سامانه امنیتی یک بانک به گونه‌ای طراحی شده باشد که هر فرد برای دسترسی به پایگاه داده محرمانه مجبور به عبور از α پست بازرسی باشد. به علت سیاست امنیتی، عبور از هر پست بازرسی تنها در صورت حضور هم‌زمان حداقل t شرکت کننده ممکن است. اگر پست‌های بازرسی (رازها) به ترتیب طی نشوند به امنیت سامانه آسیب وارد می‌شود.

پیشرفت‌های اخیر در ساخت رایانه‌های کوانتومی تهدیدی جدی برای امنیت الگوریتم‌های رمزنگاری کلید عمومی رایج به حساب می‌آید. این الگوریتم‌ها بر اساس سختی مسائل تجزیه اعداد صحیح و لگاریتم گسسته می‌باشند. پس از معرفی الگوریتم‌های کوانتومی برای تجزیه و محاسبه لگاریتم گسسته توسط شور در ۱۹۹۴، مسیر تحقیقات به شیوه کلاسیک به سمت رمزنگاری پساکوانتوم در حال تغییر است [۲۱].

با این انگیزه در سال ۱۹۷۸، مک الیس اولین سامانه رمزنگاری پساکوانتوم که یک طرح رمزنگاری کلید عمومی بر اساس سختی مسئله کدینگ می‌باشد را ارائه کرد [۲۲]. هر چند تاکنون حتی یک حمله کوانتومی که تهدیدی جدی برای طرح مک الیس باشد شناخته نشده، الگوریتم‌های رمزنگاری بر مبنای کد کاربردی نیستند، زیرا نیاز به یک کلید عمومی با سایز بزرگ دارند (از ۱۰۰ کیلوبایت تا چندین مگابایت) [۲۳].

سامانه‌های رمزنگاری بر مبنای شبکه‌ها سهم مهمی در رمزنگاری پساکوانتوم دارند. این سامانه‌ها دارای محاسبات خطی کارآمدی بوده و امنیت آن‌ها بر اساس سختی مسائل شبکه‌ها قابل اثبات می‌باشد. به علاوه از آنجایی که تا کنون هیچ الگوریتم کوانتومی برای حل مسائل شبکه‌ها ارائه نشده، سامانه‌های رمز بر اساس شبکه‌ها در برابر حملات رایانه‌های کوانتومی مقاوم هستند [۲۳].

در سال ۱۹۹۶، آجتای اولین الگوریتم رمزنگاری مبتنی بر شبکه‌ها را ارائه کرد که ساختار یک خانواده از توابع یک طرفه می‌باشد و امنیت آن معادل سختی تقریب n^c از مسائل شبکه‌ها است [۲۴]. در اینجا n بعد فضای شبکه و c یک ثابت مثبت است.

امنیت طرح‌های رمزنگاری کلید عمومی بر مبنای شبکه‌ها مانند GGH [۲۵] و NTRU [۱۵] بر اساس سختی مسائل شبکه‌ها می‌باشد.

می‌باشد. بنابراین دسته اول این طرح‌ها به‌طور قابل توجهی کاربردی‌تر و عملی‌تر هستند. در یک دسته‌بندی دیگر طرح‌های تصدیق پذیر به دو نوع تعاملی و غیر تعاملی تقسیم می‌شوند. در طرح‌های تعاملی درستی، واسطه و سهامداران پس از رد و بدل کردن اطلاعاتی بین سهامداران و واسطه قابل ارزیابی است ولی در طرح‌های غیر تعاملی هیچ تعاملی برای بررسی درستی سهم‌های فرستاده شده لازم نیست. در یک تقسیم بندی دیگر هر گروه از سهامداران مجاز صادق به یک مقدار راز منحصر به فرد می‌رسند ولی در تقسیم بندی دیگر ممکن است علی‌رغم اینکه سهامداران مجموعه‌های مجاز درستکار باشند ولی به رازهای متفاوتی در بازسازی برسند.

طرح‌های تسهیم چند راز (MSS)، تعمیمی از طرح‌های تسهیم راز هستند. در این طرح‌ها که در دنیای واقعی کاربردهای زیادی دارند، از طریق یک فرآیند تسهیم راز، بیش از یک راز در میان سهامداران توزیع می‌شود. در طرح‌های تسهیم چند راز نیازی به تکرار فرآیند تسهیم راز و نگهداری از چند سهم توسط هر سهامدار نیست. هر سهامدار تنها یک سهم در ابتدای فرآیند توزیع راز دریافت می‌کند.

این طرح‌ها بر اساس نحوه بازسازی راز به دو دسته تقسیم بندی می‌شوند:

طرح‌های تسهیم چند راز عمومی (GMSS) و تسهیم چند راز چند مرحله‌ای (MSSS) که هر کدام با توجه به موقعیت ممکن است مفید باشند. در یک طرح عمومی همه رازها به‌طور هم‌زمان بازسازی می‌شوند [۱۷-۱۴، ۱۲].

در یک طرح تسهیم چند راز چند مرحله‌ای، رازها دارای درجات مختلفی از اهمیت بوده و هر زیرمجموعه مجاز از سهامداران قادر به بازسازی تنها یک راز در هر مرحله می‌باشد [۲۰-۱۸، ۱۶، ۱۴].

در این طرح‌ها واسطه می‌تواند تعداد دلخواهی راز را بین سهامداران بدون نیاز به تجدید سهم برای هر سهامدار توزیع نماید. از طرف دیگر هر سهامدار اطلاعات مورد نیاز برای بازسازی هر یک از رازها را با استفاده از سهم خود محاسبه و ارائه می‌دهد. این اطلاعات محاسبه شده از سهم، شبه سهم نامیده می‌شود. به عبارت دیگر در طرح‌های تسهیم راز چند مرحله‌ای، سهم هر سهامدار مشابه یک دسته کلید است که شبه سهم مورد نیاز برای بازسازی هر راز را برای وی تولید می‌کند.

طرح‌های تسهیم چند راز چند مرحله‌ای شامل دو دسته می‌باشند:

۲. رازها مرحله به مرحله با توجه به یک ترتیب از پیش تعیین شده بازسازی می‌شوند (MSSST2).
 ۳. خاصیت تصدیق پذیری غیر تعاملی برای واسطه و شرکت کنندگان وجود دارد.
 ۴. سهم‌ها چند بار مصرف بوده و پس از بازسازی راز مجدد قابل استفاده می‌باشند.
 ۵. امنیت محاسباتی طرح در مدل استاندارد ثابت شده است.
- علاوه بر این، دیگر طرح‌های تسهیم راز خطی دیگر می‌توانند به روش مشابه طرح ما [۳۳] به گونه‌ای توسعه داده شوند که دارای مزایای فوق باشند.

در این مقاله به یکی از مسائل مهم رمزنگاری یعنی آسیب پذیری طرح‌های مبتنی بر مسائل سخت نظریه اعداد در برابر حملات کوانتومی پرداخته شده است. در مرجع [۲۶] یک طرح تصدیق پذیر شبکه مینا مطرح شده بود که تمام سهامداران باید برای بازسازی رازها شرکت می‌کردند. در این مقاله با هدف بهبود طرح [۲۶]، یک طرح تسهیم چند راز با آستانه کمتر از n برای یک مجموعه متشکل از n سهامدار بر اساس مسئله LWE ارائه داده می‌شود. در این طرح سهامداران قادر به تصدیق سهم‌های دریافت شده از واسطه به صورت غیر تعاملی و تنها با استفاده از مقادیر عمومی هستند. مهم‌ترین تفاوت‌های دو طرح تصدیق پذیری که در این مقاله ارائه خواهد شد عبارتند از:

۱. طرح اول [۳۳] چند مرحله‌ای است ولی بازسازی تمام رازها در دومی هم‌زمان است.
 ۲. سهامداران مجاز درستکار در طرح اول به مقادیر منحصر به فرد از رازها می‌رسند ولی از آنجا که تصدیق سهم‌ها در طرح دوم بر اساس توابع درهم است ممکن است سهامداران مجاز درستکار به رازهای متفاوتی برسند.
 ۳. امنیت محاسباتی طرح اول به روش استاندارد اثبات شده است ولی این طرح در مقابل حملات کوانتومی آسیب پذیر است. اما طرح دوم شبکه میناست و در برابر حملات کوانتومی امن می‌باشد.
- ساختار مقاله به این ترتیب است که ابتدا مفاهیمی همچون چگونگی استفاده از مسئله غلاف یکنواخت span program (MSS) در طراحی تسهیم رازهای خطی، محاسبات چند بخشی، (MPC) طرح‌های رمزنگاری کلید خصوصی و مدل استاندارد طرح‌های (GMSS) و (MSSST2) بیان شده است. سپس طرح تسهیم چند راز خطی با قابلیت

طراحی تسهیم رازها بر اساس شبکه یک موضوع جدید است. در سال ۲۰۱۱، ژرژسو [۲۶] یک طرح تسهیم راز (n, n) را ارائه کرد که امنیت آن بر اساس سختی مسئله یادگیری با خطا (LWE) قابل اثبات بوده و در آن سهامداران قادر به تصدیق تمامی سهم‌های ارائه شده توسط واسطه می‌باشند. در سال ۲۰۱۲، بنزرخانی [۲۷] یک طرح تسهیم راز تصدیق پذیر (n, n) بر اساس شبکه‌ها ارائه کرد که در آن با استفاده از توابع درهم ساز خطی بر اساس شبکه‌ها هر سهامدار قادر به تصدیق سهم خود و همچنین راز بازسازی شده می‌باشد. امنیت این طرح بر اساس سختی تقریب n^c از مسئله کوتاه‌ترین بردار (SVP) است و به جای عملیات نمایی رایج در طرح‌های قبلی از عملیات ماتریس برداری کارآمد برای تصدیق سهم‌ها استفاده می‌کند.

۱-۱- انگیزه و هدف

تاکنون مدل‌ها و تعاریف متفاوتی برای طرح‌های تسهیم چند راز تصدیق پذیر آستانه‌ای ارائه شده است [۲۹-۲۸, ۱۴, ۱۱, ۹-۸].

در طرح‌های آستانه‌ای تمامی سهامداران از ارزش یکسانی برخوردار هستند و در نتیجه سهامداران توانایی یکسانی برای دستیابی به راز دارند. اما در واقعیت، با موارد فراوانی مواجه می‌شوید که بازسازی رازها، با استفاده از این روش مطلوب نمی‌باشد. مثلاً دو شرکت کننده با موقعیت‌های متفاوت که در یک طرح تقسیم راز شرکت می‌نمایند متناسب با موقعیتشان باید از حق دسترسی متفاوتی برای راز برخوردار باشند. همین امر موجب تعریف مدل کلی‌تر و انعطاف پذیرتری با عنوان طرح‌های تسهیم راز با ساختار دسترسی عمومی شده است.

طرح‌های تسهیم راز خطی شاخه مهمی از طرح‌های تسهیم راز با ساختار دسترسی عمومی می‌باشند. طرح‌های تسهیم چند راز خطی با ساختار دسترسی عمومی مانند [۳۲-۳۰, ۹, ۵-۴] که قبلاً ارائه شده‌اند:

۱. عمدتاً MSSST1 هستند.
 ۲. دارای خاصیت تصدیق پذیری برای واسطه و شرکت کنندگان نیستند.
 ۳. سهم‌ها چند بار مصرف نیستند و پس از بازسازی راز، مجدد قابل استفاده نمی‌باشند.
 ۴. اثبات امنیت استاندارد ندارند.
- برای از بین بردن این کمبودها، ما یک طرح تسهیم چند راز خطی (LMSS) جدید در [۳۳] ارائه شد که دارای خواص زیر می‌باشد:
۱. ساختار دسترسی عمومی دارد.

در ۱۹۹۳، کراچمر و ویگدرسن، مسئله غلاف یکنواخت (MSP) را به عنوان مدل خطی برای محاسبه توابع بولی یکنوا معرفی کردند [۳۵].

تعریف ۲-۴: یک MSP، سه تایی (F, M, ψ) است که F یک میدان متناهی، M یک ماتریس $l \times d$ روی میدان F و $\psi: \{1, \dots, l\} \rightarrow \{P_1, \dots, P_n\}$ یک تابع پوشا است که به هر سهامدار بعضی از سطرهای M را نسبت می دهد.

برای هر زیرمجموعه $A \subseteq P$ می توان یک بردار مشخصه $\delta_A = (\delta_1, \dots, \delta_n) \in \{0, 1\}^n$ در نظر گرفت به طوری که برای $1 \leq i \leq n$

$$\delta_i = 1 \text{ اگر و تنها اگر } i \in A$$

یک تابع بولی یکنوا $f: \{0, 1\}^n \rightarrow \{0, 1\}$ را در نظر بگیرید که برای هر $A \subseteq P$ و $B \subseteq A$ ، $f(\delta_B) = 1$ نتیجه می دهد $f(\delta_A) = 1$.

در نتیجه یک MSP تابع بولی یکنوا f را نسبت به بردار هدف $v \in K^l \setminus \{(0, \dots, 0)\}$ محاسبه می کند اگر رابطه زیر برقرار باشد:

$$f(\delta_A) = 1 \text{ اگر و تنها اگر } v \in \text{span}\{M_A\}$$

منظور از M_A سطرهای r از ماتریس M هستند که $\psi(r) \in A$.

یک طرح تسهیم راز با ساختار دسترسی Γ و تابع بولی یکنوا f_Γ به طوری که $f(\delta_A) = 1$ اگر و تنها اگر $A \in \Gamma$ را در نظر بگیرید.

محاسبه تابع f_Γ توسط یک MSP معادل است با وجود یک بردار هدف v که در فضای $\bigcap_{A \in \Gamma} \sum_{i \in A} V_i - \bigcup_{B \notin \Gamma} \sum_{i \in B} V_i$ قرار دارد. در اینجا V_i فضای تولید شده توسط سطرهای M است که توسط تابع ψ به سهامدار i ام نسبت داده شده است.

مفاهیم بالا را به آسانی می توان به بیش از یک بردار هدف تعمیم داد.

تعریف ۲-۵: یک MSP با α بردار هدف (v_1, \dots, v_α) ، چهار تایی (F, M, ψ, α) است که F یک میدان متناهی، M یک ماتریس $l \times d$ روی میدان F و $\psi: \{1, \dots, l\} \rightarrow \{P_1, \dots, P_n\}$ یک تابع پوشا است که به هر سهامدار بعضی از سطرهای M را نسبت می دهد.

در نتیجه یک MSP توابع بولی یکنوا f_1, \dots, f_α را نسبت به بردارهای هدف $v_1, \dots, v_\alpha \in K^l \setminus \{(0, \dots, 0)\}$ محاسبه می کند اگر رابطه زیر برقرار باشد:

$$\text{برای } j = 1, \dots, \alpha$$

تصدیق پذیری به همراه اثبات امنیت در مدل استاندارد [۳۳] شرح داده شده است. در بخش پایانی نیز یک طرح تسهیم چند راز تصدیق پذیر بر مبنای مسئله LWE پیشنهاد شده است. همچنین به منظور ارزیابی عملکرد طرح های پیشنهادی این طرح ها با طرح های مشابه دیگر مقایسه شده اند.

۲- پیشنیازها

۲-۱- ساختار دسترسی

تعریف ۲-۱: مجموعه سهامداران $\{P_1, \dots, P_n\}$ را در نظر بگیرید. یک خانواده $B \subseteq C$ و $B \in A$ اگر $A \subseteq 2^{\{P_1, \dots, P_n\}}$ یکنوا است. آنگاه $C \in A$. یک ساختار دسترسی، خانواده یکنوا Γ از زیرمجموعه های ناتهی $\{P_1, \dots, P_n\}$ است.

مجموعه های عضو Γ ، مجموعه مجاز و مجموع هایی که عضو Γ نیستند غیر مجاز نامیده می شوند.

مجموعه تمام زیرمجموعه های غیر مجاز را یک ساختار متخاصم Δ می نامند که در واقع همان $\Delta = \Gamma^c$ می باشد و تحت شمول پایینی بسته است. مجموعه Γ^- شامل اعضای مینیمال Γ و مجموعه Δ^+ شامل اعضای ماکسیمال Δ می باشد.

تعریف ۲-۲: [۳۴] یک طرح تسهیم راز شامل یک واسطه، n سهامدار P_1, P_2, \dots, P_n و یک ساختار دسترسی یکنوا $\Gamma \subseteq 2^{\{1, \dots, n\}}$ می باشد. برای تسهیم یک راز s در میان سهامداران، واسطه یک الگوریتم توزیع $Share$ را برای محاسبه سهم ها اجرا می کند.

$$Share(s) = (s_1, \dots, s_n)$$

سپس واسطه هر سهم s_i را به صورت مخفیانه به سهامدار P_i ، $i = 1, \dots, n$ می فرستد. اگر یک گروه از سهامداران قصد بازسازی راز را داشته باشند، یک الگوریتم بازسازی $Recover$ را که دارای خاصیت زیر می باشد اجرا می کنند:

$$\forall A \in \Gamma : Recover(\{s_i, i \in A\}) = s$$

و برای هر $A \notin \Gamma$ محاسبه s با استفاده از $\{s_i, i \in A\}$ به صورت محاسباتی غیر عملی است.

تعریف ۲-۳: [۳۴] یک تسهیم راز تصدیق پذیر، یک طرح تسهیم راز به همراه یک الگوریتم اضافی واری $Verify$ است که به سهامداران اجازه تصدیق اعتبار سهم هایشان را می دهد:

$$\exists u \forall A \in \Gamma : (\forall i \in A : Verify(s_i) = 1) \Rightarrow Recover(\{s_i, i \in A\}) = u,$$

و $u = s$ اگر واسطه صادق باشد.

۲-۲- مسئله غلاف یکنواخت

۲. هر شرکت کننده P_i فقط از داده خصوصی خود یعنی

$$\kappa_i \text{ و خروجی } \sum_{i=1}^t \kappa_i \text{ اطلاع دارد.}$$

در ادامه یک پروتکل MPC برای محاسبه مجموع داده‌ها را

بررسی می‌شود. هر شرکت کننده P_i به صورت تصادفی y_{ij} ، $1 \leq j \leq t-1$ را انتخاب می‌کند و y_{it} را نیز به صورت زیر در نظر می‌گیرد:

$$y_{ij} = \kappa_i - \sum_{j=1}^{t-1} y_{ij}$$

سپس P_i به صورت محرمانه y_{ij} را به P_j انتقال می‌دهد. P_j

$z_j = \sum_{i=1}^t y_{ij}$ را محاسبه کرده و z_j را منتشر می‌کند. سرانجام هر شرکت کننده مجموع زیر را محاسبه می‌کند:

$$\sum_{j=1}^t z_j = \sum_{j=1}^t \sum_{i=1}^t y_{ij} = \sum_{i=1}^t \sum_{j=1}^t y_{ij} = \sum_{i=1}^t \kappa_i = f(\kappa_1, \dots, \kappa_t)$$

	P_1	P_2	\dots	P_t	
$P_1: \kappa_1 \rightarrow$	y_{11}	y_{12}	\dots	y_{1t}	$\kappa_1 = \sum_{j=1}^t y_{1j}$
$P_2: \kappa_2 \rightarrow$	y_{21}	y_{22}	\dots	y_{2t}	$\kappa_2 = \sum_{j=1}^t y_{2j}$
\vdots	\vdots	\vdots	\dots	\vdots	\vdots
$P_t: \kappa_t \rightarrow$	y_{t1}	y_{t2}	\dots	y_{tt}	$\kappa_t = \sum_{j=1}^t y_{tj}$
	$z_1 = \sum_{i=1}^t y_{i1}$	$z_2 = \sum_{i=1}^t y_{i2}$	\dots	$z_t = \sum_{i=1}^t y_{it}$	

۲-۴- مشبکه‌ها

تعریف ۲-۶: فرض کنید Λ یک زیرگروه جمعی از $(\mathbb{R}^m, +)$ باشد که توسط یک پایه (غیر یکتا) $B = \{b_1, \dots, b_m\} \subset \mathbb{Z}^m$ از بردارهای مستقل خطی از اعداد صحیح تولید شده است.

$$\Lambda = L(B) := \left\{ \sum_{i=1}^m z_i \cdot b_i : z_i \in \mathbb{Z} \right\}$$

آنگاه Λ یک مشبکه m بعدی نامیده می‌شود.

از مشهورترین مسائل مشبکه‌ها مسئله کوتاه‌ترین بردار (SVP) و مسئله نزدیک‌ترین بردار (CVP) می‌باشند [۳۶].

الگوریتم‌های رمزنگاری بر مبنای مشبکه‌ها با فرض سختی این مسائل، سخت در نظر گرفته می‌شوند.

۲-۵- مسئله یادگیری با خطا

مسئله یادگیری با خطا (LWE) را رگو [۳۷] برای اولین بار به عنوان تعمیمی از مسئله شناخته شده "توازن یادگیری با اختلال" معرفی کرد. پارامترهای مسئله را یک بعد $n \geq 1$ و یک

$$f_j(\vec{\delta}_A) = 1 \text{ اگر } v_j \in \text{span}\{M_A\}$$

در ادامه می‌بینید که چگونه می‌توان با استفاده از یک MSP، یک طرح تسهیم راز خطی ساخت.

طرح‌های تسهیم راز خطی، طرح‌هایی هستند که در آن‌ها هر مجموعه مجاز از سهامداران، راز را با استفاده از یک ترکیب خطی از سهم‌هایشان بازسازی می‌کنند.

فرض کنید (F, M, ψ, α) یک MSP باشد.

اگر فضای تولید شده توسط سطرهاى ماتریس M باشد که توسط ψ به P_i نسبت داده شده است، آنگاه بردار هدف‌های $1 \leq j \leq \alpha$ را $e_j \in \bigcap_{A \in \Gamma_j} \sum_{i \in A} V_i - \bigcup_{B \in \Delta_j} \sum_{i \in B} V_i$ در نظر بگیرید.

فرض کنید MSP، توابع بولی یکنوا $f_{\Gamma_1}, \dots, f_{\Gamma_\alpha}$ را محاسبه می‌کند. یک طرح تسهیم چند راز خطی به شرح زیر است:

- مرحله توزیع: واسطه قصد دارد رازهای s_1, \dots, s_α را در میان سهامداران توزیع کند. وی بردار تصادفی ρ را به گونه‌ای در نظر می‌گیرد که $s_j = v_j \cdot \rho$ برای $j = 1, \dots, \alpha$ واسطه مؤلفه i ام $M\rho$ را به عنوان سهم به $P_{\psi(i)}$ می‌دهد.

- مرحله بازسازی: برای هر مجموعه مجاز $A \in \Gamma_j$ ، با توجه به تعریف MSP، بردار $w_A \in F^{|\Lambda|}$ وجود دارد به طوری که $w_A M_A = v_j$ پس

بنابراین سهامداران مجموعه A راز s_j را با محاسبه یک ترکیب خطی از سهم‌هایشان به دست می‌آورند.

۲-۳- محاسبات چند بخشی

هدف از محاسبات چند بخشی (MPC) امن، طراحی روش‌هایی است که با استفاده از آن، افراد بدون آنکه مقدار ورودی‌هایشان را افشا نمایند می‌توانند یک تابع از مقادیر ورودی‌هایشان را محاسبه نمایند.

امنیت به معنی تضمین صحت خروجی و امنیت داده‌های شرکت کننده‌ها حتی در صورت متقلب بودن بعضی از شرکت کننده‌ها می‌باشد.

مجموعه مجاز $A = \{P_1, \dots, P_t\}$ را در نظر بگیرید. فرض کنید κ_i داده خصوصی شرکت کننده P_i است. شرکت کننده‌ها برای محاسبه $f(\kappa_1, \dots, \kappa_t)$ یک پروتکل MPC را اجرا می‌کنند و در انتها

۱. مقدار صحیح $\sum_{i=1}^t \kappa_i$ توسط هر شرکت کننده محاسبه می‌شود.

ورودی‌های این الگوریتم شامل یک کلید k و متن m بوده و خروجی آن یک متن رمز شده تصادفی c می‌باشد.

$$c \leftarrow \text{Enc}(m, k)$$

۳- الگوریتم قطعی رمزگشایی Dec

ورودی‌های این الگوریتم شامل یک کلید k و متن رمز شده c بوده و خروجی آن پیام m می‌باشد.

$$m := \text{Dec}(c, k)$$

برای درستی طرح، برقراری شرط $\text{Dec}(k, \text{Enc}(k, m)) = m$ برای هر k و m الزامی است [15, 34].

آزمایش تمایز ناپذیری استراق سمع کننده چند پیامی:

در ادامه یک بازی میان مهاجم A_1 و چالشگر را توضیح داده می‌شود که امنیت یک طرح رمزنگاری کلید خصوصی، $\Gamma = (\text{Gen}, \text{Enc}, \text{Dec})$ بر اساس آن تعریف می‌شود [34]:

بازی G

۱. یک بیت تصادفی $\beta \in \{0,1\}$ توسط چالشگر انتخاب می‌شود.

۲. A_1 تعداد کلیدهای بازی را برابر با κ در نظر می‌گیرد.

۳. الگوریتم $\text{Gen}(1^\lambda)$ مرتبه برای تولید κ کلید محرمانه k_1, \dots, k_κ توسط چالشگر اجرا می‌شود.

۴. A_1 سه تایی (i_j, m_j^0, m_j^1) به طوری که $i_j \in \{1, \dots, \kappa\}$ و برای هر $j = 1, \dots, q_c$ $m_j^0 \neq m_j^1$ طول برابر دارند و q_c برابر با تعداد چالش‌ها است را انتخاب کرده و به عنوان پرسش به چالشگر می‌فرستد.

۵. الگوریتم $\text{Enc}(m_j^\beta, k_{i_j}) \leftarrow c_j^*$ توسط چالشگر اجرا شده و خروجی آن برای $j = 1, \dots, q_c$ به A_1 ارسال می‌شود.

۶. A_1 یک بیت β' را به عنوان خروجی می‌دهد.

۷. خروجی بازی در صورتی که $\beta = \beta'$ و در غیر این صورت ۰ تعریف می‌شود. در صورتی که خروجی ۱ باشد در واقع A_1 موفق شده است و در این حالت نوشته می‌شود $\text{PrivK}_{A_1}^{M, \text{Eav}}(\lambda) = 1$.

چنانچه برای هر (κ, q_c) مهاجم در زمان چند جمله‌ای A_1 یک تابع قابل چشم پوشی negl وجود داشته باشد که

$$\Pr[\text{PrivK}_{A_1}^{M, \text{Eav}}(\lambda) = 1] \leq \frac{1}{2} + \text{negl}(\lambda).$$

مبنای صحیح $q \geq 2$ و همچنین یک توزیع خطای χ تشکیل می‌دهند که معمولاً یک توزیع گاوسی $D_{Z,s}$ با انحراف معیار $\sigma = \frac{s}{\sqrt{2\pi}}$ در نظر گرفته می‌شود. بردار m مؤلفه‌های $s \in \mathbb{Z}_q^m$ را به عنوان راز در نظر بگیرید. یک نمونه LWE ، یک دوتایی $(a, b = \langle a, s \rangle + e \pmod q) \in \mathbb{Z}_q^m \times \mathbb{Z}_q$ می‌باشد که از یک بردار $a \in \mathbb{Z}_q^m$ که به صورت تصادفی با توزیع احتمال یکنواخت انتخاب شده است و یک بردار خطای χ تشکیل شده است. توزیع متشکل از این نمونه‌ها $A_{s,\chi} \subset \mathbb{Z}_q^m \times \mathbb{Z}_q$ ، توزیع LWE نامیده می‌شود.

برای راحتی مسئله LWE گاهی به صورت ماتریسی نمایش داده می‌شود. برای n نمونه LWE به صورت

$$(a_i, b_i = \langle a_i, s \rangle + e_i \pmod q)$$

فرض کنید $A \in \mathbb{Z}_q^{m \times n}$ ماتریسی باشد که ستون‌های آن a_i است و مقادیر $e_i \leftarrow \chi$ و $b \in \mathbb{Z}_q$ به ترتیب درایه‌های \mathbb{Z}_q^n و $B \in \mathbb{Z}_q^n$ باشند.

دو نوع مسئله LWE وجود دارد. با این نمادها، مسائل LWE رامی‌توان به صورت زیر تعریف کرد:

تعریف ۲-۷: (مسئله تصمیم‌گیری LWE)

دوتایی (A, B) را در نظر بگیرید به طوری که $A \in \mathbb{Z}_q^{m \times n}$ و $B \in \mathbb{Z}_q^n$ ، تعیین کنید که آیا B به صورت تصادفی با احتمال یکنواخت از \mathbb{Z}_q^n انتخاب شده است یا

$$B = As + e \pmod q.$$

تعریف ۲-۷: (مسئله جستجوی LWE)

دوتایی (A, B) را در نظر بگیرید به طوری که $A \in \mathbb{Z}_q^{m \times n}$ و $s \in \mathbb{Z}_q^n, B \in \mathbb{Z}_q^n$ را بیابید به طوری که

$$B = As + e \pmod q$$

۲-۶- طرح رمزنگاری کلید خصوصی

یک طرح رمزنگاری کلید خصوصی، از سه الگوریتم (احتمالاتی در زمان چند جمله‌ای) Stp, Dist و Rec ساخته شده است:

خروجی	ورودی	الگوریتم
pms	1^λ	تولید کلید
c	k, m	رمزنگاری
m	k, c	رمزگشایی

۱- الگوریتم تصادفی تولید کلید Gen

ورودی این الگوریتم یک پارامتر امنیتی 1^λ و خروجی آن تعدادی پارامتر عمومی pms برای طرح می‌باشد.

$$k \leftarrow \text{Gen}(1^\lambda)$$

۲- الگوریتم تصادفی رمزنگاری Enc

بازی G_1

۱. یک بیت تصادفی $b \in \{0,1\}$ توسط چالشگر انتخاب می‌شود.
۲. A_1 مجموعه سهامداران P و ساختار دسترسی Γ را منتشر می‌کند.
۳. الگوریتم $(Stp(1^\lambda, P, \Gamma), pms) \leftarrow$ توسط چالشگر اجرا شده و خروجی آن به A_1 ارسال می‌شود.
۴. یک زیرمجموعه $B \subseteq P$ به طوری که $B \notin \Gamma$ از شرکت کنندگان خرابکار توسط A_1 منتشر می‌شود.
۵. دو راز متفصلاً $s^0 = (s_1^0, \dots, s_\alpha^0) \neq (s_1^1, \dots, s_\alpha^1) = s^1$ توسط A_1 انتخاب و منتشر می‌شوند.
۶. الگوریتم $(\{sh_i\}_{P_i \in P}, Out_{pub}) \leftarrow$ $Dist(pms, s^b)$ توسط چالشگر اجرا شده و $(\{sh_i\}_{P_i \in B}, Out_{pub})$ فرستاده می‌شود.
۷. A_1 یک بیت b' را به عنوان خروجی می‌دهد.
۸. اگر $b = b'$ ، خروجی بازی ۱ و در غیر این صورت ۰ تعریف می‌شود. در صورتی که خروجی ۱ باشد در واقع A_1 موفق شده است و در این حالت نوشته می‌شود $GMSS_{A_1}^{CSA}(\lambda) = 1$.

چنانچه برای هر مهاجم در زمان چند جمله‌ای A_1 یک تابع قابل چشم پوشی $negl$ وجود داشته باشد که

$$\Pr[GMSS_{A_1}^{CSA}(\lambda) = 1] \leq \frac{1}{2} + negl(\lambda)$$

در نتیجه طرح $GMSS$ ، $\Omega = (Stp, Dist, Rec)$ امنیت تمایز ناپذیری در برابر حمله راز منتخب را دارد.

۲-۸- مدل استاندارد طرح‌های (MSSST2)

در یک طرح $MSSST2$ ، رازهای s_1, \dots, s_α توسط واسطه و بر اساس ساختار دسترسی‌های $\Gamma_1, \dots, \Gamma_\alpha$ (به طوری که $\Gamma_i \subseteq \Gamma_{i-1}$ برای $i = 2, \dots, \alpha$) در میان سهامداران توزیع می‌شوند. رازها مرحله به مرحله و با ترتیب s_1, \dots, s_α بازسازی می‌شوند. یک $MSSST2$ مانند Ω ، از سه الگوریتم $Stp, Dist, Rec$ ساخته شده است:

خروجی	ورودی	الگوریتم
pms	$1^\lambda, P, \Gamma_1, \dots, \Gamma_\alpha$	برپایی
$\{sh_i\}_{P_i \in P}, Out_{pub}$	$pms, s = (s_1, \dots, s_\alpha)$	توزیع
s'_j	$pms, Out_{pub}, j, s'_{j-1}, \{sh_i\}_{P_i \in A}$	بازسازی

در نتیجه طرح رمزنگاری کلید خصوصی $\Pi = (Gen, Enc, Dec)$ امنیت تمایز ناپذیری در حضور استراق سمع کننده را دارد.

۲-۷- مدل استاندارد طرح‌های (GMSS)

در یک طرح $GMSS$ ، رازهای s_1, \dots, s_α توسط واسطه و بر اساس ساختار دسترسی Γ در میان سهامداران توزیع می‌شود به گونه‌ای که هر زیرمجموعه مجاز از سهامداران قادر به بازسازی هم‌زمان تمامی رازها خواهند بود. یک $GMSS$ مانند Ω ، از سه الگوریتم $Stp, Dist, Rec$ ساخته شده است:

خروجی	ورودی	الگوریتم
pms	$1^\lambda, P, \Gamma$	برپایی
$\{sh_i\}_{P_i \in P}, Out_{pub}$	$pms, s = (s_1, \dots, s_\alpha)$	توزیع
$s' = (s'_1, \dots, s'_\alpha)$	$pms, Out_{pub}, \{sh_i\}_{P_i \in A}$	بازسازی

۱- الگوریتم برپایی Stp

ورودی‌های این الگوریتم شامل یک ساختار دسترسی Γ ، مجموعه سهامداران P و یک پارامتر امنیتی 1^λ و خروجی آن تعدادی پارامتر عمومی pms برای طرح می‌باشد.

$$pms \leftarrow Stp(1^\lambda, P, \Gamma)$$

۲- الگوریتم توزیع $Dist$

ورودی‌های این الگوریتم شامل pms و یک راز عمومی $s = (s_1, \dots, s_\alpha)$ که قرار است در میان سهامداران توزیع شود بوده و خروجی آن مجموعه سهم‌های $\{sh_i\}_{P_i \in P}$ و احتمالاً مقادیر عمومی Out_{pub} می‌باشد.

$$(\{sh_i\}_{P_i \in P}, Out_{pub}) \leftarrow Dist(pms, s)$$

۳- الگوریتم بازسازی Rec

ورودی‌های این الگوریتم شامل pms, Out_{pub} و سهم‌های $\{sh_i\}_{P_i \in A}$ برای شرکت کنندگان زیرمجموعه $A \subseteq P$ بوده و خروجی آن یک مقدار $s' = (s'_1, \dots, s'_\alpha)$ کمی‌باشد.

$$s' := Rec(pms, Out_{pub}, \{sh_i\}_{P_i \in A})$$

برای هر زیرمجموعه $A \in \Gamma$ و هر راز s ، لازمه درستی طرح، برقرار بودن شرط زیر می‌باشد:

$$s = Rec(pms, Out_{pub}, \{sh_i\}_{P_i \in A})$$

آزمایش تمایز ناپذیری در برابر حمله راز منتخب:

در ادامه یک بازی میان مهاجم A_1 و چالشگر را توضیح داده می‌شود که امنیت یک طرح $GMSS$ ، $\Omega = (Stp, Dist, Rec)$ بر اساس آن تعریف می‌شود [۳۴]:

۵. دو راز عمومی متفاوت $s^0 = (s_1^0, \dots, s_\alpha^0) \neq$

$$s^1 = (s_1^1, \dots, s_\alpha^1) \text{ به طوری که}$$

برای هر j که $B \in \Gamma_j$ دارید:

$$s_j^0 = s_j^1$$

توسط A_2 انتخاب و منتشر می‌شوند.

۶. الگوریتم $(\{sh_i\}_{P_i \in P}, Out_{pub}) \leftarrow$

$Dist(pms, s^b)$ توسط چالشگر اجرا شده و

$(\{sh_i\}_{P_i \in B}, Out_{pub})$ به A_2 فرستاده می‌شود.

۷. A_2 یک بیت b' را به عنوان خروجی می‌دهد.

۸. اگر $b = b'$ ، خروجی بازی ۱ و در غیر این صورت ۰

تعریف می‌شود. در صورتی که خروجی ۱ باشد در واقع

A_2 موفق شده است و در این حالت نوشته می‌شود

$$MSSS_{A_2}^{CSA}(\lambda) = 1$$

چنانچه برای هر مهاجم در زمان چند جمله‌ای A_2 یک تابع قابل

چشم پوشی $negl$ وجود داشته باشد که

$$\Pr[MSSS_{A_2}^{CSA}(\lambda) = 1] \leq \frac{1}{2} + negl(\lambda)$$

در نتیجه طرح $MSSS$ ، $(Stp, Dist, Rec)$ امنیت

تمایزناپذیری در برابر حمله راز منتخب را دارد.

۳- طرح MSSS خطی تصدیق پذیر

در ادامه یک طرح جدید $MSSST2$ با امنیت محاسباتی ارائه داده

می‌شود. ساختار طرح بر اساس مسئله غلاف یکنواخت می‌باشد

[۳۳]. در این طرح، m راز $s_1, \dots, s_m \in \mathbb{Z}_q$ توسط واسطه D

میان سهامداران مجموعه P توزیع می‌شود. طرح ارائه شده در این

بخش دارای خواص زیر می‌باشد:

- بازسازی رازها بر اساس ترتیب s_1, \dots, s_m که از قبل

توسط واسطه تعیین شده به طور جداگانه و در مراحل

متفاوت انجام می‌شوند.

- زیرمجموعه‌های غیر مجاز هیچ اطلاعی راجع به مقدار

راز s_i ندارند و تنها زیرمجموعه‌های مجاز P قادر به

بازسازی راز s_i است.

- طرح ارائه شده دارای ویژگی چند بار مصرفی می‌باشد

و سهامداران می‌توانند از سهم خود برای بازسازی

رازهای دیگر مجدد استفاده کنند.

- طرح دارای ویژگی تصدیق پذیری غیر تعاملی بوده

بنابراین هر سهامداری می‌تواند درستی سهم خود و

سهامداران دیگر را چک کند همچنین تمام

۱- الگوریتم برپایی Stp

ورودی‌های این الگوریتم شامل α ساختار دسترسی متفاوت

$\Gamma_1, \dots, \Gamma_\alpha$ به طوری که $\Gamma_i \subseteq \Gamma_{i-1}$ برای $i = 2, \dots, \alpha$ مجموعه

سهامداران P و یک پارامتر امنیتی 1^λ و خروجی آن تعدادی

پارامتر عمومی pms رای طرح می‌باشد.

$$pms \leftarrow Stp(1^\lambda, P, \{\Gamma_j\}_{1 \leq j \leq \alpha})$$

۲- الگوریتم توزیع Dist

ورودی‌های این الگوریتم شامل pms و یک راز عمومی

$s = (s_1, \dots, s_\alpha)$ که قرار است در میان سهامداران توزیع شود

بوده و خروجی آن مجموعه سهم‌های $\{sh_i\}_{P_i \in P}$ و احتمالاً مقادیر

عمومی Out_{pub} می‌باشد.

$$(\{sh_i\}_{P_i \in P}, Out_{pub}) \leftarrow Dist(pms, s)$$

۳- الگوریتم بازسازی Rec

ورودی‌های این الگوریتم شامل pms ، Out_{pub} ، یک اندیس

$z \in \{1, \dots, \alpha\}$ ، یک مقدار احتمالی s'_{j-1} برای راز $j-1$ ام و

سهم‌های $\{sh_i\}_{P_i \in A}$ برای شرکت کنندگان زیرمجموعه $A \subseteq P$

بوده و خروجی آن یک مقدار احتمالی s'_j برای راز j ام می‌باشد.

$$s'_j : = Rec(pms, Out_{pub}, j, s'_{j-1}, \{sh_i\}_{P_i \in A})$$

برای هر $z \in \{1, \dots, \alpha\}$ و هر زیرمجموعه $A \in \Gamma_j$ ، لازمه درستی

طرح، برقرار بودن شرط زیر می‌باشد [۳۴]:

$$s_j = Rec(pms, Out_{pub}, j, s_{j-1}, \{sh_i\}_{P_i \in A})$$

آزمایش تمایزناپذیری در برابر حمله راز منتخب

در ادامه یک بازی میان مهاجم A_2 و چالشگر را توضیح داده

می‌شود که امنیت یک طرح $MSSS$ ، $(Stp, Dist, Rec)$ بر Ω بر

اساس آن تعریف می‌شود [۳۴، ۱۵]:

بازی G_2

۱. یک بیت تصادفی $b \in \{0,1\}$ توسط چالشگر انتخاب

می‌شود.

۲. A_2 مجموعه سهامداران P و ساختار دسترسی‌های

$\Gamma_1, \dots, \Gamma_\alpha$ به طوری که $\Gamma_i \subseteq \Gamma_{i-1}$ برای $i = 2, \dots, \alpha$ را

منتشر می‌کند.

۳. الگوریتم $pms \leftarrow Stp(1^\lambda, P, \{\Gamma_j\}_{1 \leq j \leq \alpha})$ توسط

چالشگر اجرا شده و خروجی آن به A_2 ارسال

می‌شود.

۴. یک زیرمجموعه $B \subseteq P$ از شرکت کنندگان خرابکار

توسط A_2 منتشر می‌شود.

۴. واسطه عضو اولیه $g \in \mathbb{Z}_q$ را انتخاب کرده و g^{r_i} را برای $1 \leq i \leq d$ محاسبه می‌کند. اگر M_j نشان دهنده سطر j ام ماتریس M باشد، سهم $sh_j = M_j \cdot r$ از طریق یک کانال امن توسط واسطه به سهامدار P_j می‌شود.

۵. در انتها واسطه $N_j = g^{sh_j}$ برای $1 \leq j \leq n$ و $c_i = Enc(s_i, k_i)$ برای $2 \leq i \leq m$ را محاسبه می‌کند.

۶. مقادیر عمومی طرح عبارتند از:

$$Out_{pub} = \{c_2, \dots, c_m, N_1, \dots, N_n, g^{r_1}, \dots, g^{r_d}\}$$

۳-۳- تصدیق سهمها

از طریق چک کردن معادله زیر هر سهامدار P_i می‌تواند صحت سهم خود را تصدیق کند:

$$g^{sh_j} = (g^{r_1})^{m_{j1}} \times \dots \times (g^{r_d})^{m_{jd}} \pmod{q} \quad (1)$$

۴-۳- مرحله بازسازی رازها $\{sh_j\}_{P_j \in A}$ ، $ec(pms, out_{pub})$

۱-۴-۳ بازسازی راز s_1

مجموعه مجاز $A_1 = \{P_1, \dots, P_{t_0}\} \in \Gamma_1$ را در نظر بگیرید. اعضای این مجموعه برای بازسازی راز s_1 به صورت زیر عمل می‌کنند:

۱. برای بردار هدف $V_i = \langle v_i \rangle$ فضای تولید شده توسط بردار v_i باشد. واسطه بردار $v_i \in \mathbb{Z}_q^d$ را برای عدد مثبت d به هر سهامدار P_i نسبت می‌دهد به طوری که

$$\omega_{A_1} \cdot M_{A_1} = e_1 \quad (2)$$

قرار دهید $sh_j^+ := \omega_j sh_j = (\omega_j M_j) \cdot r$

۲. هر سهامدار $P_j \in A_1$ یک عدد صحیح تصادفی κ_j را انتخاب می‌کند. سپس شبه سهم خود یعنی $sh_j^+ + \kappa_j$ را به همراه $K_j^+ = g^{\kappa_j}$ منتشر می‌کند.

۳. هر سهامدار P_i با استفاده از معادله زیر قادر به تصدیق صحت سهم سهامدار P_j ، $(i \neq j)$ می‌باشد:

$$(3)$$

$$g^{(\kappa_j + sh_j^+)} = (N_j)^{\omega_j} K_j^+ \pmod{q}$$

۴. اعضای مجموعه A_1 ، مقدار $K^+ := \kappa_1 + \dots + \kappa_{t_0}$ را بر اساس محاسبات چند بخشی محاسبه می‌کنند.

۵. اعضای مجموعه A_1 ، راز s_1 را با استفاده از معادله زیر محاسبه می‌کنند:

$$\left(\sum_{P_j \in A_1} sh_j^+ \right) - K^+ = s_1 \quad (4)$$

مجموعه‌های مجاز درستکار به رازهای یکسانی می‌رسند.

۳-۱- مرحله برپایی $Stp(1^\lambda, P, \Gamma_1, \dots, \Gamma_m)$

فرض می‌شود مسئله لگاریتم گسسته در \mathbb{Z}_q برای عدد اول بزرگ $q > n$ مشکل باشد. رازهای $s_1, \dots, s_m \in \mathbb{Z}_q$ توسط واسطه D در میان سهامداران P_1, \dots, P_n به ترتیب بر اساس ساختار دسترسی‌های $(\Gamma_1)_{min}, \dots, (\Gamma_m)_{min}$ به صورت زیر توزیع می‌شوند:

واسطه D به هر سهامدار P_j یک مقدار j نسبت داده و یک طرح رمزنگاری کلید خصوصی امن $\Pi = (Gen, Enc, Dec)$ را انتخاب می‌کند. پارامترهای عمومی عبارتند از $pms = (q, \Pi, P, \Gamma_1, \dots, \Gamma_m)$.

۳-۲- مرحله توزیع سهمها $Dist(pms, s)$

مراحل زیر توسط واسطه انجام می‌شوند:

۱. واسطه با هدف تولید m کلید محرمانه k_1, \dots, k_m مرتبه الگوریتم $Gen(1^\lambda)$ را اجرا می‌کند.

۲. واسطه با روش زیر یک MSP ، $(\mathbb{Z}_q, M, \psi, m)$ می‌سازد:

- فرض کنید $V_i = \langle v_i \rangle$ فضای تولید شده توسط بردار v_i باشد. واسطه بردار $v_i \in \mathbb{Z}_q^d$ را برای عدد مثبت d به هر سهامدار P_i نسبت می‌دهد به طوری که

$$\bigcap_{A \in \Gamma_j^-} \sum_{i \in A} V_i - \bigcup_{B \in \Delta_j^+} \sum_{i \in B} V_i \neq \emptyset$$

- واسطه تابع $\psi(i) = P_i$ و ماتریس $M_{n \times d}$ را $[m_{ij}]$ در نظر می‌گیرد.

- واسطه بردار هدف‌های دلخواه $e_j = (e_{j1}, \dots, e_{jd}) \in \mathbb{Z}_q^d$

$$\bigcap_{A \in \Gamma_j^-} \sum_{i \in A} V_i - \bigcup_{B \in \Delta_j^+} \sum_{i \in B} V_i$$

را برای $1 \leq j \leq m$ انتخاب می‌کند.

۳. واسطه بردار تصادفی $r = (r_1, \dots, r_d)^T$ را طوری انتخاب می‌کند که

$$\begin{cases} e_1 \cdot r = \sum_{i=1}^d e_{1i} r_i = k_1 \\ e_2 \cdot r = \sum_{i=1}^d e_{2i} r_i = k_2 + f(k_1) \\ \vdots \\ e_m \cdot r = \sum_{i=1}^d e_{mi} r_i = k_m + f(k_{m-1}) \end{cases}$$

وی همچنین تابع یک طرفه $f(x)$ را در نظر می‌گیرد.

اثبات. به روش کاهش انجام می‌شود. فرض کنید A_2 یک مهاجم در برابر امنیت محاسباتی طرح MSSST2 خطی Ω که در بالا توصیف شد، باشد. در ادامه یک مهاجم A_1 به امنیت طرح رمزنگاری کلید خصوصی Γ در برابر حملات استراق سمع چندتایی ساخته می‌شود که از A_2 به صورت زیر استفاده می‌کند:

۱. یک بیت تصادفی $\beta \in \{0,1\}$ توسط چالشگر بازی G انتخاب می‌شود.

• بازی G_2 توسط مهاجم A_2 با انتخاب مجموعه سهامداران P و m ساختار دسترسی $\Gamma_1, \dots, \Gamma_m$ به طوری که $\Gamma_i \subseteq \Gamma_{i-1}$ برای $2 \leq i \leq m$ شروع می‌شود.

• A_1 به عنوان چالشگر بازی G_2 عمل کرده، عدد اول $q > n$ را انتخاب می‌کند و $pms = (q, \Pi, P, \Gamma_1, \dots, \Gamma_m)$ را به A_2 می‌فرستد.

• A_2 یک زیرمجموعه $B \subset P$ به طوری که $|B| = t^*$ از سهامداران فاسد را منتشر می‌کند.

• دو راز عمومی متفاوت $s^0 = (s_1^0, \dots, s_m^0) \neq s^1 = (s_1^1, \dots, s_m^1)$ به طوری که برای هر i که $B \in \Gamma_i$ داشته باشید:

$$s_i^0 = s_i^1$$

توسط A_2 انتخاب و منتشر می‌شوند.

قرار دهید $I^* = \{i \in \{1, \dots, m\} \mid s_i^0 = s_i^1\}$.

بنابراین اگر $B \in \Gamma_i$ ، آنگاه $i \in I^*$.

• الگوریتم $\text{Gen}(1^\lambda)$ توسط A_1 اجرا شده و $|I^*|$ کلید محرمانه $k_1, \dots, k_{|I^*|}$ تولید می‌شوند.

• A_1 یک تابع یک طرفه $f(x)$ و $\text{MSP}(\mathbb{Z}_q, M, \psi, m)$ را در نظر می‌گیرد.

• بردارهای تصادفی $r = (r_1, \dots, r_d)^T$ توسط A_1 انتخاب می‌شوند به طوری که در رابطه زیر صدق کنند:

$$\text{برای } 2 \leq i \leq |I^*|$$

$$e_i \cdot r = k_i + f(s_{i-1}^0)$$

• سهم هر سهامدار P_j برابر با $r \cdot M_j = \text{sh}_j$ توسط A_1 محاسبه شده و به او ارسال می‌شود.

• یک عنصر اولیه $g \in \mathbb{Z}_q$ توسط A_1 انتخاب شده و g^{r_i} برای $2 \leq i \leq d$ منتشر می‌شوند.

• مقادیر A_1 $N_j = g^{\text{sh}_j}$ را برای $1 \leq j \leq n$ و $c_i = \text{Enc}(k_i, s_i)$ را برای $2 \leq i \leq |I^*|$ محاسبه می‌کند.

۳-۴-۲- بازسازی راز s_i ، $i \neq 1$

مجموعه مجاز $A_2 = \{P_1, \dots, P_t\} \in \Gamma_i$ را در نظر بگیرید اعضای این مجموعه در مرحله t ام، پس از بازسازی رازهای قبلی، برای راز s_i به روش زیر عملی می‌کنند:

۱. برای بردار هدف $\sum_{j \in A} V_j$ ، $e_i \in \cap_{A \in \Gamma_i} V_j$ بردار $\omega_{A_2} = (\omega_1, \dots, \omega_t)$ در \mathbb{Z}_q^t وجود دارد که در رابطه زیر صدق می‌کند:

$$\omega_{A_2} \cdot M_{A_2} = e_i \quad (5)$$

۲. قرار دهید $sh_j^* := \omega_j sh_j = (\omega_j M_j) \cdot r$.

۳. هر سهامدار $P_j \in A_2$ ، یک عدد صحیح تصادفی κ_j را انتخاب می‌کند. سپس شبه سهم خود یعنی $sh_j^i = sh_j^* + \kappa_j$ را به همراه $K_j = g^{\kappa_j}$ منتشر می‌کند.

۴. اعضای مجموعه A_2 ، مقدار $K := \kappa_1 + \dots + \kappa_t$ را بر اساس محاسبات چند بخشی محاسبه می‌کنند.

۵. هر سهامدار P_i با استفاده از معادله زیر قادر به تصدیق صحت سهم سهامدار P_j ، $(i \neq j)$ می‌باشد:

$$(6)$$

$$g^{(\kappa_j + sh_j^*)} = (N_j)^{\omega_j} K_j \pmod{q}$$

۶. سهامداران عضو مجموعه A_2 ، مقدار k_i را با استفاده از معادله زیر محاسبه می‌کنند:

$$\left(\sum_{P_j \in A_1} sh_j^i \right) - K - f(s_{i-1}) = k_i \quad (7)$$

سپس با استفاده از مقدار عمومی c_i ، راز $s_i = \text{Dec}(c_i, \kappa_i)$ به دست می‌آورند.

۳-۵- امنیت

در قضیه بعدی امنیت محاسباتی طرح ارائه شده را بر مبنای امنیت سامانه رمزنگاری متقارن Γ اثبات می‌شود.

قضیه: برای هر مهاجم A_2 به امنیت طرح Ω در برابر حمله راز منتخب، که t^* سهامدار فاسد از میان مجموعه P متشکل از n سهامدار و رازهای عمومی

$$s^0 = (s_1^0, \dots, s_m^0) \neq (s_1^1, \dots, s_m^1) = s^1$$

را انتخاب می‌کند، یک $(m - t^*, m - t)$ -مهاجم A_1 به امنیت طرح رمزنگاری کلید خصوصی Γ در برابر حمله استراق سمع وجود دارد به طوری که

$$\Pr [MSSS_{A_2}^{CSA}(\lambda) = 1] = \Pr [PrivK_{A_1}^{M.Eav}(\lambda) = 1]$$

• از آنجایی که سهامداران از شبه سهم‌های خود یعنی $sh_j^* + \kappa_j$ در مرحله بازسازی استفاده می‌کنند، سهم واقعی آن‌ها یعنی sh_j حتی بعد از بازسازی راز نیز پنهان می‌ماند. بنابراین طرح ما یک تسهیم راز چند بار مصرفی است.

• چون همه می‌توانند صحت شبه سهم ارائه شده توسط یک سهامدار را بررسی کنند، هیچ سهامداری قادر به تقلب کردن نخواهد بود.

• امکان تقلب کردن برای واسطه نیز وجود ندارد چون سهامداران می‌توانند صحت سهم خود را بررسی کنند.

• یک ترتیب برای بازسازی رازها از پیش توسط واسطه تعیین می‌شود و رازها بر اساس آن و در مراحل جداگانه بازسازی می‌شوند. این ویژگی بسیار کاربردی است. به عنوان مثال، ممکن است سامانه امنیتی یک بانک به گونه‌ای طراحی شده باشد که هر فرد برای دسترسی به پایگاه داده محرمانه مجبور به عبور از α پست بازرسی باشد. به علت سیاست امنیتی، عبور از هر پست بازرسی تنها در صورت حضور هم‌زمان یک زیرمجموعه مجاز از شرکت کنندگان ممکن است. اگر پست‌های بازرسی (رازها) به ترتیب طی نشوند به امنیت سامانه آسیب وارد می‌شود.

• طرح ما دارای این ویژگی بسیار کاربردی می‌باشد که همه سهامداران دارای قدرت برابر و یا احتمال یکسان برای خلافتکار بودن نیستند.

• نویسندگان طرح‌های MSS خطی قبلی برای طرح‌هایشان اثبات امنیت ارائه نکرده بودند اما طرح ما دارای امنیت تمایزناپذیری در برابر حملات راز منتخب در مدل استاندارد است.

در جدول (۲) طرح مان را با طرح‌های MSS خطی [۳۱-۳۰، ۳۸] با در نظر گرفتن پیچیدگی محاسباتی مقایسه شده است. برای راحتی از نمادهای زیر در تحلیل پیچیدگی محاسباتی استفاده شده است:

- T_f زمان لازم برای محاسبه یک تابع یک طرفه است.
- T_m زمان لازم برای محاسبه یک عملیات ضرب است.
- T_e زمان لازم برای محاسبه یک عملیات به توان رساندن است.
- T_i زمان لازم برای محاسبه یک معکوس است.

۲. A_1 ، تعداد کلیدها را در بازی G برابر با $|I^*| - \tau = m$ در نظر می‌گیرد.

۳. الگوریتم $\text{Gen}(1^\lambda)$ توسط چالشگر بازی G ، τ مرتبه اجرا شده و τ کلید محرمانه $k_{|I^*|+1}, \dots, k_m$ تولید می‌شوند.

۴. سه تایی‌های (i, s_i^0, s_i^1) برای $i = |I^*| + 1, \dots, m$ توسط A_2 انتخاب شده و به A_1 ارسال می‌شوند.

۵. الگوریتم $\text{Enc}(k_i, s_i^b)$ $c_i \leftarrow$ توسط چالشگر اجرا شده و خروجی آن برای $i = |I^*| + 1, \dots, m$ به A_2 ارسال می‌شود.

• A_1 ، مقادیر عمومی $\text{Out}_{pub} = \{c_2, \dots, c_m, N_1, \dots, N_n, g^{r_1}, \dots, g^{r_d}\}$ را منتشر کرده و سهم اعضای مجموعه B به A_2 ارسال می‌کند. به این ترتیب A_1 ، در واقع پروتکل توزیع $\text{Dist}(pms, s^b) \leftarrow (\{sh_i\}_{P_i \in P}, \text{Out}_{pub})$ را برای $b = \beta$ شبیه‌سازی می‌کند.

• A_2 یک بیت $b' \in \{0, 1\}$ را به عنوان خروجی نهایی می‌دهد (بازی G_2).

۶. A_1 همان بیت $b' = \beta'$ را به عنوان خروجی نهایی اش می‌دهد (بازی G).

بنابراین داریم:

$$\Pr[\text{PrivK}_{A_1}^{MEav}(\lambda) = 1] = \Pr[b' = \beta] = \Pr[b' = b] = \Pr[\text{MSSS}_{A_2}^{CSA}(\lambda) = 1]$$

تساوی دوم به علت $b' = \beta'$ و $\beta = b$ برقرار است و این اثبات را کامل می‌کند.

۳-۶- ویژگی چند بار مصرفی

طرح ارائه شده دارای ویژگی چند بار مصرفی می‌باشد زیرا هر سهامدار P_j ، در مرحله بازسازی هر کدام از رازهای s_i ، شبه سهم خود یعنی $sh_j^* = sh_j^* + \kappa_j$ را ارائه می‌کند. او می‌تواند برای بازسازی رازهای دیگر همچنان از sh_j استفاده کند زیرا به دلیل امنیت MSP ، sh_j^* هرگز فاش نخواهند شد.

۳-۷- مقایسه با طرح‌های دیگر

در جدول (۱) می‌توانید جزئیات مقایسه طرح MSSST2 ارائه شده در این مقاله [۳۳] را با طرح‌های تسهیم راز دیگر [۳۱-۳۰، ۳۸-۴] مشاهده کنید. ویژگی‌های اساسی طرح ما شامل موارد زیر می‌باشد:

۴- طرح MSS بر اساس مسئله LWE

در ادامه یک طرح جدید تسهیم چند راز آستانه‌ای $\Omega = (Stp, Dist, Rec)$ با آستانه t ارائه شده است. امنیت طرح بر اساس سختی مسئله LWE می‌باشد. در این طرح، m راز $s_1, \dots, s_m \in \mathbb{Z}_q$ برای عدد صحیح q توسط واسطه D در میان سهامداران P_1, \dots, P_n توزیع می‌شود. طرح مورد نظر یک طرح آستانه‌ای با آستانه $n \geq t \geq 2$ بوده و بنابراین حضور حداقل t شرکت کننده برای بازسازی رازها لازم است.

جدول (۲): پیچیدگی محاسباتی طرح‌های MSS خطی

مرحله	[۵]	[۳۰]	[۴, ۳۱]	[۳۳]
برپایی	$(t+1)T_m$	-	$ A nT_m$	$(m-1)T_f$
توزیع	$2ntT_m$	ndT_m	nT_m	$ndT_m + (d+n)T_e$
تصدیق	$(n+1)t(T_e + T_m)$	-	-	$d(T_e + T_m)$
بازسازی	$t(t+1)T_m$	$n A T_m$	$ A T_m$	$ A T_e + 2T_i$

۴-۱- مرحله برپایی

راز $s = (s_1, \dots, s_m) \in \mathbb{Z}_q^m$ را در نظر بگیرید. فرض کنید واسطه توزیع احتمال $\chi \in \mathbb{Z}_q$ را برای بردار خطا در نظر بگیرید. پارامترهای این طرح مشابه با پارامترهای مسئله LWE می‌باشند.

۴-۲- مرحله توزیع

واسطه سهام‌های شرکت کنندگان را به روش زیر محاسبه می‌کند: برای هر $1 \leq i \leq n$,

۱. عددهای $e_i \in \mathbb{Z}_q$ ، $1 \leq i \leq n$ را بر اساس توزیع احتمال خطای χ انتخاب می‌کند.

فرض کنید R مجموعه تمام ترکیب‌های t تایی ممکن از اعداد e_i برای $1 \leq i \leq n$ باشد که $|R| = \binom{n}{t}$.

$$R = \{\alpha_k := (e_{k1}, \dots, e_{kt}), 1 \leq k \leq \binom{n}{t}\}$$

واسطه ماتریس $M = [m_{kj}]_{\binom{n}{t} \times \binom{n}{t}}$ را به صورت زیر در نظر می‌گیرد:

$$M = \begin{bmatrix} \alpha_1 & \sum_{j=1}^t e_{j1} & \circ & \dots & \circ \\ \alpha_2 & \circ & \sum_{j=1}^t e_{j2} & \dots & \circ \\ \vdots & \vdots & \vdots & \dots & \circ \\ \alpha_{\binom{n}{t}-t} & \circ & \circ & \ddots & \sum_{j=1}^t e_{j(\binom{n}{t}-t)} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ \alpha_{\binom{n}{t}} & \circ & \circ & \dots & \circ \end{bmatrix}_{\binom{n}{t} \times \binom{n}{t}}$$

جدول (۱): مقایسه با طرح‌های تسهیم راز خطی			
ویژگی	[۴, ۳۰-۳۱]	[۵]	ما [۳۳]
طبقه‌بندی طرح‌های خطی	MSS	SS	MSS
طبقه‌بندی طرح‌های	MSSST1	-	MSSST2
سهام‌ها چند بار مصرف بوده و پس از بازسازی قابلیت استفاده مجدد دارند.	خیر	خیر	بله
رازها با ترتیب از پیش تعیین شده بازسازی می‌شوند.	خیر	خیر	بله
ترتیب بازسازی رازها	دلخواه	دلخواه	از پیش تعیین شده
ساختار دسترسی عمومی	بله	بله	بله
قابلیت تصدیق واسطه را دارد	خیر	بله	بله
قابلیت تصدیق سهامداران را دارد	خیر	بله	بله
نیاز به کانال امن دارد	بله	بله	بله
دارای امنیت تمایزناپذیری در برابر حملات راز منتخب است	خیر	خیر	بله
نوع امنیت	بی‌قید و شرط	بی‌قید و شرط	محاسباتی

همچنین ماتریس $\bar{M} = [\bar{m}_{kj}]_{\binom{n}{t} \times \binom{n}{t}}$ را به صورت زیر در نظر می‌گیرد:

(الف) برای $1 \leq j \leq t$ ، اگر $m_{kj} = e_{ik}$ آنگاه $\bar{m}_{kj} := i$

(ب) برای $t < j \leq \binom{n}{t}$ ، اگر $m_{kj} \neq 0$ آنگاه $\bar{m}_{kj} := 1$

موجود است را انتخاب کنند اما برای محاسبه $|M|$ نسبت به هر کدام از آن سطرها، وجود دترمینان ماتریس کهاد نسبت به یک درایه t ام ضروری است که در سهم‌های هیچ کدام از آن‌ها نیست. بنابراین آن‌ها به هیچ روشی توانایی محاسبه $|M|$ و در نتیجه حذف بردار خطای $|M| \sum_{i=1}^t e_i$ را ندارند و برای بازسازی راز s ناچار به حل مسئله LWE می‌باشند.

۴-۵- مقایسه با طرح‌های مشبکه مبنای دیگر

در ادامه ویژگی‌های اساسی طرح مان را با طرح‌های تسهیم راز مشبکه مبنای دیگر [۳۹-۴۱، ۲۶] مقایسه می‌شود. جزئیات این مقایسه در جدول (۳) آمده است. این طرح‌ها بر اساس مسئله کوتاه‌ترین بردار (SVP)، مسئله یافتن عدد صحیح کوچک (SIS)، مسئله کوچک‌ترین چندجمله‌ای (SPP) و یادگیری با خطا طراحی شدند. طرحی که ارائه شد دارای ویژگی‌های زیر می‌باشد:

- امکان توزیع و بازسازی چندین راز به صورت هم‌زمان وجود دارد و نیازی به توزیع و بازسازی هر یک از رازها در یک مرحله جداگانه نیست.
- سهامداران قادرند با اطلاعات عمومی اعلام شده توسط واسطه در مرحله توزیع درستی سهم خود و سایرین را بررسی کنند و نیازی به تعامل مجدد با واسطه ندارند.
- ایده طرح بر اساس مسئله سخت جدیدی از مشبکه‌ها است.
- نیازی به حضور تمام سهامداران در بازسازی نیست.

جدول (۳): مقایسه با طرح‌های تسهیم راز مشبکه مینا

طرح جدید	[۲۶]	[۴۱]	[۴۰]	[۳۹]	طرح خصیت
تصدیق	تصدیق	تصدیق	تصدیق	تصدیق	تصدیق
مسئله	LWE	SPP	SVP	SIS	مسئله
امنیت	محاسباتی	محاسباتی	محاسباتی	محاسباتی	امنیت
چند مرحله ای	خیر	خیر	بله	بله	چند مرحله ای
آستانه‌ای $t < n$	خیر	بله	بله	بله	آستانه‌ای $t < n$

۵- نتیجه‌گیری

امروزه با ظهور کامپیوترهای کوانتومی طراحی طرح‌هایی که بتوانند امن باشند بسیار مهم است. ما در این مقاله دو طرح تسهیم راز پیشنهاد کردیم. طرح تسهیم راز اول دارای امنیت استاندارد است ولی در برابر حملات کوانتومی مقاوم نیست. اما

۲. بردارهای a_i را به‌طور یکنواخت از \mathbb{Z}_q^m انتخاب کرده و سهم $sh_i := (a_i, a_i s + e_i | M |, e_i, \{ | M_{kj} | : m_{kj} = e_i, 1 \leq j \leq t \})$ را از طریق یک کانال خصوصی به شرکت کننده P_i ارسال می‌کند. منظور از $| M_{kj} |$ دترمینان ماتریس کهاد M_{kj} است.

۳. واسطه ماتریس \bar{M} و همچنین $| M_{ij} |$ را برای $\bar{m}_{ij} = 1$ و $t \leq j \leq \binom{n}{t}$ منتشر می‌کند.

او همچنین یک تابع چکیده ساز انتخاب کرده و پس از محاسبه $sh_j^* := H(a_i || b_i + \sum_{M_{kj}=e_j} | M_{kj} |)$ برای $b_i := a_i s + e_i | M |$ را منتشر می‌کند.

۴-۳- مرحله تصدیق و بازسازی

فرض کنید مجموعه مجاز $A = \{P_1, \dots, P_t\}$ از t سهامدار $(2 \leq t \leq n)$ ، قصد بازسازی رازها را دارند. مرحله بازسازی به همراه تصدیق سهم‌ها به روش زیر انجام می‌شود:

۱. هر سهامدار $P_i, 1 \leq i \leq t$ ، می‌تواند صحت سهم خود را با محاسبه $(a_i || b_i + \sum_{M_{kj}=e_i} | M_{kj} |)$ و مقایسه آن با sh_i^* تصدیق کند. سهامداران همچنین بعد از اعلام سهم هر شرکت کننده دیگری مانند P_j می‌توانند صحت سهم او را با محاسبه $(a_j || b_j + \sum_{M_{kj}=e_j} | M_{kj} |)$ و مقایسه آن با sh_j^* تصدیق کنند.
۲. پس از تصدیق سهم‌ها، مرحله بازسازی به صورت زیر انجام می‌شود:

ابتدا سهامداران عضو مجموعه A ، با بررسی ماتریس \bar{M} سطری که در آن اعداد $t, 1, 2, \dots$ یعنی شناسه آنهاست را پیدا کرده و $| M |$ را از طریق بسط دترمینان نسبت به همان سطر محاسبه می‌کنند. سپس با کم کردن $| M | e_i$ از دومین مولفه سهم خود، $a_i s$ را محاسبه می‌کنند. بنابراین با حل یک دستگاه با داشتن مقادیر $a_i s$ و a_i مقدار راز s را بدست می‌آورند.

۴-۴- امنیت

در ادامه می‌بینید که اگر هر زیرمجموعه‌ای از سهامداران با کمتر از t عضو سعی کنند راز s را بازسازی کنند، ناچار به حل مسئله LWE خواهند شد.

قضیه: در طرح پیشنهاد شده، هر زیرمجموعه از سهامداران با تعداد اعضای کمتر از t قادر به بازسازی راز s نمی‌باشد.

اثبات. بدون خلی به کلیت فرض کنید سهامداران مجموعه $A = \{P_1, \dots, P_{t-1}\}$ قصد بازسازی راز s را دارند. آن‌ها می‌توانند یکی از سطرهاى ماتریس \bar{M} که اعداد $1, 2, \dots, t-1$ در آن

- Security," *Inf. Proc. Lett.*, 113, pp. 572–579, 2013.
- [16] S. Mashhadi, "How to Fairly Share Multiple Secrets Stage by Stage", *Wirel. Pers. Commun.*, 90, pp. 93–107, 2016.
- [17] L. J. Pang, Y. M. Wang, "A New (t, n) Multi-Secret Sharing Scheme Based on Shamir's Secret Sharing," *Applied Mathematics and Computation*, vol. 167, pp. 840-848, 2005.
- [18] T. Y. Chang, M. S. Hwang, W. P. Yang, "A New Multi-Stage Secret Sharing Scheme Using One-Way Function," *ACM SIGOPS Oper. Syst.*, 39, pp. 48–55, 2005.
- [19] J. He, E. Dawson, "Multistage Secret Sharing Based on One-Way Function," *Electron. Lett.*, vol. 30, pp. 1591–1592, 1994.
- [20] H. X. Li, C. T. Cheng, L. J. Pang, "An Improved Multi-Stage (t, n)-Threshold Secret Sharing Scheme," *WAIM*, (LNCS, 3739), pp. 267–274, 2005.
- [21] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proc. of the 35th Annual Symposium on Foundations of Computer Science*, Washington, DC, USA: IEEE Computer Society, pp. 124-134, 1994.
- [22] R. J. McEliece, "A Public-Key Cryptosystem Based on Algebraic Coding Theory," *DSN Progress Report*, vol. 42, no. 44, pp. 114-116, 1978.
- [23] D. Bernstein, J. Buchmann, E. Dahmen, "Post-Quantum Cryptography," Springer, 2009.
- [24] M. Ajtai, "Generating Hard Instances Of Lattice Problems (Extended Abstract)," *Proc. of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, New York, NY, USA: ACM, pp. 99-108, 1996.
- [25] O. Goldreich, S. Goldwasser, S. Halevi, "Public-key Cryptosystems from Lattice Reduction Problems," *Advances in Cryptology CRYPTO 97*, ser. Lecture Notes in Computer Science, J. Kaliski, Burton S., Ed. Springer Berlin Heidelberg, vol. 1294, pp. 112-131, 1997.
- [26] Georgescu, "A Lwe-Based Secret Sharing Scheme," *IJCA Special Issue on Network Security and Cryptography*, no. 3, pp. 27-29, December, published by Foundation of Computer Science, New York, USA, 2011.
- [27] R. El Bansarkhani, M. Meziari, "An Efficient Lattice-Based Secret Sharing Construction," *Information Security Theory and Practice. Security, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems*, ser. Lecture Notes in Computer Science, I. Askoxylakis, H. Phls, and J. Posegga, Eds. Springer Berlin Heidelberg, vol. 7322, pp. 160-168, 2012.
- [28] J. Shao, Z. F. Cao, "A New Efficient (t, n) Verifiable Multi-Secret Sharing (VMSS) Based on YCH Scheme," *Applied Mathematics and Computation*, 168, pp. 135–140, 2005.
- [29] M. Tadayon, H. Khanmohammadi, M. Haghghi, "Dynamic and Verifiable Multi-Secret Sharing

طرح دوم شبکه میناست و در برابر حملات کوانتومی مقاومت می کند.

۶- مراجع

- [1] A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.
- [2] G. Blakley, "Safeguarding Cryptographic Keys," *In Proc. AFIPS 1979 National Computer Conf.*, pp. 313–317, June 1979.
- [3] Z. Eslami, S. Kabiri Rad, "A New Verifiable Multi-Secret Sharing Scheme Based on Bilinear Maps," *Wirel. Pers. Commun.*, 63, pp. 459–467, 2012.
- [4] Ch. Hsu, Q. Cheng, X. Tang, et al, "An Ideal Multi-Secret Sharing Scheme Based on MSP," *Inf. Sci.*, 181, pp. 1403–1409, 2011.
- [5] J. Zhang, F. Zhang, "Information-theoretical Secure Verifiable Secret Sharing with Vector Space Access Structures over Bilinear Groups and its Application," *Future Gener. Comput. Syst.* 52, pp. 109–115, 2015.
- [6] M. Ben-Or, Sh. Goldwasser, A. Wigderson, "Completeness Theorems for Non-cryptographic Fault-Tolerant Distributed Computation (Extended Abstract)," *STOC*, pp. 1–10, 1988.
- [7] D. Chaum, C. Crepeau, I. Damgard, "Multiparty Unconditionally Secure Protocols (Extended Abstract)," *STOC*, pp. 11–19, 1988.
- [8] B Chor, Sh. Goldwasser, S Micali, B. Awerbuch, "Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults (Extended Abstract)," *FOCS*, pp. 383–395, 1985.
- [9] C. Ma, X. Ding, "Proactive Verifiable Linear Integer Secret Sharing Scheme," *Information and Communications Security*, (LNCS, 5927), pp. 439–448, 2009.
- [10] S. Mashhadi, M. Hadian, "Two Verifiable Multi Secret Sharing Schemes Based on Nonhomogeneous Linear Recursion and LFSR Public-Key Cryptosystem," *Inf. Sci.*, 294, pp. 31–40, 2015.
- [11] T. S. Wu, Y. M. Tseng, "Publicly Verifiable Multi-Secret Sharing Scheme from Bilinear Pairings," *IET Inf. Sec.*, 7, pp. 239–246, 2013.
- [12] C. Lin, L. Harn, "Unconditionally Secure Verifiable Secret Sharing Scheme," *AISS: Adv. Inf. Sci. Serv. Sci.*, 4, pp. 514–518, 2012.
- [13] D. R. Stinson, R. Wei "Unconditionally Secure Proactive Secret Sharing Scheme with Combinatorial Structures, Selected Areas in Cryptography," *Selected Areas in Cryptography: SAC'99*, (LNCS, 1758), pp. 200–214, 2000.
- [14] M. Fatemi, R. Ghasemi, T. Eghlidos, M. R. Aref, "Efficient Multistage Secret Sharing Scheme Using Bilinear Map," *IET Inf. Sec.*, 8, pp. 224–229, 2014.
- [15] J. Herranz, A. Ruiz, G. Sáez, "Sharing Many Secrets with Computational Provable

- Structure in Complexity, San Diego, CA, pp. 102-111, May 1993.
- [36] D. Micciancio, S. Goldwasser, "Complexity of Lattice Problems: A Cryptographic Perspective," Ser. Milken Institute Series on Financial Innovation and Economic Growth. Springer US, 2002. [Online]. Available: <http://books.google.com/books?id=N4IHIGwy1AUC>
- [37] O. Regev, "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography," J. ACM, 56(6):34:134:40, September 2009.
- [38] J. Hoffstein, J. Pipher, J. Silverman, Ntru "A Ring-Based Public Key Cryptosystem," Algorithmic Number Theory, Ser. Lecture Notes in Computer Science, 1423, pp.267-288, 1998.
- [39] M.H. Dehkordi, R. Ghasemi, "A Lightweight Public Verifiable Multi Secret Sharing Scheme Using Short Integer Solution," In Wireless Personal Communications, Springer, pp. 1459–1469, 2016.
- [40] H. Pirlam, T. Eghlidos "An Efficient Lattice Based Multi-stage IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 1, pp.2-8, 2015.
- [41] B. Rajabi, Z. Eslami, "A Verifiable Threshold Secret Sharing Scheme Based on Lattices," Information Sciences, Vol. 501 pp.655–661, 2019.
- Scheme Based on Hermite Interpolation and Bilinear Maps," IET Inf. Sec., 9, pp. 234–239, 2015.
- [30] Ch. Hsu, L. Harn, G. Cui, "An Ideal Multi-Secret Sharing Scheme Based on Connectivity of Graphs," ۳۹۴-۳۸۳pp. , ۷۷Wireless Personal Communication, ۲۰۱۴
- [31] Ch. Hsu, G. Cui, Q. Cheng, J. Chen, "A Novel Linear Multi-Secret Sharing Scheme for Group Communication in Wireless Mesh Networks," Network and Computer Applications, 34, pp. 464-468, 2011.
- [32] M. Liu, L. Xiao, Z. Zhang, "Linear Multi-Secret Sharing Schemes Based on Multi-Party Computation," Finite Fields and Their Applications, vol. 12, pp.704-13, 2006.
- [33] S. Mashhadi, M. Hadian Dehkordi, N. Kiamari, "Provably Secure Verifiable Multi-Stage Secret Sharing Scheme Based on Monotone Span Program," IET Information Security, vol. 11, pp.326-331, 2017.
- [34] S. Mashhadi, "Computationally-Secure Multiple Secret Sharing: Models, Schemes, and Formal Security Analysis," The ISC Int. J. Inf. Sec., vol. 7, pp. 1–10, 2015.
- [35] M. Karchmer, A. Wigderson, "On Span Programs," In Proceedings of the Eighth Annual Conf. On

Two Verifiable Multi-Secret Sharing Schemes: A Linear Scheme with Standard Security and A Lattice-Based Scheme

M. Hadian Dehkordi*, S. Mashhadi, N. Kiamari

*Iran University of Science & Technology

(Received: 02/10/2019, Accepted: 01/02/2020)

ABSTRACT

In this paper, we present two verifiable multi-secret sharing schemes, including a linear multi-secret sharing scheme with public access structure and a threshold (t, n) scheme based on the learning with errors (LWE) problem. The first scheme is a linear multi-secret sharing scheme in which a number of secrets is distributed by a dealer among a set of participants according to the access structure corresponding to each secret. This scheme has the advantages of the earlier ones and it also has many practical applications compared to previous schemes including a multi-use verifiable multi-secret sharing scheme in which the secret reconstruction is according to the dealer's preassigned order. In addition, the security of the scheme has been proven in the standard model. This scheme is based on the hard problems in number theory and therefore is not secure against quantum attacks. The second scheme presented in this paper is a lattice-based secret sharing scheme. In this scheme, which is a threshold (t, n) multi-secret sharing scheme, the presence of at least t participants is required for the reconstruction of the secret. The security of this scheme is based on the difficulty of the LWE problem and so it is resistant against quantum attacks.

Keywords: Secret Sharing, Verifiability, Standard Security, Post-Quantum, Lattice, LWE Problem.

* Corresponding Author Email: mhadian@iust.ac.ir