Electronic and Cyber Defens 2025/ Vol. 13/ No. 2/ 35-44

Electronic and Cyber Defens

ISSN: 2322-4347 , E-ISSN: 2980-8979

A Threshold Secret Sharing Scheme Resistant to Quantum Attacks

P. Dalir Hassanjani[1], H. Daghigh[2*]

[1] PhD student, Faculty of Science, Kashan University, Kashan, Iran

[2] Associate Professor, Faculty of Science, Kashan University, Kashan, Iran ([*]Correspondence: hassan@kashanu.ac.ir)

ARTICLE INFO

Article history:

Article Type: Research paper

Received: 18 April 2025

Revised: 27 May 2025

Accepted: 08 June 2025

Available online: 28 June 2025

Keywords:

Secret Sharing Scheme

Lattice

With Errors

Ring Learning

Cryptosystem

Lindner-Peikert

Hash Function

ABSTRACT

In this paper, a new verifiable secret sharing scheme is presented. This scheme uses the idea used by Lindner-Peikert in his well-known cryptosystem. The security is based on the Ring Learning With Error (RLWE) problem, which is an algebraic variant of the Learning With Error (LWE) problem, and is believed to be quantum resistant. Our new scheme does not require any secure channel.

Cite this article: Dalir Hassanjani, P.©, Daghigh, H.© (2025). A Threshold Secret Sharing Scheme Resistant to Quantum Attacks. Journal of Electronic and Cyber Defens. 2025; 13l(2):35-44.
DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.2.4.1

Publisher: Imam Hossein University.

پدافند الکترونیک و سایبری/ سال ۱۴۰۴/ دوره ۱۳/ شماره ۲/ صفحه ۴۴-۳۵

پدافند الکترونیک و سایبری

شاپا الکترونیکی: ۴۳۴۷- ۲۳۲۲۲ شاپا چاپی: ۸۹۷۹-۲۹۸۰

یک طرح تسهیم راز آستانه‌ای مقاوم در برابر حملات کوانتومی

پریسا دلیری حسن جانی[۱]، حسن دقیق[۲*]

[۱] دانشجوی دکتری، دانشکده علوم، دانشگاه کاشان،کاشان، ایران (parisa.daliri@grad.kashanu.ac.ir)

[۲] دانشیار، دانشکده علوم، دانشگاه کاشان، ایران (نویسنده مسئول: hassan@kashanu.ac.ir)

چکیده

یکی از مسائل مهم رمزنگاری، آسیب‌پذیری طرح‌های تسهیم راز در برابر حملات کوانتومی است. این مقاله، یک طرح تسهیم راز تأییدپذیر با استفاده از سامانه رمزنگاری پساکوانتومی لیندنر-پایکرت را معرفی کرده است. امنیت این طرح به دلیل استفاده از سامانه رمزنگاری پساکوانتومی لیندنر-پایکرت در برابر حملات کوانتومی تأییدشده است. این طرح بر اساس مسئله یادگیری با خطا در حلقه استوار است که نسخه جبری مسئله یادگیری با خطا است. به‌طوری‌که پارامترها از یک حلقه چندجمله‌ای با استفاده از توزیع گاوسی انتخاب‌شده‌اند. ازآنجاکه تمامی پارامترهای کلید عمومی و سهام در برابر حملات کوانتومی مقاوم هستند، در این طرح به کانال امن نیازی نیست.

مشخصات مقاله

تاریخچه مقاله:

نوع مقاله: علمی پژوهشی

دریافت: ۱۴۰۴/۱/۲۹

بازنگری: ۱۴۰۴/۳/۶

پذیرش: ۱۴۰۴/۳/۱۸

ارائه آنلاین: ۱۴۰۴/۴/۷

کلید واژه‌ها:

پایدارسازی غیرفعال

آفرود

شرایط سخت

مشبکه

تابع چکیده ساز

مسئله یادگیری با خطای حلقه‌ای

استناد: دلیری حسن جانی، پریسا ©، دقیق، حسن©. یک طرح تسهیم راز آستانه‌ای مقاوم در برابر حملات کوانتومی. پدافند الکترونیک و سایبری. (۱۴۰۴)؛ ۱۳ (۲): ۴۴-۳۵. DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.2.4.1

ناشر: دانشگاه جامع امام حسین(ع).

۱- مقدمه

تسهیم راز، فرایندی است که در آن‌یک یا چند راز توسط واسطه یا توزیع‌کننده به اشتراک گذاشته می‌شود، به‌گونه‌ای که زیرمجموعه‌های مشخص از پیش تعیین‌شده قادر به بازسازی راز هستند، درحالی‌که سایر زیرمجموعه‌ها نمی‌توانند راز را بازسازی کنند. زمانی که تعداد سهام‌داران هر زیرمجموعه از پیش تعیین‌شده بزرگ‌تر یا مساوی مقداری باشد که به آن حد آستانه گفته می‌شود، به این روش تسهیم راز آستانه‌ای می‌گویند. درواقع، راز بین سهام‌داران به‌گونه‌ای توزیع می‌شود که تنها زیرمجموعه‌هایی با تعداد سهام‌دارانی برابر یا بیشتر از حد آستانه قادر به بازسازی راز باشند، اما زیرمجموعه‌هایی با تعداد کمتر از حد آستانه نمی‌توانند به راز دسترسی پیدا کنند.طرح تسهیم راز آستانه‌ای اولین بار توسط شامیر [۱] و بلکلی [۲] به‌طور مستقل معرفی شد. طرح شامیر بر اساس درون‌یابی چندجمله‌ای لاگرانژ روی میدان‌های متناهی و طرح بلکلی بر پایه هندسه متناهی است.

طرح شامیر پس از معرفی، دارای محدودیت‌هایی مانند عدم‌تشخیص فریب واسطه و سهام‌داران و نیاز به استفاده از کانال خصوصی بود.

بنابراین، طرح‌های تسهیم راز تأیید پذیر معرفی شدند. در این طرح‌ها، واسطه سهام را به‌صورت عمومی منتشر می‌کند تا هر سهام‌دار بتواند پس از دریافت سهم خود از صحت آن اطمینان حاصل کند. همچنین، سهام‌داران پس از بازسازی راز قادر به تأیید درستی آن خواهند بود. به‌این‌ترتیب، احتمال تقلب سهام‌داران و واسطه بررسی می‌شود.

چام و ژانگ [۳] یک طرح تسهیم راز ساده مبتنی بر تابع چکیده ساز پیشنهاد کردند و آن را به نسخه تأیید پذیر گسترش دادند. این طرح، به دلیل استفاده از تابع چکیده ساز، از سرعت بالایی برخوردار بود؛ بااین‌حال، نتوانست تمام ایرادات طرح شامیر را برطرف کند.

دس و ادهیکاری [۴] طرح تسهیم چند راز تأیید پذیر مبتنی بر تابع چکیده ساز را پیشنهاد کردند. در این طرح، بیش از یک راز میان سهام‌داران توزیع می‌شود، به‌طوری‌که به هر سهام‌دار تنها یک سهم اختصاص داده می‌شود. همچنین، به دلیل استفاده از تابع چکیده ساز، از سرعت بالایی برخوردار است.

در این طرح، تقلب سهام‌داران قابل‌شناسایی است، اما تقلب واسطه قابل‌تشخیص نیست. علاوه بر این، از کانال خصوصی برای انتقال سهام استفاده می‌شود. شائو [۵] نیز طرح تسهیم چند راز تأیید پذیر مبتنی بر تابع چکیده ساز را معرفی کرد که در آن ادعاشده است تقلب واسطه قابل‌شناسایی است.

طرح تسهیم راز چند گامی و چند استفاده بر اساس تابع چکیده ساز توسط فرهادی و همکاران [۶] معرفی‌شده است. در این نوع طرح، چند راز بین گروهی از سهام‌داران به اشتراک گذاشته می‌شود. این طرح در برابر تقلب سهام‌داران مقاوم است؛ بااین‌حال، برای ارتباط واسطه با سهام‌داران به یک کانال امن نیاز دارد.

پیشرفت‌های اخیر در ساخت رایانه‌های کوانتومی تهدیدی جدی برای امنیت الگوریتم‌های رمزنگاری است که امنیت آن‌ها بر پایه سختی مسائل لگاریتم گسسته و تجزیه اعداد صحیح استوار است. شور [۷] الگوریتم کوانتومی‌ای ارائه کرد که قادر به شکستن بسیاری از الگوریتم‌های رمزنگاری کلاسیک بود. این امر نیاز به تحقیق درزمینهٔ الگوریتم‌های پساکوانتومی را به وجود آورد؛ الگوریتم‌هایی که در برابر حملات کوانتومی مقاوم بوده و در رایانه‌های غیر کوانتومی نیز قابل‌اجرا باشند.

اولین سامانه رمزنگاری پساکوانتومی توسط مک الیس [۸] معرفی شد، که یک طرح رمزنگاری کلید عمومی مبتنی بر سختی مسئله کد است.

در فرآیند استانداردسازی موسسه ملی استانداردها و فنّاوری، به دلیل پیچیدگی، محاسبات کمتر، قابلیت تطبیق‌پذیری بالا و اثبات پذیری امنیت ، سامانه‌های رمزنگاری مبتنی بر مشبکه و مسئله یادگیری با خطا توجه بیشتری را به خود اختصاص داد.

در رمزنگاری مشبکه مبنا بررسی الگوریتم‌هایی که مبتنی بر مسائل سخت مشبکه هستند، پرداخته می‌شود.

نخستین الگوریتم رمزنگاری مبتنی بر مشبکه توسط آجتای [۹] ارائه شد.

با توجه به‌تازگی سامانه‌های رمزنگاری مبتنی بر یادگیری با خطا، بسیاری از مسائل مربوط به آن‌ها هنوز بهینه‌سازی نشده‌اند.

یک طرح تسهیم راز آستانه‌ای توسط جئورجسکو [۱۰] معرفی شد که امنیت آن مبتنی بر سختی مسئله یادگیری با خطا بوده و در آن تمامی سهام‌داران قادر هستند درستی راز را تأیید کنند. در این طرح، سهام‌داران با استفاده از مسئله لگاریتم گسسته صحت سهام‌هایشان را تأیید می‌کنند، اما این روش در برابر حملات کوانتومی آسیب‌پذیر است.

بنذرخانی [۱۱] طرح تسهیم راز آستانه‌ای تأیید پذیر بر پایه مشبکه‌ها را مطرح کرد که در آن برای تأیید سهام توسط سهام‌داران از یک تابع چکیده ساز مشبکه مبنا (آجتای) استفاده‌شده است.

طرح تسهیم راز آستانه‌ای (t, n) مبتنی بر مشبکه توسط اسعد و همکارانش [۱۲] معرفی شد. امنیت این طرح بر اساس سختی مسئله نزدیک‌ترین بردار در مشبکه است. ایرادات این طرح عدم‌تأیید پذیری آن و استفاده از کانال خصوصی جهت توزیع سهام‌ها است.

امینی و همکارانش [۱۳] طرح تسهیم راز آستانه‌ای (t, n) مبتنی بر سختی مسئله یادگیری با خطا را ارائه کردند، که ایرادات طرح اسعد همچنان بر این طرح نیز وجود داشت.

اگر در یک گروه متناهی بزرگ تعداد زیادی عنصر یکنواخت را

به‌صورت تصادفی در نظر بگیریم، هدف مسئله جواب صحیح کوتاه یافتن یک ترکیب خطی صحیح نا صفر از این عناصر است، به‌طوری‌که مجموع ترکیب‌های خطی برابر با صفر باشد. طرح تسهیم چند راز تأیید پذیر مبتنی بر مسئله جواب صحیح کوتاه نیز ارائه‌شده است [۱۴].

کیاماری و هادیان [۱۵-۱۶] نیز طرح تسهیم چند راز تأیید پذیری را معرفی کردند. در این طرح، تشخیص تقلب سهام‌داران امکان‌پذیر است، اما تشخیص تقلب واسطه ممکن نیست.

رمزنگاری مشبکه‌مبنا مبتنی بر کلید عمومی NTRU توسط هافشتین و همکارانش [۱۷] مطرح شد و به‌عنوان یکی از اولین و کارآمدترین روش‌های رمزنگاری مشبکه‌ای شناخته می‌شود.

نخعی و همکارانش [۱۸] طرح تسهیم چند راز آستانه‌ای (k,t,n) مبتنی بر سیستم رمزنگاری NTRU را معرفی کردند که در برابر حملات کوانتومی مقاوم است و برای تأیید درستی سهام از توابع چکیده ساز استفاده می‌کند.

ابراهیم حسین و همکارانش [۱۹] یک سیستم رمزنگاری پساکوانتومی NTRU مبتنی بر طرح تسهیم راز شامیر معرفی کردند. این طرح به زمان کمتری برای تبادل و رمزگشایی کلیدها نسبت به الگوریتم اصلی NTRU نیاز دارد.

شرفی و دقیق [۲۰] با استفاده از سامانه رمز مشبکه‌مبنا لیندنر-پایکرت و بهره‌گیری از مسائل سخت مشبکه، یک الگوریتم امضای دیجیتال و یک طرح تبادل کلید مبتنی بر مشبکه معرفی کردند.

در این مقاله، یک طرح تسهیم راز جدید آستانه‌ای تأیید پذیر مقاوم در برابر حملات کوانتومی ارائه‌شده است، ساختار مقاله به شرح زیر است:

در بخش مقدمه، تاریخچه و توسعه طرح‌های تسهیم راز آستانه‌ای مرور شده است. به طرح‌های اولیه مانند طرح شامیر و بلکلی اشاره‌شده است که بر اساس درونیابی چندجمله‌ای و هندسه متناهی بناشده‌اند. علاوه بر این، به طرح‌های تأیید پذیر مبتنی بر تابع چکیده ساز و مشبکه پرداخته‌شده و مزایا و معایب هرکدام بررسی می‌شود. در ادامه، تهدیدات ناشی از پیشرفت رایانه‌های کوانتومی و تلاش‌های صورت گرفته برای طراحی الگوریتم‌های مقاوم در برابر حملات کوانتومی بیان‌شده است. در بخش دوم و سوم، مفاهیم اساسی که مبنای طرح پیشنهادی هستند شرح داده می‌شود. این مفاهیم شامل مشبکه، مسائل سخت مشبکه، اصول رمزنگاری مبتنی بر سامانه رمز لیندنر-پایکرت و ویژگی‌های امنیتی آن است. همچنین، به نقش توزیع گاوسی در رمزنگاری مشبکه‌مبنا اشاره می‌شود و نحوه استفاده از این توزیع برای تولید پارامترها توضیح داده می‌شود. در بخش چهارم، به تشریح کامل مراحل طراحی و پیاده‌سازی طرح تسهیم راز آستانه‌ای تأیید پذیر پیشنهادی پرداخته‌ایم. ابتدا مراحل آغازین شامل انتخاب پارامترها و توزیع سهام بین سهام‌داران توضیح داده‌شده است، سپس فرآیند بازسازی راز و روند تأیید پذیری برای اطمینان از صحت داده‌های سهام شرح داده می‌شود.

در طرح پیشنهادی تقلب سهامداران بعد از بازسازی راز قابل‌شناسایی است. همچنین به دلیل استفاده از مسئله یادگیری با خطای حلقه‌ای دیگر نیازی به استفاده از کانال خصوصی جهت ارتباط بین واسطه و سهام‌داران نیست. همچنین، اگر هر زیرمجموعه از سهام‌داران با کمتر از m عضو سعی کنند راز S را بازسازی کنند، باید مسئله یادگیری با خطای حلقه‌ای را حل کنند، که یک مسئله مقاوم در برابر حملات کوانتوم است و یا یک تصادم بیابند که تابع چکیده ساز (SHAKE-۱۲۸) در برابر تصادم مقاوم است. در پایان، چهار ویژگی عملکردی طرح پیشنهادی با طرح‌های دیگر مقایسه شده است.

۲- پیش‌نیازها

۲-۱- آشنایی با مشبکه‌ها

کاربرد مشبکه در رمزنگاری بهبود زیادی در امنیت و کارایی رمزنگاری ایجاد کرده است. امنیت اکثر سامانه‌های رمزنگاری کلید عمومی مبتنی بر مشبکه بر پایه‌ی مسائل سخت در مشبکه بناشده است[۲۱-۲۲]. این سامانه‌ها از پیچیدگی کمتر و سرعت بیشتری نسبت به سامانه‌های مبتنی بر تجزیه‌ی اعداد صحیح و لگاریتم گسسته برخوردارند.

تعریف۱: فرض کنیم $v_1, \dots, v_n \in R^m$ یک مجموعه از بردارهای مستقل خطی باشند. مشبکه $\mathcal{L}$ به‌صورت زیر تعریف می‌شود:

$$\boldsymbol{\mathcal{L}} = \{a_1 v_1 + \cdots + a_n v_n | a_1, \dots, a_n \in \mathbb{Z}\}$$

بردارهای $\boldsymbol{v_1}. \dots . \boldsymbol{v_n}$ پایه مشبکه $\boldsymbol{\mathcal{L}}$ را می‌سازند. تعداد بردارهای مستقل خطی در هر پایه از مشبکه را مرتبه می‌نامند.

نتایج مهمی در زمینه رمزنگاری مبتنی بر مشبکه، توسط توزیع گسسته گاوسی حاصل‌شده است. درواقع دو کاربرد مهم در این حوزه، داشتن نقش مهم و محوری در اثبات امنیت سامانه‌های رمزنگاری مبتنی بر مشبکه است. نمونه‌برداری توزیع، یکی از مهم‌ترین عملیات‌هایی است که در سامانه‌های مشبکه مبنا مانند رمزنگاری، رمزگشایی، تبادل کلید و امضای دیجیتال مورداستفاده قرار می‌گیرد. در رمزگذاری، پیام از مبهم سازی توسط برداری به نام بردار خطا استفاده می‌شود، که با استفاده از یک توزیع آماری مانند توزیع گاوسی گسسته نمونه‌برداری شده است.

تعریف۲: برای هر عدد $n \in \mathbb{Z}^+$ و $s \in \mathbb{R}^+$ تابع گاوسی $\rho_s(x): \mathbb{R}^n \to \mathbb{R}^+$ با پارامتر s به‌صورت زیر تعریف می‌شود:

$$\rho_s(x) := \exp(-\frac{\pi \|x\|^2}{s^2})$$

که در آن $\|x\|$ همان نرم اقلیدسی است.

توزیع گسسته گاوسی روی $\mathbb{Z}$ برای هر $x \in \mathbb{Z}$ به‌صورت زیر تعریف می‌شود:

$$D_{Z.s}(x) \sim \frac{1}{S} exp\left(-\pi \frac{x^2}{s^2}\right)$$

که در آن S یک ثابت نرمال‌سازی است که اطمینان می‌دهد مجموع احتمالات برای تمام اعداد صحیح برابر یک است.

۲-۲- مسائل سخت مشبکه

مسائل مشبکه زمانی که بعد کوچک و پایه متعامد باشد، ساده است. بنابراین در زمان چندجمله‌ای حل خواهند شد. زمانی این مسئله را می‌توان در دسته مسائل سخت قرارداد که دارای بردارهایی دور از حالت متعامد و ابعاد بزرگ باشد.

مسئله کوتاه‌ترین بردار(SVP): هدف این مسئله، یافتن بردار ناصفری است که دارای کمترین نرم اقلیدسی در مشبکه باشد.

مسئله نزدیک‌ترین بردار(CVP): فرض کنیم $t \in \mathbb{R}^n$، در این مسئله، هدف یافتن یک بردار v از مشبکه است به‌طوری‌که فاصله v تا t مینیمم شود.

مسئله یادگیری با خطا (LWE): هدف این مسئله، یافتن بردار ضرایب s و بردار خطای e است که در رابطه $b = As + e$ صدق کنند، که در آن $A \in \mathbb{Z}_q^{m\times n}$ و $b \in \mathbb{Z}_q^m$. این مسئله در دو مدل جستجو و تصمیم‌گیری بیان‌شده است.

- مسئله جستجوی یادگیری با خطا: پارامترهای m و n، پیمانه q و توزیع خطای D که معمولاً یک توزیع گاوسی $D_{Z.s}$ با انحراف معیار $\sigma = \frac{s}{\sqrt{2\pi}}$ در نظر گرفته می‌شود. برای بردار راز $s \in \mathbb{Z}_q^n$ که به‌صورت یکنواخت نمونه‌گیری شده است، عنصر تصادفی $e \in \mathbb{Z}_q$ با استفاده از توزیع D نمونه‌سازی شده است. بنابراین

که در آن $a_i \in \mathbb{Z}_q^n$.

هدف، بردار راز s را بازیابی کنید.

- مسئله تصمیم‌گیری یادگیری با خطا: با توجه به پارامترهای بیان‌شده در مسئله جستجوی یادگیری با خطا، در این مسئله m نمونه مستقل

$(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$

مشخص می‌کند که (a_i, b_i)ها به فرم معادله زیر هستند؟

$(a_i, b_i) =: < s, a_i > + e(\ mod\ q)$

برخلاف مسئله نزدیک‌ترین بردار و مسئله کوتاه‌ترین بردار، ارتباط بین مسئله یادگیری با خطا و مشبکه‌ها چندان واضح نیست. درواقع، می‌توان گفت حل مسئله یادگیری با خطا حالتی خاص از مسئله نزدیک‌ترین بردار با بردار هدف b و مسئله کوتاه‌ترین بردار با بردار کوتاه s است [۹].

ازآنجاکه در طرح‌های رمزنگاری مبتنی بر مسئله یادگیری با خطا، اندازه کلید عمومی بزرگ است، این موضوع موجب کاهش کارایی پیاده‌سازی مسئله یادگیری با خطا می‌شود. ازاین‌رو، لباچفسکی و همکارانش [۲۴] رمزنگاری مبتنی بر مسئله یادگیری با خطای حلقه‌ای (Ring-LWE) را مطرح کردند که نسخه جبری مسئله یادگیری با خطا است. در این روش، به‌جای بردارها از عناصر یک حلقه چندجمله‌ای استفاده می‌شود که به حافظه کمتری نیاز دارد.

مسئله یادگیری با خطای حلقه‌ای: مسئله یادگیری با خطای حلقه‌ای با یک حلقه‌ی R از درجه n روی $\mathbb{Z}$ و یک توزیع خطای D روی R پارامتر سازی می‌شود. در حالت خاص زمانی که n توانی از ۲ باشد، حلقه به‌صورت $R_q = \frac{\mathbb{Z}[x]}{<x^n+1>}$ در نظر گرفته می‌شود.

برای عنصر $s \in R_q$، توزیع $A_{s.D}$ روی $R \times R_q$ با انتخاب $a \in R_q$ به‌صورت یکنواخت تصادفی، انتخاب $e \leftarrow D$ و خروجی $(a, b := a \cdot s + e \mod q)$ نمونه‌سازی می‌شود. (ضرب $a \cdot s$ عمل ضرب روی حلقه R است.) همانند مسئله یادگیری با خطا، نسخه حلقه‌ای این مسئله نیز در دو مدل جستجو و تصمیم‌گیری به‌صورت زیر تعریف‌شده است.

- مسئله جستجوی یادگیری با خطای حلقه‌ای: در مدل
- جستجو برای m نمونه (a_i, b_i) که با یک توزیع $A_{s,D}$ برای یک عنصر مخفی s نمونه‌سازی شده‌اند، هدف یافتن s است.
- مسئله تصمیم‌گیری یادگیری با خطای حلقه‌ای: مدل تصمیم‌گیری مسئله یادگیری با خطای حلقه‌ای تشخیص تفاوت بین نمونه‌های (a_i, b_i) خروجی از توزیع $A_{s,D}$ با نمونه‌های دارای توزیع یکنواخت است.

۳- سامانه رمز لیندنر-پایکرت

لیندنر و پای کرت [۲۳] سامانه‌ی رمزنگاری مبتنی بر مسئله یادگیری با خطا را معرفی کردند، که در آن به تحلیل اندازه‌های کلید و سطح امنیت پرداختند. در این مقاله کلیدهای ارائه‌شده دو برابر کوچک‌تر از نمونه‌های قبلی است [۲۵,۲۷,۳۰]. درحالی‌که کوچک‌ترین خدشه‌ای به سطح امنیتی طرح وارد نیامده است.

۱-۳- سیستم رمزگذاری

پارامترهای موردنیاز در این سامانه رمزنگاری به شرح زیر است: یک پیمانه صحیح $q \geq 2$ و بعدهای صحیح $n_1 . n_2 \geq 1$ که به مسئله یادگیری با خطا مرتبط هستند، پارامترهای گاوسی s_e و s_k به ترتیب مربوط به رمزگذاری و تولید کلید است، و الفبای پیام Σ (به‌طور مثال $\Sigma = \{0,1\}$) و طول پیام $\ell > 1$ در نظر گرفته‌شده است.

همچنین توابع کدگذاری و کدگشایی به‌این‌ترتیب $encode: \Sigma \to R_q$ و $decode: R_q \to \Sigma$ تعریف‌شده‌اند، که در برابر خطا مقاوم باشند. برای آستانه به‌اندازه کافی بزرگ $t \geq 1$ و برای هر $e \in [-t, t]$، خواهیم داشت:

$$decode(encode(m) + e(mod\ q)) = m$$

به‌طور مثال، برای الفبای پیام $\Sigma = \{0,1\}$، تابع کدگذاری

$encode(m) \coloneqq m \cdot \left\lfloor \frac{q}{۲} \right\rfloor$ با ضابطه $encode: \{۰,۱\} \to \mathbb{Z}_q$

و تابع کدگشایی $decode: \mathbb{Z}_q \to \{۰,۱\}$ با ضابطه

$$decode(\bar{m}) \coloneqq \begin{cases} ۰ & \bar{m} \in [-\left\lfloor \frac{q}{۴} \right\rfloor, \left\lfloor \frac{q}{۴} \right\rfloor) \\ ۱ & o.w. \end{cases}$$

تعریف‌شده‌اند.

این تعریف تا آستانه $t = \left\lfloor \frac{q}{۴} \right\rfloor$ تحمل این خطا را دارد. درنهایت، توابع فوق برای بردارها، به‌صورت مؤلفه به مؤلفه گسترش داده می‌شود.

برای به دست آوردن کلیدهای عمومی به‌اندازه کافی کوچک، سامانه از یک ماتریس عمومی به‌طور یکنواخت تصادفی $\bar{A} \in \mathbb{Z}_q^{n_۱ \times n_۲}$ استفاده می‌کند، به‌عبارت‌دیگر این ماتریس توسط یک منبع معتمد تولیدشده و توسط تمام شرکت‌کنندگان در سامانه مورداستفاده قرار می‌گیرد. اگر هیچ منبع معتمدی وجود نداشته باشد، در این صورت $\bar{A}$ در هر بخش از تولید کلید توسط کاربر مرتبط انتخاب می‌شود و در کلید عمومی مربوطه استفاده شود. **مرحله آغازین:** پارامترهای $R_۱ \leftarrow D_{\mathbb{Z}.s_k}^{n_۱ \times \ell}$ و $R_۲ \leftarrow D_{\mathbb{Z}.s_k}^{n_۲ \times \ell}$ انتخاب‌شده است. فرض می‌شود $P = R_۱ - \bar{A} \cdot R_۲ \in \mathbb{Z}_q^{n_۱ \times \ell}$. کلید عمومی همان $(P.\bar{A})$ و کلید خصوصی این سامانه برابر $R_۲$ است. فرم ماتریسی رابطه بین کلیدهای خصوصی و عمومی به شکل زیر خواهد بود:

$$[\bar{A} \quad P] \cdot \begin{bmatrix} R_۲ \\ I \end{bmatrix} = R_۱ \quad mod\ q.$$

مرحله رمزگذاری: بردارهای خطای

$$e=\left(e_۱,e_۲,e_۳\right) \in Z^{n_۱} \times Z^{n_۲} \times Z^{l}$$

با هر ورودی به‌طور مستقل از $D_{\mathbb{Z}.s_e}$ انتخاب می‌شوند. فرض کنیم $\bar{m} = encrypt(m) \in \mathbb{Z}_q^{\ell}$. متن رمز به‌صورت زیر محاسبه می‌شود:

$$[c_۱ = a \cdot e_۱ + e_۲, c_۲ = p \cdot e_۱ + e_۳ + \bar{m}] \in R_q.$$

مرحله رمزگشایی: رمزگشایی با محاسبه رابطه زیر حاصل می‌شود:

$$c_۱ \cdot r_۲ + c_۲ = \begin{bmatrix} c_۱ & c_۲ \end{bmatrix} \cdot \begin{bmatrix} R_۲ \\ I \end{bmatrix} = \begin{bmatrix} e_۱^T & e_۲^T + \bar{m}^T \end{bmatrix} \cdot \begin{bmatrix} R_۲ \\ I \end{bmatrix} = e^T \cdot R + \bar{m}^T$$

که در آن $R = \begin{bmatrix} R_۱ \\ R_۲ \\ I \end{bmatrix}$.

رمزگشایی تا زمانی که آستانه $| < e.r_j > | < t$ برقرار باشد، درست عمل می‌کند.

۲-۳- سیستم رمزگذاری مبتنی بر حلقه

به‌طور خلاصه، در اینجا طرحی مبتنی بر نسخه تصمیم مسئله یادگیری با خطای حلقه‌ای است، را بیان می‌کنیم [۲۳].

حلقه چندجمله‌ای $R = \frac{\mathbb{Z}[x]}{f(x)}$ برای چندجمله‌ای $f(x)$ که روی $\mathbb{Z}$ تحویل‌ناپذیر است، در نظر گرفته می‌شود. در [۲۴] چندجمله‌ای $f(x) = x^n + ۱$ برای n توانی از ۲ موردمطالعه قرارگرفته است. فرض کنید $q \in \mathbb{Z}$ یک پیمانه صحیح مثبت و $R_q = \frac{\mathbb{Z}_q[x]}{f(x)}$. فرض کنید D_e و D_k توزیع خطاهایی روی R باشند.

همچنان Σ را الفبای پیام می‌دانیم. پیام رمزگذاری شده و رمزگشایی‌شده طبق توابع کدگذاری و کدگشایی $encode: \Sigma \to R_q$ و $decode: R_q \to \Sigma$ هستند، به‌طوری‌که برای $e \in R$ داریم:

درواقع، ضرایب چندجمله‌ای در $\frac{\mathbb{Z}_q[x]}{f(x)}$ همگی در بازه $[-t,t)$ قرار دارند. پارامتر $a \in R_q$ به‌طور یکنواخت تصادفی توسط یک منبع معتمد یا کاربر انتخاب می‌شود.

مرحله آغازین: پارامترهای $r_۱, r_۲ \leftarrow D_k$ انتخاب می‌شوند و $p = r_۱ - a \cdot r_۲ \in R_q$. کلید عمومی (a,p) و کلید خصوصی $r_۲$ است.

مرحله رمزگذاری: پارامترهای $e_۱, e_۲, e_۳ \leftarrow D_k$ انتخاب می‌شوند و $\bar{m} = encode(m) \in R_q$. متن رمز شده به‌صورت زیر محاسبه می‌شود:

مرحله رمزگشایی: با محاسبه $decode(c_۱ \cdot r_۲ + c_۲) \in \Sigma^n$ رمزگشایی انجام خواهد شد. درواقع این رمزگشایی تا زمانی درست عمل خواهد کرد که $e_۱ \cdot r_۱ + e_۲ \cdot r_۲ + e_۳$ در بازه آستانه خطای تابع کدگشایی قرار بگیرد. به‌عبارت‌دیگر $| < e, r_j > | < t$.

۳-۳- تعیین پارامترها برای صحیح بودن کدگشایی

در این بخش؛ یک کران بالا روی انحراف معیار از توزیع گاوسی گسسته آورده شده است که اجرای صحیح سامانه لیندنر-پایکرت را تضمین می‌کند.

لم ۳: در سامانه رمز لیندنر-پایکرت، انحراف s_k و s_e متناظر با توزیع گسسته D_k و D_e برای هر $۰ < \delta < ۱$ از بالا کران‌دار با δ است، هرگاه داشته باشیم:

$$s_k \cdot s_e \leq \frac{\sqrt{۲\pi}}{c} \cdot \frac{t}{\sqrt{(n_۱ + n_۲) \cdot \log(\frac{۲}{\delta})}}$$

که در آن $c \geq ۱$ یک مقدار وابسته به n است، و لگاریتم در مبنای ۲ است. مقادیر دیگر در جدول (۱) با احتمال خطای ۰/۰۱ آورده شده است.

اثبات- لم ۱.۳ از [۲۳] را ببینید.

بنابراین با احتمال خطای δ خواهیم داشت:

که در آن هر بردار خطا $e \in [-t, t)$ و بردار پیام $m \in \Sigma$.

جدول(۱): تعیین پارامترها جهت محاسبه کران بالای انحراف معیار

$(n_۱ + n_۲)$	$c \geq$	$\frac{s_k \cdot s_e}{t} \leq$
۲۵۶	۱/۳۵	۰/۰۸۹۳۶
۳۸۴	۱/۲۸	۰/۰۷۶۹۵
۵۱۲	۱/۲۵	۰/۰۶۸۲۴
۶۴۰	۱/۲۲	۰/۰۶۲۵۳

امنیت سامانه رمز لیندنر-پایکرت، طبق نسخه تصمیم مسئله یادگیری با خطای حلقه‌ای برای توزیع‌های خطای D_k و D_e حاصل می‌شود. درواقع، اگر نسخه تصمیم مسئله یادگیری با خطای حلقه‌ای با پارامترهای q و n حل شود، آنگاه مسئله کوتاه‌ترین بردار مشبکه‌ای روی مشبکه n-بعدی نیز حل خواهد شد[۲۳-۲۴].

قضیه ۴: سامانه رمز لیندنر-پایکرت در برابر حمله تحلیل همبستگی توان (CPA) با فرضیات مسئله تصمیم یادگیری با خطا با پیمانه q برای

۱) بعد $n_۲$ با توزیع خطای $D_{\mathbb{Z},s_k}$

۲) بعد $n_۱$ با توزیع خطای $D_{\mathbb{Z},s_e}$

امن است.

اثبات- قضیه ۳.۲ از [۲۳] را ببینید.

سختی مسئله یادگیری با خطای حلقه‌ای و کاهش آن به یک مسئله سخت مشبکه‌ای برای بعدهای n که توانی از ۲ نیستند، در [۲۴] با روش‌های پیچیده اثبات‌شده است.

۴- طرح تسهیم راز آستانه‌ای (m, m) پیشنهادی

۴-۱- مرحله آغازین

واسطه قصد دارد راز

$$S = k_{n-۱}x^{n-۱} + k_{n-۲}x^{n-۲} + \cdots + k_{.} \in R_q$$

بین m سهامدار $P_۱ \ldots . P_m$ توزیع شود. مراحل زیر توسط واسطه انجام می‌شود:

۱) مقدار q و حلقه R_q را به‌صورت زیر

$$q \equiv ۱ \ (mod\ n). \qquad R_q = \frac{\mathbb{Z}_q[x]}{<x^n+۱>}$$

در نظر گرفته‌شده‌اند، که در آن n توانی از ۲ است و سپس این مقادیر منتشر می‌شوند.

۲) پارامترهای s_k (انحراف معیار) و D_k (توزیع گاوسی) طبق سامانه رمز لیندنر-پایکرت در نظر گرفته می‌شوند.

۳) توابع کدگذاری و کدگشایی طبق سامانه رمز لیندنر-پایکرت همراه با یک آستانه خطای $t \in \mathbb{N}$ ساخته می‌شوند.

$$decode\big(encode(m) + e(mod\ q)\big) = m$$

۴-۲- مرحله توزیع سهام

مقادیر $a_i \in R_q$ به‌صورت یکنواخت تصادفی توسط هر سهامدار P_i تولید می‌شوند. سپس سهامدار P_i با استفاده از توزیع گاوسی گسسته D_k چندجمله‌ای‌های $r_{۱i}, r_{۲i} \in R_q$ را نمونه‌سازی می‌کند.

کلید عمومی هر سهامدار توسط خود سهامدار به‌صورت زیر ساخته و به‌صورت عمومی منتشر می‌شود:

$$\left(a_i, b_i = r_{۱i} - a_i r_{۲i}\right) \in R_q$$

و کلید خصوصی هر سهامدار P_i برای $i = ۱, \ldots, m$ همان مقدار $r_{۲i}$ است، که نزد هر سهامدار نگهداری می‌شود.

واسطه چندجمله‌ای‌های خطای $e_{۱i}, e_{۲i}, e_{۳i} \in R_q$ برای هر سهامدار با استفاده از توزیع D_k نمونه‌سازی و سپس چندجمله‌ای‌های زیر را محاسبه می‌کند:

$$C_{۱i} = a_i e_{۱i} + e_{۲i}$$
$$C_{۲i} = b_i e_{۱i} + \bar{s}_i$$
$$C_{۳i} = b_i e_{۲i} + e_{۳i}$$

که در آن $s_i = k_{n-i}$ برای $i = ۱, \ldots, m$ و $\bar{s_i} = encode(s_i)$.

در گام بعدی، واسطه مقادیر

$$h_i = H(s_i) \| H\left(decode\left(-b_i a_i e_{۱i}\right)\right)$$

را محاسبه می‌کند. در اینجا H همان تابع چکیده ساز SHAKE-۱۲۸ است، که در برابر تصادم مقاوم است.

درنهایت واسطه بدون نیاز به کانال خصوصی سهام $\left(C_{۱i}, C_{۲i}, C_{۳i}, h_i\right)$ را برای هر سهامدار P_i که $i = ۱, \ldots, m$ توزیع می‌کند.

۴-۳- مرحله تأیید پذیری و بازسازی راز

با توجه به سهم هر سهامدار و کلید خصوصی که در اختیار هر سهامدار است، سهامداران با محاسبه

$$decode\left(C_{۲i} + r_{۲i} C_{۱i}\right) = s_i$$

سهم راز خویش را بازسازی می‌کنند، سپس صحت سهم دریافتی خود را با محاسبه

$$h_i = H(s_i) \| H(decode\left(C_{۲i} - b_i C_{۱i}\right))$$

تأیید می‌کنند.

ازآنجایی‌که همه سهام‌داران به داده‌های عمومی دسترسی دارند، پس از اعلام سهم P_i توسط خودش سایرین می‌توانند با محاسبه h_i صحت آن سهم را تأیید نمایند. درنهایت، مجموع سهام‌داران با قرار دادن سهم‌های خود در چندجمله‌ای مرتبط با راز، $S = s_{n-1}x^{n-1} + s_{n-2}x^{n-2} + \cdots + s_0$ می‌توانند راز اصلی را بازسازی کنند.

۵- تحلیل ویژگی طرح

ابتدا ثابت می‌کنیم بازسازی راز به‌درستی انجام‌شده است، سپس درستی فرآیند تأیید پذیری نشان داده خواهد شد.

قضیه ۴: مفاهیم طبق مرحله توزیع سهام در نظر گرفته‌شده‌اند.

در این صورت، ۱) $decode\left(C_{2i} + r_{2i}C_{1i}\right) = s_i$, ۲) $h_i = H(s_i) \| H(decode\left(C_{3i} - b_iC_{1i}\right))$.

اثبات- ۱) $decode\left(C_{2i} + r_{2i}C_{1i}\right) = decode(b_ie_{1i} + \bar{s}_i + r_{2i}a_ie_{1i} + r_{2i}e_{2i}) = decode\left(\bar{s}_i + (r_{1i}e_{1i} + r_{2i}e_{2i})\right)$

با توجه به لم ۳، برای این‌که طرح پیشنهادی به‌درستی اجرا شود، یک کران بالا روی انحراف معیار s_k از توزیع گسسته گاوسی D_k معرفی شد. ازآنجایی‌که چندجمله‌ای $r_{1i}e_{1i} + r_{2i}e_{2i}$ متعلق به آستانه خطای $[-\left\lfloor\frac{q}{4}\right\rfloor, \left\lfloor\frac{q}{4}\right\rfloor)$ است، بنابراین $decode\left(r_{1i}e_{1i} + r_{2i}e_{2i}\right) = 0$

درنتیجه $decode(\bar{s}_i) = decode(encode(s_i)) = s_i$.

در ادامه نشان می‌دهیم: ۲) $h_i = H(s_i) \| H(decode\left(C_{3i} - b_iC_{1i}\right)) = H(s_i)\|H(decode\left(b_ie_{2i} + e_{3i} - b_ia_ie_{1i} + b_ie_{2i}\right)) = H(s_i)\|H(decode(e_{3i} - b_ia_ie_{1i}))$

با توجه به اینکه بردارهای خطا از توزیع گاوسی با شرایط لم ۳ انتخاب می‌شوند، بنابراین $decode\left(e_{4i} - b_ia_ie_{1i}\right) =$ $decode(-b_ia_ie_{1i})$ و لذا $h_i = H(s_i)\|H\left(decode\left(-b_ia_ie_{1i}\right)\right)$.

نکته: در [۳۰] توسط لباچفسکی و همکارانش ثابت شد که جایگزینی مسئله استاندارد یادگیری با خطا با مسئله یادگیری با خطای حلقه‌ای، سختی بیشتر این تابع رمزنگاری را تضمین می‌کند.

در ادامه نشان می‌دهیم، اگر هر زیرمجموعه از سهام‌داران با کمتر از m عضو سعی کنند راز S را بازسازی کنند، باید مسئله یادگیری با خطای حلقه‌ای را حل کنند، که یک مسئله مقاوم در برابر حملات کوانتوم است و یا یک تصادم بیابد که تابع چکیده ساز (SHAKE-۱۲۸) در برابر تصادم مقاوم است.

قضیه ۵: در طرح پیشنهادی، هر زیرمجموعه از سهام‌داران با تعداد اعضای کمتر از m قادر به بازسازی راز S نیست.

اثبات- فرض کنید سهام‌داران مجموعه $\{P_1, \dots, P_{m-1}\}$ قصد بازسازی راز را داشته باشند. برای این کار با توجه به سهم $C_{2m} = b_me_{1m} + \bar{s}_m$ باید مقدار e_{1m} را بیابند. ازآنجایی‌که واسطه بردارهای خطا را برای هر سهام به‌طور جداگانه نمونه‌سازی کرده است بنابراین این بردار خطا در اطلاعات سهام‌داران دیگر وجود ندارد و برای به دست آوردن آن باید مسئله یادگیری با خطای حلقه‌ای را حل کنند. از طرفی اگر بخواهند با در دست داشتن کلید عمومی، چندجمله‌ای خطای e'_{1m} را طوری بیابند که $H\left(decode\left(-b_ma_me'_{1m}\right)\right) = H(decode\left(C_{3m} - b_mC_{1m}\right))$ باشد، امکان‌پذیر نیست. به این دلیل که با مسئله مقاومت در برابر تصادم تابع چکیده ساز (SHAKE-۱۲۸) روبه‌رو خواهند شد.

۵- نتیجه‌گیری

در دنیای کوانتوم کنونی، طرح‌هایی که بتوانند امنیت را تضمین کنند، از اهمیت بالایی برخوردارند. در این مقاله، یک طرح تسهیم راز (m,m)-آستانه‌ای مبتنی بر سامانه رمز لیندنر-پایکرت پیشنهادشده است. این طرح نیاز به کانال خصوصی ندارد، زیرا سهام‌ها با استفاده از کلید عمومی و مبتنی بر مسئله یادگیری با خطای حلقه‌ای ساخته‌شده‌اند و بازسازی را تنها با کمک کلید خصوصی که نزد هر سهام‌دار است، انجام می‌شود. همچنین، تأیید پذیری در این طرح بر اساس تابع چکیده ساز صورت می‌گیرد. به‌این‌ترتیب، سهام‌داران می‌توانند با استفاده از اطلاعات عمومی ارائه‌شده توسط واسطه در مرحله توزیع سهام، صحت سهام‌های خود و دیگر سهام‌داران را بررسی کنند و نیازی به تعامل مجدد باواسطه ندارند.

جهت بررسی بیشتر روش پیشنهادی، جدول (۲) کارایی این روش را با چند روش دیگر مقایسه می‌کند. با توجه به مقایسه صورت گرفته در جدول فوق، مزیت روش پیشنهادی نسبت به سایر روش‌ها را بیان می‌کند.

جدول(۲): مقایسه کارایی روش پیشنهادی با روش‌های متداول دیگر

خاصیت / طرح	نیاز به کانال خصوصی	مسئله سخت	مقاوم در برابر حملات کوانتوم	تأیید پذیری
طرح CZ [۳]	بله	تابع چکیده ساز	خیر	خیر
طرح DA	بله	تابع چکیده	خیر	خیر

[۴]		ساز		
طرح اسعد [۱۲]	بله	مسئله نزدیک‌ترین بردار	بله	خیر
طرح امینی [۱۳]	بله	مسئله یادگیری با خطا	بله	خیر
جئورجسکو [۱۰]	خیر	مسئله لگاریتم گسسته	خیر	بله
بنذرخانی [۱۱]	بله	تابع چکیده ساز	بله	بله
کیا ماری [۱۵]	بله	مسئله یادگیری با خطا	بله	بله
طرح پیشنهادی	خیر	یادگیری با خطای حلقه‌ای	بله	بله

۶- مراجع

[1] A di. Shamir, "How to share a secret," Communications of the ACM 2.11. 612-613, 1979. https://doi.org/10.1145/359168.359176

[2] G. Blakley, "Safeguarding Cryptographic Keys," In Proc. AFIPS 1979 National Computer Conf, pp. 313–317, June 1979. https://doi.org /10.1109 /MARK .1979 .88 1 7296.

[3] C. S. Chum, X. Zhang, "Hash function-based secret sharing scheme designs," Security and Communication Networks, 6(5). pp. 584-592, 2013. https://doi.org /10.1002/sec.576.

[4] A. Das, A. Adhikari, "An efficient multi-use multi-secret sharing scheme based on hash function," Applied mathematics letters, 23(9), pp. 993-996, 2010. https:// doi.org/10.1016/j.aml.2010.04.024.

[5] J. Shao, "Efficient verifiable multi-secret sharing scheme based on hash function," Information Sciences, 278. pp. 104-109, 2014. https://doi.org/10.1016/j.ins.2014.03.025.

[6] M. Farhadi, H. Bypour, and R. Mortazavi, "A Hash-Based Multi-Use Multi-Stage Secret Sharing Scheme with General Access Structure," JOURNAL OF ELECTRONIC AND CYBER DEFENCE, vol. 6, no. 3 (23) , pp. 107–115, 2018, (in Persian), https://dor.isc.ac/dor/20.1001.1.23224347.1397.6 .3.9.9

[7] 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. https://doi.org /10.1109 /SFCS.1994. 365700.

[8] R . J . McEliece, "A Public-Key Cryptosystem Based on Algebraic Coding Theory," DSN Progress Report, vol . 42, no . 44 , pp. 114-116 , 1978 .

[9] 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.

[10] 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. https://doi.org/10.2478/v10127-012-0042-8.

[11] R. El Bansarkhani and M. Meziani, "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. https://doi.org/10.1007/978-3-642-30955-7_14.

[12] S. Asaad, H. A. Khorasgani, T. Eghlidos, and M. Aref, "Sharing secret using lattice construction," In Telecommunications (IST), 2014 7th International Symposium on, pp. 901-906. IEEE, 2014. https://doi.org/10.1109/ISTEL.2014.7000831.

[13] Khorasgani, Hamidreza Amini, Saba Asaad, Taraneh Eghlidos, and Mohammadreza Aref. "A lattice-based threshold secret sharing scheme." In Information Security and Cryptology (ISCISC), 2014 11th International ISC Conference on, pp. 173-179. IEEE, 2014. https://doi.org/10.1109/ISCISC.2014.6994043.

[14] F. Li, J. Yan, S. Zhu, H. Hu, "A verifiable multi-secret sharing scheme based on short integer solution," Chinese Journal of Electronics, 32(3), 1-8, 2023. https://doi.org/10.23919/cje.2021.00.062.

[15] N. Kiamari, M. Hadian, S. Mashhadi, "Non-interactive verifiable LWE-based multi secret sharing scheme," Multimedia Tools and Applications, 82(14), 22175-22187, 2023. https://doi.org/10.1007/s11042-022-13347-4

[16] M. Hadian Dehkordi, S. Mashhadi, and N. Kiamari, "Two Verifiable Multi-Secret Sharing Schemes: A Linear Scheme with Standard Security and A Lattice-Based Scheme," JOURNAL OF ELECTRONIC AND CYBER DEFENCE, vol. 8, no. 3 (31) , pp. 101–115, 2020, (in Persian), https://dor.isc.ac/dor/20.1001.1.23224347.1399.8 .3.8.2

[17] J. Hoffstein, P. Jill, and H. Silverman. "NTRU: A ring-based public key cryptosystem," International algorithmic number theory symposium. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998.

[18] A. Amroudi, Nakhaei, A. Zaghain, and M. Sajadieh. "A verifiable (k, n, m)-threshold multi-secret sharing schem e based on ntru cryptosystem," Wireless Personal Comm unications 96, 1393-1405, 2017.

Springer 2010. https://doi.org/10.1007/978-3-642-13190-5_1.

[25] B. Rajabi and Z. Eslami, "A Verifiable Threshold Secret Sharing Scheme Based on Lattices," Information Science , vol. 501 pp. 655–661, 2019. https://doi.org /10 .101 6 /j.ins.2018.11.004.

[26] O. Regev, "On Lattices , Learning with Errors , Random Linear Codes , and Cryptography," J .ACM, 56(6): 34: 134:40, September 2009. https://doi.org/10.1145/1568318.1568324.

[27] D . Micciancio and S . Goldwasser , "Complexity of Lattice Problems : A Cryptographic Perspective," Ser . Milken Institute Series on Financial Inno vation and Economic Growth . Springer US, 2002. https://doi.org/10.1007/978-1-4615-0897-7

[28] D . Bernstein , J . Buchmann , and E . Dahmen , "Post-Quantum Cryptography," Springer , 2009. https://doi.org/10.1038/nature23461.

[29] C. Peikert, "Public-key cryptosystems from the worst-case shortest vector problem," InProceedings of the forty-first annual ACM symposium on Theory of computing May 31 (pp. 333-342), 2009.

[30] V. Lyubashevsky, C. Peikert, O. Regev, "On ideal lattic es and learning with errors over rings," Journal of the ACM (JACM), Vol. 6, 1–35, 2013.

[19] A. I. Hussein, A. T. MaoLood, E. K. Gbashi, "NTRU- SSS: Anew Method Signcryption Post Quantum Cryp tography Based on Shamir's Secret Sharing, " Computers, Materials & Continua, 76(1), 2023. https://doi.org/10.32604/cmc.2023.039804.

[20] J. Sharafi, H. Daghigh. "A Ring-LWE-based digital sign ature inspired by Lindner–Peikert scheme." Journal of Mathematical Cryptology 16, no. 1 205-214, 2022. https://doi.org/10.1515/jmc-2021-0013.

[21] D. Micciancio, O. Regev, "Lattice-based cryptography," In Post-quantum cryptography (pp. 147-191). Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. https://doi.org/10.1007/978-3-540-88702-7-5.

[22] O.Regev, "New lattice-based cryptographic constructio ns," Journal of the ACM (JACM), 51(6), 899-942, 2004. https://doi.org/10.1145/1039488.1039490.

[23] R. Lindner, C. Peikert, "Better key sizes (and attacks) for LWE-based encryption,"Cryptographers Track at the RSA Conference. Springer, Berlin, Heidelberg, 2011. https://doi.org/10.1007/978-3-642-19074-2-21.

[24] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 1-2,