دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۳، جلد ۲۲، شماره ۲ (۶۵-۷۴)
https://monadi.isc.org.ir

ارائه‌شده در بیست و یکمین کنفرانس بین‌المللی انجمن رمز ایران در دانشگاه تربیت مدرس و پژوهشگاه ارتباطات و فناوری اطلاعات، ۲۵ و ۲۶ مهرماه ۱۴۰۳

تحلیل امنیت یک طرح رمزگذاری جستجوپذیر احراز اصالت شده فاقد گواهی‌نامه★

مهناز نوروزی[۱،*] و عطیه صادقی[۲]

[۱]گروه علوم کامپیوتر، دانشکده علوم ریاضی، دانشگاه الزهرا، تهران، ایران
[۲]گروه ریاضی، دانشکده علوم ریاضی، دانشگاه الزهرا، تهران، ایران

اطلاعات مقاله

کلمات کلیدی:
رمزگذاری جستجوپذیر
رمزنگاری فاقد گواهی‌نامه
احراز اصالت
تمایزناپذیری

نوع مقاله: پژوهشی

چکیده

روش‌های رمزگذاری جستجوپذیر فاقد گواهی‌نامه، ضمن حفظ محرمانگی داده‌ها، امکان جستجو بر روی متون رمزگذاری شده را فراهم کرده و همزمان بر هر دو مشکل مدیریت گواهی‌نامه‌ها و امان‌سپاری کلید غلبه می‌نمایند. از آنجا که عملیات زوج‌نگاری دوخطی از نظر محاسباتی هزینه‌بر بوده و برای دستگاه‌های با محدودیت منابع مناسب نیستند، پژوهشگران به دنبال ارائه راهکارهایی بدون زوج‌نگاری دوخطی هستند تا بتوانند کارایی را افزایش دهند. اخیرا در سال ۲۰۲۴ سنوسی و همکاران یک طرح رمزگذاری جستجوپذیر فاقد گواهی‌نامه بدون زوج‌نگاری دوخطی پیشنهاد نموده و ادعا کردند که از نظر ویژگی‌های امنیتی، هزینه‌های محاسباتی و هزینه‌های ارتباطی از سایر طرح‌های موجود بهتر عمل می‌کند. با این حال در این مقاله نشان می‌دهیم که طرح پیشنهادی آنها، از چندین مشکل امنیتی بسیار مهم رنج می‌برد. اولاً اثبات می‌کنیم که طرح آنها ویژگی فاقد گواهی‌نامه بودن را احراز نمی‌کند و کاربران می‌توانند خود را به جای شخصی دیگر جا زده و عملیاتی را که باید منحصراً توسط آن شخص قابل انجام باشد، به جای او انجام دهند. همچنین نشان می‌دهیم که برخلاف ادعای سنوسی و همکاران، طرح ارائه شده توسط آنها نیازمندی‌های ضروری تمایزناپذیری متون رمزی و تمایزناپذیری دریچه را برآورده نمی‌کند.

© ۱۴۰۳ انجمن رمز ایران

۱ مقدمه

رمزگذاری جستجوپذیر (SE [۱]) اولین بار در سال ۲۰۰۰ توسط سانگ و همکاران معرفی شد [۱]. چنین روش‌هایی ضمن حفظ محرمانگی داده‌ها، امکان جستجو بر روی متون رمزگذاری شده را فراهم می‌کنند [۲]. در این امر سه نهاد درگیر هستند: (۱) فرستنده داده که کلیدواژه‌های یک سند را استخراج نموده و متون رمزی جستجوپذیر مربوط به این کلیدواژه‌ها را تولید می‌کند و آنها را همراه با سند رمزگذاری شده بر روی سرویس‌دهنده ابری بارگذاری می‌نماید، (۲) گیرنده داده که با ساخت دریچه [۲] متناظر با کلیدواژه مورد نظرش، درخواست جستجو در داده‌های بارگذاری شده را می‌دهد و (۳) سرویس‌دهنده ابری که به کمک الگوریتم آزمایش، داده‌های رمزگذاری شده را جستجو می‌کند تا نتایج مورد نظر را بازگرداند. طرح‌های SE به دو دسته رمزگذاری متقارن جستجوپذیر [۳] و رمزگذاری کلید عمومی جستجوپذیر [۴] تقسیم می‌شوند. دسته اول برای سناریوهای به اشتراک‌گذاری داده مناسب نیست و مسئله ذاتی توزیع کلید را دارد؛ اما

★از کمیته علمی بیست و یکمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول (این پژوهش در آزمایشگاه ریاضیات گسسته دانشکده علوم ریاضی دانشگاه الزهرا (س) انجام شده است.)
آدرس‌های رایانامه: m.noroozi@alzahra.ac.ir (مهناز نوروزی)، atiye76.s6@gmail.com (عطیه صادقی)
© ۱۴۰۳ تمامی حقوق متعلق به انجمن رمز ایران است.

[1] Searchable Encryption
[2] Trapdoor

دسته دوم، این مسائل را برطرف می‌کند. در سال ۲۰۰۴، بونه و همکاران اولین طرح رمزگذاری کلید عمومی جستجوپذیر که رمزگذاری کلید عمومی با قابلیت جستجوی کلیدواژه (PEKS [1]) نامیده شد را ارائه کردند [۵].

در سال ۲۰۰۶، بیون و همکاران یک حمله قابل توجه به طرح‌های PEKS به نام حمله حدس کلیدواژه (KGA [2]) معرفی کردند [۶] که از این واقعیت ناشی می‌شود که کلیدواژه‌ها همانند گذرواژه‌ها کاملاً تصادفی نیستند و از یک دامنه محدود انتخاب می‌شوند و بنابراین با یک فضای کلیدواژه کوچک روبرو هستیم. در یک KGA، متخاصم فهرستی از تمام کلیدواژه‌های ممکن ایجاد کرده و متون رمزی متناظر با آنها را محاسبه می‌کند. سپس با دستیابی به یک دریچه، الگوریتم آزمایش را بر روی این دریچه و تک‌تک متون رمزی فهرست اجرا می‌کند تا کلیدواژه متناظر با دریچه را بدست آورد.

در سال ۲۰۱۰، ری و همکاران با تغییر الگوریتم‌های PEKS یک مفهوم جدید به نام رمزگذاری کلید عمومی با قابلیت جستجوی کلیدواژه توسط آزمایش‌گر خاص ارائه کردند [۷] که در آن با تابعیت الگوریتم آزمایش از کلید خصوصی سرویس‌دهنده، تنها او قادر به اجرای این الگوریتم است و بنابراین روش حمله فوق برای حدس کلیدواژه از طرف متخاصمین خارجی (یعنی به جز سرویس‌دهنده) غیرقابل انجام خواهد شد. آنها همچنین مفهوم غیرقابل تمایز بودن دریچه را به عنوان یک شرط کافی برای تأمین امنیت در برابر KGA معرفی کردند که بدین معنا است که دریچه هیچ اطلاعاتی در مورد کلیدواژه متناظر به خود فاش نمی‌کند.

در سال ۲۰۱۷ هوانگ و لی، به منظور تأمین امنیت طرح‌های PEKS در برابر KGA از طرف متخاصم داخلی (سرویس‌دهنده ابری) علاوه بر متخاصم خارجی، با بکارگیری ایده استفاده از روش‌های توافق کلید در PEKS، مفهوم رمزگذاری کلیدعمومی احراز اصالت شده با قابلیت جستجوی کلیدواژه (PAEKS [3]) را معرفی کردند [۸]. در PAEKS فرستنده داده نیز به یک جفت کلید خصوصی و عمومی مجهز است. این کلید خصوصی در تولید متن رمزی و کلید عمومی متناظر نیز در تولید دریچه استفاده می‌شود. به این ترتیب، دریچه‌ها مختص فرستنده داده هستند و نمی‌توان از دریچه تولید شده برای جستجو بر روی داده‌های رمزگذاری شده توسط یک فرستنده، در جستجو بر روی داده‌های یک فرستنده دیگر استفاده کرد. در نتیجه، امنیت در برابر KGA از طرف متخاصمین داخلی و خارجی بدست می‌آید. با این وجود، مدل امنیتی ارائه شده در [۸] دارای اشکالاتی بود که در کارهای بعدی برطرف گردیده و طرح‌های امنی پیشنهاد شد که عدم تمایز دریچه را در برابر هر متخاصمی فراهم می‌کند [۹، ۱۰].

تمام طرح‌های فوق در زیرساخت کلید عمومی ارائه شده‌اند که با مسئله مدیریت کلیدهای عمومی مواجه هستند. به عبارتی زمانی که یک کاربر می‌خواهد از کلید عمومی کاربر دیگر استفاده کند، باید از این که کلید متعلق به فرد مورد نظر است اطمینان حاصل کند. به همین دلیل، به منظور جلوگیری از تغییر مقادیر کلید عمومی توسط متخاصم، باید یک مرجع قابل اعتماد بر روی تمامی کلیدهای عمومی گواهی‌نامه صادر کند و در هنگام استفاده از کلیدهای عمومی، اعتبار و تعلق کلید عمومی به فرد مورد نظر با استفاده از گواهی‌نامه بررسی شود. از این رو، مسئله مدیریت این گواهی‌نامه‌ها مانند ذخیره، توزیع و ابطال آنها مطرح می‌شود. برای رفع مشکل پیچیدگی مدیریت گواهی‌نامه، مفهوم رمزگذاری شناسه مبنا ارائه شده است. سپس برای افزودن قابلیت جستجو به این طرح‌ها، مفهوم رمزگذاری شناسه مبنا با قابلیت جستجوی کلیدواژه ارائه شد [۱۱–۱۵].

در یک طرح شناسه مبنا، کلید عمومی هر کاربر تابعی از شناسه او است که به راحتی قابل محاسبه می‌باشد؛ در حالی که کلید خصوصی او توسط یک مرجع قابل اعتماد به نام تولید کننده کلید خصوصی (PKG [4]) محاسبه می‌شود. به این ترتیب برای احراز اصالت کلیدهای عمومی نیازی به مدیریت گواهی‌نامه‌ها نخواهد بود.

اگرچه با روش‌های شناسه‌مبنا مشکل مدیریت گواهی‌نامه حل می‌شود، اما چون PKG به کلیدهای خصوصی دسترسی دارد، نگرانی جدیدی به نام امان‌سپاری کلید ایجاد می‌شود. برای غلبه بر هر دو مشکل مدیریت گواهی‌نامه و امان‌سپاری کلید به طور همزمان، اولین طرح PEKS فاقد گواهی‌نامه (CLPEKS [5]) توسط پنگ و همکاران ارائه شد [۱۶].

در طرح‌های فاقد گواهی‌نامه نیز موجودیتی به نام مرکز تولید کلید (KGC [6]) وجود دارد؛ با این حال، این مرکز تنها بخشی از کلیدهای خصوصی افراد که «کلید خصوصی جزئی» نامیده می‌شود را تولید می‌کند و خود کاربران، کلیدهای خصوصی نهایی را تولید می‌کنند. نویسندگان در [۱۶] ادعا کردند که طرح CLPEKS ارائه شده توسط آنها غیرقابل تمایز بودن متون رمزی جستجوپذیر و امنیت در برابر KGAها را فراهم می‌کند. با این وجود، در [۱۷] نشان داده شد که این طرح در برابر KGAهای انجام شده توسط KGC ایمن نیست. در [۱۸] و [۱۹]، نویسندگان دو طرح CLPEKS دیگر پیشنهاد کردند که به طور ایمن غیرقابل تمایز بودن متون رمزی جستجوپذیر را فراهم می‌کند.

به منظور تأمین امنیت در برابر KGAهایی که توسط افراد خارجی انجام می‌شود، یک طرح CLPEKS با آزمایش‌گر خاص توسط ما و همکاران پیشنهاد شد [۲۰] که در آن سرویس‌دهنده برای اجرای الگوریتم آزمایش باید کلیدواژه جستجو شده را بداند. بنابراین، این طرح حریم خصوصی کلیدواژه‌ها را که حداقل نیاز امنیتی یک طرح SE است، برآورده نمی‌کند. بعدها در سال ۲۰۱۹، پاک‌نیت طرح CLPEKS با آزمایش‌گر خاص دیگری را پیشنهاد کرد [۲۱] که غیرقابل تمایز بودن متون رمزی جستجوپذیر را همراه با مقاومت در برابر KGAهایی که توسط متخاصمان خارجی انجام می‌شود، ارائه می‌دهد. برای اطمینان از امنیت در برابر KGA توسط سرویس‌دهنده، محققان مفهوم PAEKS فاقد گواهی‌نامه

[1] Public Key Encryption with Keyword Search [2] Keyword Guessing Attack [3] Public Key Authenticated Encryption with Keyword Search

[4] Private Key Generator [5] Certificateless Public Key Encryption with Keyword Search [6] Key Generation Center

(CLPAEKS [1]) را پیشنهاد دادند [۲۲، ۲۳].

در سال ۲۰۲۰ پاک‌نیت و همکاران کاستی‌های مربوط به مدل‌های امنیتی CLPAEKS موجود را بررسی کرده و متوجه شدند که طرح‌های موجود از برخی اشکالات جدی رنج می‌برند که تقریباً تمام پتانسیل‌های مفهوم تعریف شده را از بین می‌برد [۲۴]. بنابراین، نویسندگان مدل امنیتی CLPAEKS را بهبود بخشیده و یک طرح جدید پیشنهاد کردند که در مدل امنیتی بهبود یافته به‌طور قابل اثبات ایمن است.

طرح‌های فاقد گواهی‌نامه ذکر شده در بالا از عملیات زوج‌نگاری دوخطی، که از نظر محاسباتی هزینه‌بر بوده و برای دستگاه‌های با محدودیت منابع مناسب نیستند، استفاده می‌کنند. زوج‌نگاری دوخطی به مقدار قابل توجهی از منابع محاسباتی نیاز دارد؛ از این رو به سرعت باتری دستگاه‌ها را تخلیه می‌کند و همچنین با طولانی‌تر کردن زمان پاسخگویی، کارایی را به شدت کاهش می‌دهد. برای غلبه بر این مسئله، روش‌هایی بدون زوج‌نگاری دوخطی در ادبیات موضوع پیشنهاد شد.

در سال ۲۰۱۹، لو و لی یک طرح CLPEKS کارا که در آن از عملگر هزینه‌بر زوج‌نگاری دوخطی استفاده نشده را پیشنهاد دادند و ادعا کردند که طرح آنها غیرقابل تمایز بودن متون رمزی را در برابر حملات کلیدواژه منتخب وفقی فراهم می‌کند [۲۵]. با این حال، ما و همکاران ثابت کردند که طرح لو و لی تمایزناپذیری متون رمزی را فراهم نمی‌کند [۲۶]. نویسندگان همچنین یک طرح CLPEKS بدون زوج‌نگاری دوخطی جدید پیشنهاد کردند و ثابت کردند که طرح آنها می‌تواند در برابر KGA انجام شده توسط متخاصمان خارجی مقاومت کند.

لو و همکاران اولین طرح CLPAEKS بدون زوج‌نگاری دوخطی را پیشنهاد کردند [۲۷]. با این حال، همان‌طور که در [۲۸] نشان داده شده این طرح کاملاً ناامن است. نویسندگان در [۲۸] همچنین یک طرح CLPAEKS بدون زوج‌نگاری دوخطی کارا ارائه کرده و اثبات کردند که طرحشان می‌تواند در برابر KGA انجام شده توسط متخاصمان داخلی و خارجی مقاومت کند.

اخیرا در سال ۲۰۲۴ سنوسی و همکاران یک طرح CLPAEKS جدید فاقد زوج‌نگاری دوخطی و سبک وزن با ادعای تضمین ویژگی «تمایزناپذیری چند دریچه‌ای» ارائه کرده‌اند [۲۹]. ویژگی تمایزناپذیری چند دریچه‌ای بدین معناست که متخاصم نتواند بین دو مجموعه از دریچه‌ها که توسط دو مجموعه از کلیدواژه‌ها ساخته شده‌اند، تمایز قائل شود. به عبارتی یعنی حتی اگر متخاصم به چند دریچه دسترسی داشته باشد، نمی‌تواند مشخص کند که کدام دریچه به کدام مجموعه کلیدواژه تعلق دارد.

طرح ارائه شده توسط سنوسی و همکاران قصد دارد یک کلید مشترک را که تنها فرستنده و گیرنده قادر به محاسبه آن هستند در متن رمزی و دریچه تعبیه کند تا بدین طریق ویژگی‌های احراز اصالت و امنیت در برابر KGA را فراهم کند. همچنین با غیرقطعی‌سازی دریچه‌ها با استفاده از مقادیر تصادفی، ویژگی تمایزناپذیری چند دریچه‌ای را تأمین کند. سنوسی و همکاران ادعا کرده‌اند که طرح پیشنهاد شده توسط آنها ایمن بوده و از نظر ویژگی‌های امنیتی، هزینه‌های محاسباتی و هزینه‌های ارتباطی از سایر طرح‌های موجود بهتر عمل می‌کند. با این حال، در این مقاله نشان خواهیم داد که این طرح از چندین مشکل امنیتی رنج برده و ناامن است.

به عبارت دقیق‌تر، اولاً نشان خواهیم داد که طرح ارائه شده توسط سنوسی و همکاران علی‌رغم اینکه در تنظیمات فاقد گواهی‌نامه ارائه شده است، ویژگی فاقد گواهی‌نامه بودن را احراز نمی‌کند و نیاز به گواهی‌نامه برای کلیدهای عمومی همچنان وجود دارد؛ چرا که در صورت عدم وجود گواهی‌نامه، متخاصم می‌تواند خود را به جای شخص دیگر جا زده و با داشتن مقادیر خصوصی متناظر با کلیدعمومی ادعا شده، عملیات منحصر به آن شخص را به جای او انجام دهد. همچنین نشان خواهیم داد که برخلاف ادعای سنوسی و همکاران، طرح ارائه شده توسط آنها دارای ویژگی‌های تمایزناپذیری متون رمزی و تمایزناپذیری چند دریچه‌ای نیست.

در ادامه ابتدا در بخش ۲، چارچوب کلی و مدل امنیتی طرح‌های CLPAEKS مرور می‌شود. سپس در بخش ۳، جزئیات طرح CLPAEKS پیشنهاد شده توسط سنوسی و همکاران بیان خواهد شد. در بخش ۴، به تحلیل امنیت طرح سنوسی و همکاران پرداخته و نشان می‌دهیم که این طرح ویژگی‌های فاقد گواهینامه بودن و تمایزناپذیری متون رمزی و دریچه‌ها را تأمین نمی‌کند. در نهایت، نتیجه‌گیری در بخش ۵ ارائه خواهد شد.

۲ رمزگذاری جستجوپذیر احراز اصالت شده فاقد گواهی‌نامه

در این بخش، ابتدا چارچوب کلی یک طرح CLPAEKS را شرح داده و سپس الزامات امنیتی آن را بیان می‌کنیم.

۱.۲ چارچوب کلی

یک طرح CLPAEKS از ۸ الگوریتم زیر تشکیل شده است [۲۹].

راه‌اندازی: این الگوریتم توسط مرکز تولید کلید (KGC) اجرا شده و با دریافت پارامتر امنیتی λ به عنوان ورودی، کلید مخفی اصلی s و پارامترهای عمومی سیستم PP را برمی‌گرداند. s توسط KGC مخفی نگه داشته شده و PP منتشر می‌شود.

استخراج کلید خصوصی جزئی: این الگوریتم توسط KGC اجرا شده و با دریافت پارامترهای عمومی سیستم PP، کلید مخفی اصلی s و شناسه کاربر id_U به عنوان ورودی، کلید خصوصی و عمومی جزئی psk_U و ppk_U را به کاربر برمی‌گرداند.

تعیین مقدار مخفی: این الگوریتم توسط کاربر U، که می‌تواند فرستنده یا گیرنده باشد، اجرا شده و مقدار مخفی x_U را برمی‌گرداند.

[1] Certificateless Public Key Authenticated Encryption with Keyword Search

تعیین کلید خصوصی: این الگوریتم توسط کاربر U اجرا شده و با دریافت کلید خصوصی جزئی کاربر psk_U و مقدار مخفی او x_U به عنوان ورودی، کلید خصوصی کاربر sk_U را برمی‌گرداند.

تعیین کلید عمومی: این الگوریتم توسط کاربر U اجرا شده و با دریافت پارامترهای عمومی سیستم PP، مقدار مخفی کاربر x_U و کلید عمومی جزئی او ppk_U به عنوان ورودی، کلید عمومی کاربر pk_U را برمی‌گرداند.

تولید متن رمزی: این الگوریتم توسط یک فرستنده اجرا شده و با دریافت پارامترهای عمومی سیستم PP، کلید خصوصی فرستنده sk_S، شناسه گیرنده id_R، کلید عمومی گیرنده pk_R و کلیدواژه w به عنوان ورودی، متن رمزی C_w را برمی‌گرداند.

تولید دریچه: این الگوریتم توسط گیرنده اجرا شده و با دریافت پارامترهای عمومی سیستم PP، کلید خصوصی گیرنده sk_R، کلید عمومی گیرنده pk_R، شناسه فرستنده id_S، کلید عمومی فرستنده pk_S و کلید واژه w' به عنوان ورودی، دریچه $T_{w'}$ را برمی‌گرداند.

آزمایش: این الگوریتم توسط سرویس‌دهنده ابری اجرا شده و با دریافت پارامترهای عمومی سیستم PP، کلید عمومی فرستنده pk_S، کلید عمومی گیرنده pk_R، یک متن رمزی C_w و یک دریچه T_w به عنوان ورودی، اگر C_w و T_w حاوی یک کلیدواژه باشند $\top$ و در غیر این صورت $\perp$ را برمی‌گرداند.

۲.۲ مدل امنیتی

در این بخش، مدل امنیتی در نظر گرفته شده برای یک طرح CLPAEKS در [۲۹] را ارائه می‌کنیم.

یک طرح رمزگذاری جستجوپذیر احراز اصالت شده فاقد گواهی‌نامه را امن گویند هرگاه ویژگی‌های تمایزناپذیری دریچه و تمایزناپذیری متن رمزی را در برابر متخاصمین ممکن تأمین کند. به طور معمول، امنیت سیستم‌های رمزنگاری فاقد گواهی‌نامه را در برابر دو نوع متخاصم بررسی می‌کنند:

(۱) متخاصم نوع ۱ ($\mathcal{A}_1$) که قادر است کلید عمومی هر کاربری را با هر مقدار دلخواهی جایگزین کند، اما به کلید مخفی اصلی دسترسی ندارد. این متخاصم شبیه‌ساز یک کاربر بیرونی است که سعی می‌کند با تغییر کلیدهای عمومی و با توجه به عدم نیاز به گواهی‌نامه در سیستم‌های فاقد گواهی‌نامه، مزایایی به دست آورد.

(۲) متخاصم نوع ۲ ($\mathcal{A}_2$) که به کلید مخفی اصلی دسترسی دارد، اما قادر به تعویض کلیدهای عمومی نیست. این متخاصم شبیه‌ساز یک مرکز تولید کلید بداندیش است که تلاش می‌کند با استفاده از دسترسی‌های خود، مزایایی را به دست آورد.

با توجه به توضیحات بالا، امنیت یک طرح CLPAEKS از طریق ۴ بازی مابین متخاصمین ممکن و یک چالشگر بررسی می‌شود که از طریق هر یک از این ۴ بازی، متخاصم (نوع ۱ یا ۲) قادر به انجام تعدادی محدود به چندجمله‌ای پرسش از چالشگر بوده و هدف او نقض یکی از ویژگی‌های تمایزناپذیری مورد نیاز این طرح‌ها (تمایزناپذیری متون رمزی یا تمایزناپذیری دریچه‌ها) است. با توجه به محدودیت تعداد صفحه، در اینجا تنها ۲ بازی از ۴ بازی مورد نظر را ارائه خواهیم کرد: بازی ۱ یعنی تمایزناپذیری متون رمزی در برابر متخاصم نوع ۱ و بازی ۲ یعنی تمایزناپذیری دریچه‌ها در برابر متخاصم نوع ۲.

۱.۲.۲ تمایزناپذیری متون رمزی

تمایزناپذیری متون رمزی در یک طرح CLPAEKS با استفاده از دو بازی در برابر متخاصمین نوع ۱ و ۲ بررسی می‌شود که همان‌طور که بیان شد، در اینجا تنها بازی در برابر متخاصم نوع ۱ ارائه خواهد شد.

بازی ۱: این بازی بین $\mathcal{A}_1$ و یک چالشگر B انجام شده و از مراحل زیر تشکیل شده است:

- **شروع.** در این مرحله، چالشگر با ورودی پارامتر امنیتی λ، الگوریتم راه‌اندازی طرح CLPAEKS را اجرا کرده، پارامترهای عمومی سیستم PP و کلید خصوصی اصلی s را به دست آورده، و PP را در اختیار $\mathcal{A}_1$ قرار می‌دهد.
- **فاز ۱.** در این فاز، $\mathcal{A}_1$ می‌تواند به صورت وفقی تعدادی (محدود به چندجمله‌ای) پرسش از B انجام داده و پاسخ آنها را دریافت نماید. پرسش‌های قابل انجام توسط $\mathcal{A}_1$ به شرح زیر هستند:

(آ) **ایجاد کاربر.** با دریافت id_u به عنوان ورودی، در صورتی که کاربر متناظر با این شناسه ایجاد شده باشد، چالشگر کلید عمومی pk_u را باز می‌گرداند؛ در غیر این صورت، کاربر جدید متناظر با این شناسه با تولید (sk_u, pk_u) به عنوان کلید خصوصی و عمومی متناظر ایجاد شده و pk_u به متخاصم بازگردانده می‌شود. در مورد پرسش‌هایی که در ادامه مطرح می‌شوند فرض می‌کنیم که کاربر با شناسه‌های مورد پرسش وجود دارد؛ در صورتی که چنین نباشد، ابتدا کاربر مورد نظر ایجاد و سپس پرسش پاسخ داده می‌شود.

(ب) **استخراج کلید خصوصی جزئی.** با دریافت شناسه id_u به عنوان ورودی، کلید خصوصی جزئی متناظر psk_u بازگردانده می‌شود.

(ج) **استخراج مقدار مخفی.** با دریافت شناسه id_u به عنوان ورودی، مقدار مخفی متناظر x_u بازگردانده می‌شود.

(د) **درخواست کلید عمومی.** با دریافت شناسه id_u به عنوان ورودی، کلید عمومی متناظر pk_u بازگردانده می‌شود.

(ه) **تغییر کلید عمومی.** با دریافت شناسه id_u و کلید عمومی pk'_u به عنوان ورودی، چالشگر مقدار pk'_u را جایگزین کلید عمومی کاربر یعنی pk_u می‌کند.

(و) **تولید متن رمزی.** با دریافت شناسه یک فرستنده id_S، شناسه یک گیرنده id_R و کلیدواژه w به عنوان ورودی، یک متن رمزی متناظر C_w تولید و بازگردانده می‌شود.

(ز) **تولید دریچه.** با دریافت شناسه یک فرستنده id_S، شناسه یک گیرنده id_R و کلیدواژه w' به عنوان ورودی، یک دریچه متناظر $T_{w'}$ تولید و بازگردانده می‌شود.

- **چالش.** بعد از اتمام فاز ۱، $\mathcal{A}_1$ شناسه یک فرستنده id_S^*، شناسه یک گیرنده id_R^* و دو کلیدواژه w_0 و w_1 را خروجی می‌دهد. در ادامه، B مقدار تصادفی $b \in \{0,1\}$ را انتخاب کرده، متن رمزی متناظر با کلیدواژه w_b با فرستنده با شناسه id_S^* و گیرنده با شناسه id_R^* را ایجاد کرده و به $\mathcal{A}_1$ بازمی‌گرداند.
- **فاز ۲.** در این فاز، $\mathcal{A}_1$ می‌تواند همانند فاز ۱ مجموعه‌ای از پرسش‌ها را از چالشگر انجام داده و پاسخ متناظر را دریافت کند.
- **حدس.** متخاصم $\mathcal{A}_1$ حدس خود از کلیدواژه رمزگذاری‌شده را از طریق بیت $b' \in \{0,1\}$ اعلام می‌کند.

متخاصم $\mathcal{A}_1$ برنده بازی ۱ است اگر $b = b'$ و شرایط زیر نیز برقرار باشد:

(آ) پرسش استخراج کلید خصوصی جزئی با ورودی شناسه‌های id_S^* و id_R^* در هیچ یک از فازهای ۱ و ۲ انجام نشده باشد.

(ب) پرسش تولید دریچه با ورودی شناسه‌های id_S^* و id_R^* و هر یک از کلیدواژه‌های w_0 و w_1 در هیچ یک از فازهای ۱ و ۲ انجام نشده باشد.

۲.۲.۲ تمایزناپذیری دریچه‌ها

تمایزناپذیری دریچه‌ها در یک طرح CLPAEKS نیز با استفاده از دو بازی در برابر متخاصمین نوع ۱ و ۲ بررسی می‌شود که همان‌طور که بیان شد، در اینجا تنها بازی در برابر متخاصم نوع ۲ ارائه خواهد شد.

بازی ۲: این بازی بین $\mathcal{A}_2$ و یک چالشگر B انجام شده و از مراحل زیر تشکیل شده است:

- **شروع.** در این مرحله، چالشگر با ورودی پارامتر امنیتی λ، الگوریتم راه‌اندازی طرح CLPAEKS را اجرا کرده، پارامترهای عمومی سیستم PP و کلید خصوصی اصلی s را به دست آورده و در اختیار $\mathcal{A}_2$ قرار می‌دهد.
- **فاز ۱.** در این فاز، $\mathcal{A}_2$ می‌تواند به صورت وفقی تعدادی (محدود به چندجمله‌ای) پرسش از B انجام داده و پاسخ آنها را دریافت نماید. ایجاد کاربر، استخراج مقدار مخفی، درخواست کلید عمومی، تولید متن رمزی و تولید دریچه انواع پرسش‌های قابل انجام توسط $\mathcal{A}_2$ در این فاز بوده و B همانند بازی ۱ پاسخ‌های مربوطه را در اختیار او قرار می‌دهد.
- **چالش.** بعد از اتمام فاز ۱، $\mathcal{A}_2$ شناسه یک فرستنده id_S^*، شناسه یک گیرنده id_R^* و دو چندتایی متمایز از کلیدواژه‌ها

$$\overrightarrow{w_0} = (w_{0,1}, \cdots, w_{0,n}), \quad \overrightarrow{w_1} = (w_{1,1}, \cdots, w_{1,n})$$

را خروجی می‌دهد. در ادامه، B مقدار تصادفی $b \in \{0,1\}$ را انتخاب کرده، دریچه‌های متناظر با چندتایی کلیدواژه‌های $\overrightarrow{w_b}$ با فرستنده با شناسه id_S^* و گیرنده با شناسه id_R^* را ایجاد کرده و به $\mathcal{A}_2$ بازمی‌گرداند.

- **فاز ۲.** در این فاز، $\mathcal{A}_2$ می‌تواند همانند فاز ۱ مجموعه‌ای از پرسش‌ها را از چالشگر انجام داده و پاسخ متناظر را دریافت کند.
- **حدس.** متخاصم $\mathcal{A}_2$ حدس خود از بیت انتخاب شده توسط چالشگر را از طریق بیت $b' \in \{0,1\}$ اعلام می‌کند.

متخاصم $\mathcal{A}_2$ برنده بازی ۲ است اگر $b = b'$ و شرایط زیر نیز برقرار باشد:

(آ) پرسش استخراج کلید خصوصی جزئی با ورودی شناسه‌های id_S^* و id_R^* در هیچ یک از فازهای ۱ و ۲ انجام نشده باشد.

(ب) پرسش تولید متن رمزی با ورودی شناسه‌های id_S^* و id_R^* و هر یک از کلیدواژه‌های موجود در چندتایی‌های $\overrightarrow{w_0}$ و $\overrightarrow{w_1}$ در هیچ یک از فازهای ۱ و ۲ انجام نشده باشد.

۳ مرور طرح سنوسی و همکاران

در این بخش، جزئیات طرح CLPAEKS سبک وزن ارائه شده توسط سنوسی و همکاران [۲۹] را بیان می‌کنیم.

راه‌اندازی $(PP, s \leftarrow (\lambda)$: در این الگوریتم، KGC با دریافت پارامتر امنیتی λ به عنوان ورودی، به صورت زیر عمل می‌کند:

(۱) گروه دوری جمعی G از مرتبه $q > 2^\lambda$ و عنصر P را به عنوان مولد G انتخاب می‌کند.

(۲) مقدار تصادفی $s \in Z_q^*$ را به عنوان کلید مخفی اصلی انتخاب کرده و کلید عمومی $P_{pub} = s.P$ را محاسبه می‌کند.

(۳) توابع درهم‌ساز

$$H_1 : \{0,1\}^* \to Z_q^*,$$
$$H_2 : \{0,1\}^* \times G \to Z_q^*,$$
$$H_3 : G \times G \times G \times G \times G \to Z_q^*$$

را انتخاب می‌کند.

(۴) در نهایت، پارامترهای عمومی سیستم

$$PP := \{q, G, P, P_{pub}, H_1, H_2, H_3\}$$

را منتشر و کلید مخفی اصلی s را مخفیانه نگهداری می‌کند.

استخراج کلید خصوصی جزئی $(psk_U, ppk_U) \leftarrow (PP, s, id_U)$: در این الگوریتم، KGC با دریافت پارامترهای عمومی سیستم PP، کلید مخفی اصلی s و id_U یعنی شناسه کاربر U به عنوان ورودی، به صورت زیر عمل می‌کند:

(۱) مقدار تصادفی $y_U \in Z_q^*$ را انتخاب می‌کند.

(۲) مقدار $psk_U = y_U + s \,.\, H_1(id_U) \bmod q$ را به عنوان کلید خصوصی جزئی کاربر و $ppk_U = y_U.P$ را به عنوان کلید عمومی جزئی کاربر محاسبه می‌کند.

(۳) مقادیر (psk_U, ppk_U) را از طریق یک کانال امن به کاربر باز می‌گرداند.

تعیین مقدار مخفی $x_U \leftarrow (PP)$: در این الگوریتم، کاربر U با دریافت پارامترهای عمومی سیستم PP به عنوان ورودی، به صورت زیر عمل می‌کند:

(۱) مقدار تصادفی $x_U \in Z_q^*$ را انتخاب و مخفیانه نگهداری می‌کند.

تعیین کلید خصوصی $sk_U \leftarrow (psk_U, x_U)$: در این الگوریتم، کاربر U با دریافت کلید خصوصی جزئی خود psk_U و مقدار مخفی خود x_U به عنوان ورودی، به صورت زیر عمل می‌کند:

(۱) مقدار $sk_U = (psk_U, x_U)$ را به عنوان کلید خصوصی خود قرار می‌دهد.

تعیین کلید عمومی $pk_U \leftarrow (PP, x_U, ppk_U)$: در این الگوریتم، کاربر U با دریافت پارامترهای عمومی سیستم PP، مقدار مخفی خود x_U و کلید عمومی جزئی خود ppk_U به عنوان ورودی، به صورت زیر عمل می‌کند:

(۱) مقدار $mpk_U = x_U P$ را محاسبه و $pk_U = (ppk_U, mpk_U)$ را به عنوان کلید عمومی خود قرار می‌دهد.

تولید متن رمزی $C_w \leftarrow (PP, sk_S, id_R, pk_R, w)$: در این الگوریتم، فرستنده با دریافت پارامترهای عمومی سیستم PP، کلید خصوصی فرستنده $sk_S = (psk_S, x_S)$، شناسه گیرنده id_R، کلید عمومی گیرنده $pk_R = (ppk_R, mpk_R)$ و کلیدواژه w به عنوان ورودی، به صورت زیر عمل می‌کند:

(۱) مقدار زیر را محاسبه می‌کند:

$$K = psk_S.mpk_R + x_S.(ppk_R + H_1(id_R).P_{pub})$$

(۲) متن رمزی $C_w = H_2(w, K)$ را محاسبه کرده و برمی‌گرداند.

تولید دریچه $T_{w'} \leftarrow (PP, sk_R, pk_R, id_S, pk_S, w')$: در این الگوریتم، گیرنده با دریافت پارامترهای عمومی سیستم PP، کلید خصوصی گیرنده $sk_R = (psk_R, x_R)$، کلید عمومی گیرنده $pk_R = (ppk_R, mpk_R)$، شناسه فرستنده id_S، کلید عمومی فرستنده $pk_S = (ppk_S, mpk_S)$ و کلیدواژه w' به عنوان ورودی، به صورت زیر عمل می‌کند:

(۱) مقدار زیر را محاسبه می‌کند:

$$K' = psk_R.mpk_S + x_R.(ppk_S + H_1(id_S).P_{pub})$$

(۲) مقدار تصادفی $r \in Z_q^*$ را انتخاب و $T_1 = r.P$ را محاسبه می‌کند.

(۳) مقدار $T_2 = H_3(A, ppk_S, mpk_S, ppk_R, mpk_R)$ را محاسبه می‌کند که در آن T_1 . $A = H_2(w', K')$ است.

(۴) دریچه $T_{w'} = (T_1, T_2)$ را برمی‌گرداند.

آزمایش $\top / \perp \leftarrow (PP, pk_S, pk_R, C_w, T_{w'})$: در این الگوریتم، سرویس‌دهنده ابری با دریافت پارامترهای عمومی سیستم PP، کلید عمومی فرستنده $pk_S = (ppk_S, mpk_S)$، کلید عمومی گیرنده $pk_R = (ppk_R, mpk_R)$، متن رمزی C_w و دریچه $T_{w'} = (T_1, T_2)$ به عنوان ورودی، به صورت زیر عمل می‌کند:

(۱) مقدار $T_2' = H_3(B, ppk_S, mpk_S, ppk_R, mpk_R)$ را محاسبه می‌کند که در آن $B = C_w.T_1$ است.

(۲) اگر $T_2 = T_2'$، $\top$ و در غیر این صورت $\perp$ را برمی‌گرداند.

۴ تحلیل امنیت طرح سنوسی و همکاران

در این بخش به تحلیل امنیت طرح CLPAEKS پیشنهاد شده توسط سنوسی و همکاران در [۲۹] می‌پردازیم.

متأسفانه علی‌رغم اینکه این طرح در تنظیمات فاقد گواهی‌نامه ارائه شده است، ویژگی فاقد گواهی‌نامه بودن را احراز نمی‌کند. به عبارت دقیق‌تر نیاز به گواهی‌نامه برای کلیدهای عمومی همچنان وجود دارد؛ چرا که در صورت عدم وجود گواهی‌نامه، متخاصم می‌تواند خود را به جای شخص دیگر جا زده و با داشتن مقادیر خصوصی متناظر با کلیدعمومی ادعا شده، عملیات منحصر به آن شخص را به جای او انجام دهد. در ادامه، این مطلب تحت عنوان قضیه ۱ به طور رسمی نشان داده شده است.

همچنین طبق ادعای سنوسی و همکاران، طرح ارائه شده توسط آنها دارای ویژگی تمایزناپذیری متون رمزی است. در اینجا در قضیه ۲ نشان می‌دهیم که این ادعا صحیح نبوده و متخاصم می‌تواند متون رمزی را از یکدیگر تمایز دهد.

آنها همچنین ادعا کردند که طرحشان دارای ویژگی تمایزناپذیری چند دریچه‌ای است. با این حال در قضیه ۳ نشان می‌دهیم که این طرح نه تنها این ویژگی، بلکه ویژگی ضعیف‌تر تمایزناپذیری دریچه را نیز تأمین نمی‌کند.

قضیه ۱. طرح ارائه شده در [۲۹]، ویژگی فاقد گواهی‌نامه بودن را فراهم نمی‌کند. به عبارت دقیق‌تر، هر یک از کاربران در این طرح می‌تواند با استفاده از کلید خصوصی جزئی خود، کلید خصوصی جزئی معتبر برای سایرین بسازد.

اثبات: برای اثبات این قضیه نشان می‌دهیم که در طرح مذکور، متخاصم نوع ۱ می‌تواند با دسترسی به یک کلید خصوصی جزئی، کلید خصوصی متناظر با هر شناسه دلخواهی را ایجاد کرده و در ادامه با انتخاب مقدار مخفی و محاسبه کلید عمومی، خود را به جای او جا بزند. در ادامه نشان می‌دهیم که $\mathcal{A}_1$ چگونه این کار را انجام می‌دهد.

فرض کنیم $\mathcal{A}_1$ به کلید خصوصی و عمومی جزئی متناظر با شناسه id دسترسی یابد. با توجه به الگوریتم استخراج کلید خصوصی جزئی در این طرح، کلیدهای خصوصی و عمومی جزئی به صورت زیر هستند:

$$(psk_{id}, ppk_{id}) = (y_{id} + s.H_1(id), y_{id}.P)$$

$\mathcal{A}_1$ می‌تواند با استفاده از مقادیر فوق، کلید خصوصی و عمومی جزئی متناظر با کاربر دلخواه با شناسه id' را به صورت زیر تولید کند:

$$(psk_{id'}, ppk_{id'}) = \left(\frac{H_1(id')}{H_1(id)} psk_{id}, \frac{H_1(id')}{H_1(id)} ppk_{id}\right)$$

به این ترتیب خواهیم داشت:

$$\begin{aligned}(psk_{id'}, ppk_{id'}) &= \left(\frac{y_{id}.H_1(id')}{H_1(id)} + s.H_1(id'), \frac{y_{id}.H_1(id')}{H_1(id)}.P\right)\\ &= (y'_{id'} + s.H_1(id'), y'_{id'}.P)\end{aligned}$$

که یک جفت کلید خصوصی و عمومی جزئی صحیح و معتبر برای کاربر با شناسه id' است. □

قضیه ۲. طرح ارائه شده در [۲۹]، ویژگی تمایزناپذیری متون رمزی را فراهم نمی‌کند.

اثبات: برای نقض تمایزناپذیری متون رمزی در این طرح، در بازی ۱ متخاصم $\mathcal{A}_1$ در تعامل با چالشگر B به صورت زیر عمل می‌کند:

- در فاز ۱، پرسش «ایجاد کاربر» را با ورودی شناسه‌های id_S و id_R انجام داده و کلیدهای عمومی pk_S و pk_R را در پاسخ دریافت می‌کند. سپس پرسش «استخراج مقدار مخفی» را با ورودی شناسه‌های id_S و id_R انجام داده و مقادیر x_S و x_R را به عنوان پاسخ دریافت می‌نماید.
- در مرحله چالش، کلیدواژه‌های w_0 و w_1 را انتخاب کرده و به همراه شناسه‌های id_S و id_R به B ارسال می‌کند. در ادامه B مقدار تصادفی $b \in \{0,1\}$ را انتخاب و متن رمزی حاصل از رمزگذاری w_b با شناسه فرستنده id_S و شناسه گیرنده id_R را تولید و به $\mathcal{A}_1$ ارسال می‌کند.
- در مرحله حدس، $\mathcal{A}_1$ با استفاده از مقادیر x_S و x_R و شناسه‌ها و مقادیر عمومی متناظر با فرستنده و گیرنده به صورت زیر عمل می‌کند:
  - مقدار زیر را محاسبه می‌کند:

$$\begin{aligned}K'' &= x_R.(ppk_S + H_1(id_S).P_{pub})\\ &+ x_s.(ppk_R + H_1(id_R).P_{pub})\end{aligned}$$

  - در صورتی که $H_2(w_1, K'') = H_2(w_1, K')$ برابر با متن رمزی دریافتی از B باشد، $b' = 1$ و در غیر این‌صورت $b' = 0$ را خروجی می‌دهد.

به راحتی می‌توان نشان داد که $K = K''$ و در نتیجه در پایان حمله بیان شده، $b = b'$ خواهد بود و متخاصم با قطعیت می‌تواند کلیدواژه متناظر با متن رمزی دریافتی از چالشگر را تعیین کند. □

قضیه ۳. طرح ارائه شده در [۲۹]، ویژگی تمایزناپذیری دریچه‌ها را فراهم نمی‌کند.

اثبات: برای نقض تمایزناپذیری دریچه‌ها در این طرح، در بازی ۲ متخاصم $\mathcal{A}_2$ در تعامل با چالشگر B به صورت زیر عمل می‌کند:

- در فاز ۱، یک پرسش «ایجاد کاربر» را با ورودی شناسه‌های id_S و id_R انجام داده و کلیدهای عمومی pk_S و pk_R را در پاسخ دریافت می‌کند.
- در مرحله چالش، کلیدواژه‌های w_0 و w_1 را انتخاب کرده و به همراه شناسه‌های id_S و id_R به B ارسال می‌کند. در ادامه B مقدار تصادفی $b \in \{0,1\}$ را انتخاب و دریچه T_{w_b} متناظر با w_b و شناسه فرستنده id_S و شناسه گیرنده id_R را محاسبه کرده و به $\mathcal{A}_2$ ارسال می‌کند.
- در مرحله حدس، $\mathcal{A}_2$ با توجه به اینکه به کلیدهای خصوصی جزئی دسترسی دارد، با استفاده از مقادیر psk_S و psk_R و مقادیر عمومی متناظر با فرستنده و گیرنده به صورت زیر عمل می‌کند:
  - مقدار زیر را محاسبه می‌کند:

$$K'' = psk_S.mpk_R + psk_R.mpk_S$$

  - مقدار $C_{w_0} = H_2(w_0, K'')$ را محاسبه کرده و الگوریتم آزمایش را روی C_{w_0} و دریچه چالش T_{w_b} اجرا می‌کند. در صورت دریافت خروجی $\top$، $b' = 0$ و در غیر این‌صورت $b' = 1$ را خروجی می‌دهد.

به سادگی می‌توان نشان داد که $K'' = K'$ و در نتیجه در پایان حمله بیان شده، $b = b'$ خواهد بود و متخاصم با قطعیت می‌تواند کلیدواژه متناظر با دریچه دریافتی از چالشگر را تعیین کند. □

تذکر ۱. لازم به ذکر است که قابل تمایز بودن متون رمزی و دریچه‌ها در طرح سنوسی و همکاران که در قضایای ۲ و ۳ اثبات شد، برای همه مهاجمان چه از نوع اول ($\mathcal{A}_1$) و چه از نوع دوم ($\mathcal{A}_2$) وجود دارد. با این حال همان‌طور که بیان شد، به علت محدودیت صفحات در اینجا به اثبات تمایزپذیری متون رمزی برای $\mathcal{A}_1$ و تمایزپذیری دریچه‌ها برای $\mathcal{A}_2$ بسنده کردیم.

پیشنهاد برای بهبود طرح سنوسی و همکاران

همان‌طور که بیان شد طرح پیشنهاد شده توسط سنوسی و همکاران از دو نقطه ضعف کلیدی رنج می‌برد. اولین نقطه ضعف این روش این است که در این طرح هر کاربری با در اختیار داشتن کلید خصوصی متناظر با خود، قادر به محاسبه کلید خصوصی جزئی متناظر با هر کاربر دیگر و انجام عملیات رمزنگاشتی از سوی او است. مشکل اصلی این طرح در این زمینه، مربوط به الگوریتم تولید کلید خصوصی جزئی بوده و با استفاده از مقدار ppk_U در کنار id_U به عنوان ورودی تابع درهم‌ساز H_1، این نقطه ضعف برطرف خواهد شد.

دومین نقطه ضعف روش سنوسی و همکاران فراهم نکردن ویژگی‌های تمایزناپذیری متون رمزی و دریچه‌ها در برابر متخاصمین در نظر گرفته شده در رمزنگاری فاقد گواهی‌نامه است. این نقطه ضعف بدین جهت وجود دارد که مقادیر K و K' محاسبه شده توسط فرستنده و گیرنده، از امنیت کافی برخوردار نیست؛ یعنی ساخت این مقادیر به گونه‌ای نیست

که متخاصمین در نظر گرفته شده در رمزنگاری فاقد گواهی‌نامه نتوانند آن را محاسبه کنند. به عبارت دیگر، دسترسی به مقادیر مخفی فرستنده و گیرنده یا دسترسی به کلیدهای خصوصی جزئی فرستنده و گیرنده، برای محاسبه این مقادیر کفایت می‌کند و همان‌طور که در مورد متخاصمین در نظر گرفته شده در رمزنگاری فاقد گواهی‌نامه بیان شد، متخاصم نوع ۱ می‌تواند به مقادیر مخفی کاربران دسترسی داشته باشد و متخاصم نوع ۲، کلیدهای خصوصی جزئی کاربران را می‌داند. برای غلبه بر این نقطه ضعف، باید تولید مقادیر K و K' به گونه‌ای باشد که نیازمند دسترسی همزمان به مقدار مخفی و کلید خصوصی جزئی یکی از کاربران باشد.

۵ نتیجه‌گیری

با توجه به ارائه قابلیت جستجو بر روی داده‌های رمزگذاری‌شده و همچنین حل مسائل مدیریت گواهی‌نامه و امان‌سپاری کلید، رمزگذاری جستجوپذیر فاقد گواهی‌نامه در دهه اخیر به شدت مورد توجه قرار گرفته است. با این حال، ارائه طرح‌های رمزگذاری جستجوپذیر امن در سیستم‌های فاقد گواهی‌نامه، مساله‌ای بسیار چالشی بوده و بررسی پیشینه موضوع نشان می‌دهد که اغلب طرح‌های پیشنهاد شده ناامن هستند.

در این مقاله به تحلیل امنیت یکی از طرح رمزگذاری جستجوپذیر فاقد گواهی‌نامه سبک وزن که اخیراً توسط سنوسی و همکاران پیشنهاد شده است می‌پردازیم. این طرح اگر چه برخلاف بسیاری از طرح‌های ارائه شده در ادبیات موضوع، از عملیات زمان‌بر زوج‌نگاری دوخطی استفاده نمی‌کند تا مناسب استفاده در دستگاه‌های با محدودیت منابع باشد، اما در این مقاله نشان می‌دهیم که متاسفانه این طرح از چندین مشکل امنیتی بسیار مهم رنج می‌برد. به عبارت دقیق‌تر، در اینجا نشان می‌دهیم که طرح مذکور اولاً ویژگی فاقد گواهی‌نامه بودن را احراز نکرده و کاربران می‌توانند خود را به جای شخصی دیگر جا بزنند. به علاوه اثبات می‌کنیم که برخلاف ادعای سنوسی و همکاران، طرح ارائه شده توسط آنها نیازمندی‌های ضروری تمایزناپذیری متون رمزی و تمایزناپذیری دریچه را برآورده نمی‌کند.

مراجع

[1] Dawn Xiaoding Song, David Wagner, and Adrian Perrig. Practical techniques for searches on encrypted data. In *Proceeding 2000 IEEE symposium on security and privacy. S&P 2000*, pages 44–55. IEEE, 2000.

[2] Dhruti Sharma. Searchable encryption : A survey. *Information Security Journal: A Global Perspective*, 32(2):76–119, 2023.

[3] Feng Li, Jianfeng Ma, Yinbin Miao, Ximeng Liu, Jianting Ning, and Robert H. Deng. A survey on searchable symmetric encryption. *ACM Computing Surveys*, 56(5):1–42, 2023.

[4] Yunhong Zhou, Na Li, Yanmei Tian, Dezhi An, and Licheng Wang. Public key encryption with keyword search in cloud: A survey. *Entropy*, 22(4), 2020.

[5] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In *Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings 23*, pages 506–522. Springer, 2004.

[6] Jin Wook Byun, Hyun Suk Rhee, Hyun-A Park, and Dong Hoon Lee. Off-line keyword guessing attacks on recent keyword search schemes over encrypted data. In *Workshop on secure data management*, pages 75–83. Springer, 2006.

[7] Hyun Sook Rhee, Jong Hwan Park, Willy Susilo, and Dong Hoon Lee. Trapdoor security in a searchable public-key encryption scheme with a designated tester. *Journal of systems and software*, 83(5):763–771, 2010.

[8] Qiong Huang and Hongbo Li. An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks. *Information Sciences*, 403:1–14, 2017.

[9] Mahnaz Noroozi and Ziba Eslami. Public key authenticated encryption with keyword search: revisited. *IET Information Security*, 13(4):336–342, 2019.

[10] Baodong Qin, Yu Chen, Qiong Huang, Ximeng Liu, and Dong Zheng. Public-key authenticated encryption with keyword search revisited: Security model and constructions. *Information Sciences*, 516:515–528, 2020.

[11] Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions. *Journal of cryptology*, 21:350–391, 2008.

[12] Yang Lu, Gang Wang, Jiguo Li, and Jian Shen. Efficient designated server identity-based encryption with conjunctive keyword search. *Annals of Telecommunications*, 72:359–370, 2017.

[13] Eslami Z Noroozi M, Karoubi I. server identity-based encryption with keyword search scheme: still unsolved.

Annals of Telecommunications, 73:769–776, 2018.

[14] Hongbo Li, Qiong Huang, Jian Shen, Guomin Yang, and Willy Susilo. Designated-server identity-based authenticated encryption with keyword search for encrypted emails. *Information Sciences*, 481:330–343, 2019.

[15] Nasrollah Pakniat Danial Shiraly, Ziba Eslami. Designated-tester identity-based authenticated encryption with keyword search with applications in cloud systems. *Journal of Systems Architecture*, 152, 2024.

[16] Peng Yanguo, Cui Jiangtao, Peng Changgen, and Ying Zuobin. Certificateless public key encryption with keyword search. *China Communications*, 11(11):100–113, 2014.

[17] Tsu-Yang Wu, Fanya Meng, Chien-Ming Chen, Shuai Liu, and Jeng-Shyang Pan. On the security of a certificateless searchable public key encryption scheme. In *Genetic and Evolutionary Computing: Proceedings of the Tenth International Conference on Genetic and Evolutionary Computing, November 7-9, 2016 Fuzhou City, Fujian Province, China 10*, pages 113–119. Springer, 2017.

[18] Qingji Zheng, Xiangxue Li, and Aytac Azgin. Clks: Certificateless keyword search on encrypted data. In *Network and System Security: 9th International Conference, NSS 2015, New York, NY, USA, November 3-5, 2015, Proceedings 9*, pages 239–253. Springer, 2015.

[19] Mimi Ma, Debiao He, Neeraj Kumar, Kim-Kwang Raymond Choo, and Jianhua Chen. Certificateless searchable public key encryption scheme for industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(2):759–767, 2017.

[20] Mimi Ma, Debiao He, Muhammad Khurram Khan, and Jianhua Chen. Certificateless searchable public key encryption scheme for mobile healthcare system. *Computers & Electrical Engineering*, 65:413–424, 2018.

[21] Nasrollah Pakniat. Designated tester certificateless encryption with keyword search. *Journal of Information Security and Applications*, 49:102394, 2019.

[22] Debiao He, Mimi Ma, Sherali Zeadally, Neeraj Kumar, and Kaitai Liang. Certificateless public key authenticated encryption with keyword search for industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(8):3618–3627, 2017.

[23] Mohammed Raouf Senouci, Ilyas Benkhaddra, Abdelkader Senouci, and Fagen Li. An efficient and secure certificateless searchable encryption scheme against keyword guessing attacks. *Journal of Systems Architecture*, 119:102271, 2021.

[24] Nasrollah Pakniat, Danial Shiraly, and Ziba Eslami. Certificateless authenticated encryption with keyword search: Enhanced security model and a concrete construction for industrial iot. *Journal of Information Security and Applications*, 53:102525, 2020.

[25] Yang Lu and Ji-guo Li. Constructing pairing-free certificateless public key encryption with keyword search. *Frontiers of Information Technology & Electronic Engineering*, 20(8):1049–1060, 2019.

[26] Mimi Ma, Min Luo, Shuqin Fan, and Dengguo Feng. An efficient pairing-free certificateless searchable public key encryption for cloud-based iiot. *Wireless Communications and Mobile Computing*, 2020:1–11, 2020.

[27] Yang Lu, Jiguo Li, and Yichen Zhang. Privacy-preserving and pairing-free multirecipient certificateless encryption with keyword search for cloud-assisted iiot. *IEEE Internet of Things Journal*, 7(4):2553–2562, 2019.

[28] Danial Shiraly, Nasrollah Pakniat, Mahnaz Noroozi, and Ziba Eslami. Pairing-free certificateless authenticated encryption with keyword search. *Journal of Systems Architecture*, 124, 2022.

[29] Mohammed Raouf Senouci, Abdelkader Senouci, and Fagen Li. A pairing-free certificateless authenticated searchable encryption with multi-trapdoor indistinguishability (mtp-ind) guarantees. *Telecommunication Systems*, pages 1–18, 2024.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2024, Volume 22, Number 2 (pp. 65–74)
https://monadi.isc.org.ir

Presented at the ISCISC 2024 in Tarbiat Modares University & Research Institute for Information and Communication Technology, Tehran, Iran

Security analysis of a certificateless authenticated searchable encryption scheme★

Mahnaz Noroozi [1,*] and Atiye Sadeghi [2]

[1] *Department of Computer Science, Faculty of Mathematical Sciences, Alzahra University, Tehran, Iran*
[2] *Department of Mathematics, Faculty of Mathematical Sciences, Alzahra University, Tehran, Iran*

ARTICLE INFO.

Keywords:
Searchable encryption
Certificateless cryptography
Authentication
Indistinguishability

Type: Research paper

ABSTRACT

Certificateless searchable encryption is a cryptographic concept that simultaneously preserves data confidentiality and enables search over encrypted texts. There exist many certificateless searchable encryption schemes in the literature; however, most of them are based on computationally inefficient bilinear pairing operations. Pairing-based cryptographic schemes are not suitable for resource-constrained devices and consequently, researchers are seeking to provide pairing-free cryptographic schemes to enhance efficiency. Recently, Senouci et al. proposed a pairing-free certificateless searchable encryption scheme and claimed that their scheme outperforms other existing schemes in terms of security features, computational costs, and communication costs. However, in this paper, we disprove Senouci et al.'s claims and show that their scheme suffers from several significant security issues. More specially, we first show that their scheme is not actually a certificateless scheme. In other words, we show that in their scheme, an adversary can impersonate any user and perform cryptographic operations that should only be executable by the actual user. Then, we prove that Senouci et al.'s scheme does not meet ciphertext and trapdoor indistinguishability which are the essential security requirements of a searchable encryption scheme.

© 2024 ISC

★ The ISCISC 2024 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: m.noroozi@alzahra.ac.ir (Mahnaz Noroozi), atiye76.s6@gmail.com (Atiye Sadeghi)
© 2024 ISC. All rights reserved.