دوره پانزدهم، شماره بهار و تابستان ۱۴۰۱

مجله فناوری اطلاعات در طراحی مهندسی

Information Technology in Engineering Design

http://ited.sinaweb.net

رمزنگاری مبتنی بر شناسه فازی با آستانهٔ انعطاف‌پذیر

صدیقه خواجویی‌نژاد [۱] سام جبه‌داری* [۲] سید حمید حاج سید جوادی [۳] سید محمدحسین معطر [۴]

(۱) گروه مهندسی کامپیوتر، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران

(۲) گروه مهندسی، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران*

(۳) گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه شاهد، تهران، ایران

(۴) گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران

(تاریخ دریافت :۱۴۰۱/۰۸/۰۶ تاریخ پذیرش: ۱۴۰۱/۱۰/۲۷)

چکیده

موضوع امنیت داده‌ها و اطلاعات در اینترنت و شبکه‌های اجتماعی در سال‌های اخیر جدی‌تر و فراگیرتر شده است. رمزنگاری برای حل مشکلات امنیتی استفاده می‌شود. با این حال، صرف رمزگذاری پیام نمی‌تواند اهداف مورد نظر را برآورده کند. زیرا کنترل دسترسی بر پیام‌های رمزگذاری شده در برخی از برنامه‌ها مورد نیاز است. برای دستیابی به این الزامات، از رمزگذاری مبتنی بر ویژگی (ABE) استفاده می‌شود. این نوع رمزگذاری هم امنیت و هم ساختار دسترسی را برای کاربران شبکه به طور همزمان فراهم می‌کند. رمزگذاری مبتنی بر شناسه فازی (FI BE) را می‌توان حالت خاص از ABE در نظر گرفت که ساختار دسترسی آستانه را برای کاربران فراهم می‌کند. این مقدار آستانه توسط مرجع برای کاربران در مرحله تولید کلید تعیین می‌شود که همیشه ثابت است. این بدین معنی است که کاربری که برای دریافت کلید به مرجع مراجعه می‌کند، کلیدی را دریافت کرده که وابسته به این مقدار آستانه است. بنابراین، فرستنده (رمزگذار) که پیامی را برای این کاربر ارسال می‌کند، نقشی در تعیین مقدار آستانه ایفا نخواهد کرد. این مشکل شده در طرح‌های رمزگذاری مبتنی بر ویژگی با سیاست‌گذاری روی کلید (KP-ABE) نیز وجود دارد. در این مقاله، روشی ارائه می‌دهیم که بتوان یک طرح FI BE را به نوعی تغییر داد که برای تعیین مقدار آستانه علاوه بر مرجع، فرستنده نیز ایفای نقش کرده و بار محاسباتی و مخابراتی طرح را افزایش ندهد. این روش را روی یکی از طرح‌های FI BE معروف پیاده خواهیم کرد. بنابراین، این نوع سیاست‌گذاری نسبت به طرح‌های قبلی FI BE که مقدار آستانه فقط توسط مرجع انتخاب می‌شود، انعطاف‌پذیرتر خواهد بود. با این تغییر می‌توانیم طرح پیشنهادی را یک ABE با سیاست‌گذاری دوطرفه نیز بنامیم. روش پیشنهادی برای انعطاف پذیری مقدار آستانه را می‌توان در اکثر طرح‌های KP-ABE موجود اعمال کرد. ما از مدل امنیتی انتخابی برای اثبات تمایزناپذیری طرح پیشنهادی استفاده می‌کنیم. فرض سختی که ما استفاده می‌کنیم، مسئله تصمیم دوخطی دیفی-هلمن اصلاح شده است.

کلمات کلیدی: رمزنگاری مبتنی بر ویژگی، رمزنگاری مبتنی بر شناسه فازی، ساختار دسترسی، رمزنگاری مبتنی بر ویژگی با سیاست‌گذاری از دو طرف، انعطاف‌پذیری مقدار آستانه.

*عهده‌دار مکاتبات:

سام جبه‌داری

نشانی: گروه مهندسی کامپیوتر، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران

پست الکترونیکی: sjabbehdari@gmail.com

۱- مقدمه

تأمین همزمان امنیت اطلاعات و همچنین اعمال کنترل دسترسی بر روی پیام‌های شبکه‌های مختلف، یکی از پرکاربردترین موضوعات در رمزنگاری است. ما اهمیت این موضوع را با یک نمونه اعلام می‌کنیم. فرض کنید که یک بیمار می‌خواهد اطلاعات سلامتی خود را برای پزشکی که در یک بیمارستان خاص کار می‌کند ارسال کند. در روش‌های رمزگذاری کلاسیک، بیمار باید با پزشک آشنا باشد و کلید عمومی او را داشته باشد. سپس باید اطلاعات سلامتی را با این کلید رمزگذاری کرده و برای پزشک ارسال کند. این روش در شبکه‌های بزرگ مشکلاتی دارد. زیرا کاربران شبکه باید با همه کاربران دیگر آشنا باشند. همچنین کاربران باید کلیدهای زیادی را از کاربران دیگر بیاموزند. بنابراین، اعمال کنترل دسترسی به داده‌های رمزگذاری شده بر اساس ویژگی‌های کاربران می‌تواند این مشکل را حل کند. در این رویکرد که رمزگذاری مبتنی بر ویژگی[۱] (ABE) نامیده می‌شود، دانستن شناسه کاربر و کلید مربوطه برای رمزگذاری مورد نیاز نیست. زیرا کاربران با مجموعه ای از ویژگی‌ها توصیف می‌شوند. بنابراین، فقط فرستنده باید پیام را با این ویژگی‌ها رمزگذاری کند. این رویکرد می تواند بسیار موثر باشد. به عنوان مثال، در مثال ذکر شده، کافی است که فرستنده پیام خود را با ویژگی‌های پزشک و بیمارستان مورد نظر رمزگذاری کند. اگرچه این رویکرد واقعاً مفید است، اما در دنیای واقعی چالش‌هایی دارد. اولین و بارزترین آنها ایجاد یک ساختار دسترسی ریزدانه قوی است. این بدان معناست که ما بتوانیم هر مجموعه‌ای از کاربران را برای ارسال پیام انتخاب کنیم. در برخی از طرح‌ها، این چالش به طور کامل حل نشده است. این موضوع در [1] که از یک دروازه آستانه به عنوان ساختار دسترسی استفاده می‌کند مشهود است. این نوع خاص از ABE رمزگذاری مبتنی بر شناسه (هویت) فازی[۲] (FIBE) نامیده می‌شود. ما می‌خواهیم این طرح را بهبود بخشیم تا به ساختار دسترسی ریزدانه قوی‌تری نسبت به طرح اصلی دست یابیم. پیچیدگی محاسباتی چالش دیگری در حوزه ABE است. ما طرح [1] را بدون تحمیل هزینه‌های اضافی محاسباتی یا ارتباطی بهبود می‌دهیم. اخیراً برخی از مقالات مانند [2]، [3] و [4] سعی در کاهش پیچیدگی طرح‌های ABE داشتند. مفهوم فازی IBE برای بحث بهتر در بخش بعدی ارائه شده است.

در طرح‌های فازی مبتنی بر شناسه FIBE مانند [1] کلیدهای خصوصی کاربران مرتبط با ویژگی‌های آن‌ها تولید می‌شوند، به‌عنوان مثال، کاربر به‌عنوان گیرنده دارای مجموعه‌ای از ویژگی‌ها مانند ω است. حال فرض کنید که یک فرستنده پیامی را با تعدادی ویژگی که به صورت مجموعه ω' نشان داده شده است رمزگذاری کند. حال، اگر مجموعه ویژگی‌های گیرنده ω به اندازه کافی به مجموعه ویژگی‌های ω' نزدیک باشد، گیرنده می‌تواند پیام را رمزگشایی کند. این به این معنی است که تعداد ویژگی‌های مشترک گیرنده و متن رمز شده بیشتر از یک آستانه است. برای این منظور، مقدار آستانه d توسط مرجع تعریف می‌شود و اگر شرط $|\omega \cap \omega'| \geq d$ برقرار باشد، کاربر به عنوان گیرنده قادر به رمزگشایی خواهد بود. ضعف این نوع از ساختارهای دسترسی این است که فرستنده دخالتی در ایجاد این ساختار دسترسی ندارد. این مورد حتی در طرح‌های KP-ABE نیز وجود دارد. توضیحات بیشتر در این باره در بخش بعدی ارائه داده خواهد شد.

ساختار این مقاله در ادامه به این ترتیب است که در بخش دوم مرور ادبیات و آثار مرتبط ارائه شده است. ما پیش‌نیازهای ریاضی و الزامات پایه ABE را به عنوان مقدمات در بخش سوم معرفی خواهیم کرد. سپس طرح مورد نظر خود را در بخش چهارم

---

۱ Attribute Based Encryption

۲ Fuzzy Identity Based Encryption

ارائه خواهیم کرد. اثبات امنیتی و مقایسه کارایی طرح با [1] نیز در بخش پنج گنجانده شده است. در نهایت، ما یک نتیجه‌گیری را در بخش ششم پیشنهاد کردیم.

۲- کارهای مرتبط

ساهای و واترز برای اولین بار FIBE را در [1] معرفی کردند که منجر به ظهور ABE شد. این طرح تنها از یک دروازه آستانه استفاده می‌کرد. همانطور که قبلا ذکر شد، در این طرح فرستنده مجموعه ای از ویژگی‌ها را انتخاب کرده و پیام را رمزگذاری می‌کند. گیرندگان می‌توانند پیام را در صورتی رمزگشایی کنند که ویژگی‌های مورد نظر فرستنده را به اندازه کافی داشته باشند، یعنی تعداد ویژگی‌های مورد نظر فرستنده و ویژگی‌های گیرنده بیش از یک آستانه از پیش تعریف شده باشد. به همین دلیل است که به آن رمزگذاری آستانه‌ای نیز می‌گویند. این طرح تنها از یک دروازه آستانه پشتیبانی می‌کند در حالی که با استفاده از ساختارهای دسترسی که دروازه‌های منطقی یا به طور کلی چندین دروازه آستانه را ترکیب می‌کنند، می توانیم به ساختار دسترسی ریز دانه قوی‌تری دست یابیم. بنابراین، هدف اعمال ساختار دسترسی پیچیده‌تر (مانند توابع بولی) به طرح‌ها است. برای این منظور، گویال و همکاران [5] طرحی را برای اعمال ساختار دسترسی یکنواخت پیشنهاد کردند و همچنین مفهوم رمزگذاری مبتنی بر ویژگی (ABE) را معرفی کردند. در این طرح، خطمشی (ساختار دسترسی) به کلید کاربران اعمال می‌شود. این به این معنی است که یک ساختار دسترسی توسط مرجع در مرحله تولید کلید انتخاب و اعمال می‌شود. این طرح به عنوان رمزگذاری مبتنی بر ویژگی خطمشی کلیدی (KP-ABE) شناخته می‌شود. پس از آن، بتنکورت[۱] و همکاران در [6] طرحی را ارائه کرد که در آن خط مشی دسترسی در متن رمزی اعمال شد. برخلاف KP-ABE، در طرح [6]، ساختار دسترسی در مرحله رمزگذاری توسط فرستنده انتخاب و اعمال می‌شود. این طرح‌ها رمزگذاری مبتنی بر ویژگی خط مشی متن رمزی[۲] (CP-ABE) نامیده می‌شوند. طرح [7] یک طرح CP-ABE را پیشنهاد کرد که برخی از مشکلات و محدودیت‌های [6] را حل کرد.

اخیراً، [8] یک طرح CP-ABE پیشنهاد کرده است که از معماری سلسله مراتبی پشتیبانی می‌کند. این طرح به طور کامل توزیع شده است که سطح بالایی از مقیاس پذیری را فراهم می‌کند. با افزایش تعداد کاربران در یک سیستم، شبکه‌های ارتباطی ممکن است با چالش‌های مقیاس‌پذیری مواجه شوند. علاوه بر این، نوع دیگری از ABE پیشنهاد شده در [9] ABE با سیاست‌گذاری دو طرفه[۳] (DP-ABE) نامیده می‌شود. در DP-ABE، سیاست‌گذاری هم در کلیدهای خصوصی کاربران و هم در متن رمزگذاری شده قرار می‌گیرد. در واقع در این نوع ABE، هم مرجع و هم فرستنده در سیاست‌گذاری مشارکت خواهند داشت. همانطور که قبلاً ذکر شد، ساختار دسترسی معمولاً به عنوان یک تابع بولی تعریف می‌شود، صرف نظر از اینکه در کلید یا متن رمزگذاری اعمال می‌شود. اگر در این تابع از گیت‌های AND، OR و آستانه استفاده شود، به آن ساختار دسترسی یکنواخت می‌گویند. تعریف دقیق ساختار دسترسی یکنواخت را می‌توان در [5] و [6] یافت. در ضمن اگر در ساختار دسترسی علاوه بر گیت‌های ذکر شده از گیت NOT استفاده شود به آن ساختار دسترسی غیر یکنواخت می‌گویند. استروفسکی و همکاران اولین طرح ABE را در [10] پیشنهاد کردند که از ساختار دسترسی غیریکنواخت پشتیبانی می‌کند. همچنین طرح‌هایی مانند [11] و [12] وجود دارد که از توابع ریاضی به عنوان ساختارهای دسترسی استفاده می‌کنند.

همانطور که قبلا ذکر کردیم یکی از مهم‌ترین مشکلات در طرح‌های ABE پیچیدگی محاسباتی است. یکی از تکنیک‌های حل این مشکل برون‌سپاری است. گرین برای اولین بار رمزگذاری مبتنی بر ویژگی برون‌سپاری را در [13] ارائه کرد. این تکنیک

---

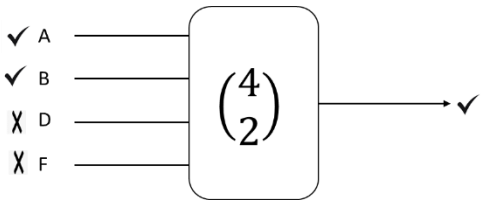
۱ Bethencourt

۲ Ciphertext Policy Attribute Based Encryption

۳ Dual Policy Attibute Based Encryption

سربار محاسباتی را از جانب کاربران کاهش می‌دهد و شخص ثالث به جای آن محاسبات را انجام می‌دهد. معمولاً از ابر به عنوان شخص ثالث استفاده می‌شود. برخی از مشکلات دیگر در حوزه ABE مانند امانسپاری کلید، سربار ارتباط، ابطال و مشکلات کارایی وجود دارد. مشکل امانسپاری کلید یک مسئله رایج در شبکه‌ها است. [14] اولین طرح ABE چند مرجع را ارائه کرد. اخیراً طرح‌های [15]، [16] و [17] سعی در حل مشکل امانسپاری کلید[1] کردند. طرح‌های [18] و [19] سعی کردند با ارائه طرحی که اندازه متن رمز ثابت باشد، مشکل سربار ارتباط را حل کنند. در طرح‌های دیگر، اندازه متن رمز با افزایش تعداد ویژگی‌های استفاده شده یا عمق مدار به عنوان ساختار دسترسی افزایش می‌یابد. ابطال کاربر یا ویژگی مشکل دیگری است که [20] طرحی برای حل این مشکل ارائه کرده است. علاوه بر این، [21] یک طرح ABE سوراخ‌پذیر را پیشنهاد کرد که می‌تواند ابطال رمزگشایی را فراهم کند. برخی مقالات جدید مانند [22] و [23] وجود دارد که بر حل این مشکل متمرکز شده‌اند. طرح‌های [24] و [25] بر کارایی متمرکز بودند و یک طرح ABE را برای کاربردهای عملی ارائه کردند.
در ادامه می خواهیم ضعف ساختار دسترسی ریز دانه را در طرح‌های FIBE به ویژه در [1] بیان کنیم.

مشکلات طرح FIBE: در یک طرح FIBE مانند [1]، ساختار دسترسی کاملاً ریزدانه نیست. فرض کنید کاربر داده u دارای یک مجموعه ویژگی ω است، مقدار آستانه d است و فرستنده مجموعه ویژگی ω' را انتخاب کرده است. کاربر داده u داده‌های رمزگذاری شده را دریافت می‌کند. اگر شرط $|\omega \cap \omega'| \geq d$ برقرار باشد، کاربر u می‌تواند رمزگشایی کند. حال فرض کنید هدف فرستنده جلوگیری از رمزگشایی این کاربر است. در طرح [1]، فرستنده فقط می‌تواند مجموعه ویژگی ω' را کاهش دهد که می‌تواند باعث شود که ویژگی‌های هدف فرستنده به طور کامل انتخاب نشده و سایر کاربران مجاز نیز نتوانند رمزگشایی کنند. به عنوان مثال، فرض کنید یک کاربر وجود دارد که خط مشی دسترسی او یک دروازه آستانه است، همانطور که در شکل ۱ نشان داده شده است. فرستنده یک پیام را با اعمال مجموعه ویژگی $\{A, B, C, E\}$ رمزگذاری می‌کند. با توجه به شکل ۱، واضح است که این کاربر می‌تواند پیام فرستنده را رمزگشایی کند. زیرا خطمشی دسترسی او دروازه آستانه است. مقدار آستانه ۲ از ۴ ویژگی ورودی است. ورودی این گیت ویژگی‌های $\{A, B, D, F\}$ است.



شکل ۱: خطمشی کاربر (گیت آستانه)

با توجه به ویژگی‌های متن رمزی، واضح است که صفات A و B مشترک هستند. بنابراین، این کاربر مجاز به رمزگشایی است. در این مثال، فرستنده می‌خواهد دسترسی این کاربر را ممنوع کند. در طرح‌های قبلی مانند [1]، [5]، [26]و [27] فرستنده باید برخی از ویژگی‌ها را در متن رمز حذف کند تا تعداد تقاطع‌ها کاهش یابد. به طور کلی، یک فرستنده نمی‌تواند خط مشی دسترسی را در طرح‌های رمزنگاری مبتنی بر ویژگی با سیاست‌گذاری روی کلید[2] (KP-ABE) تغییر دهد (به عنوان مثال، [28]). در این سناریو، هدف ما این است که فرستنده بتواند دسترسی این کاربر را بدون حذف هیچ ویژگی در متن رمزی، ممنوع کند. طرح‌های قبلی نمی‌توانند اینگونه عمل کنند. بنابراین، در این طرح‌ها، فرستنده نمی‌تواند یک ساختار دسترسی ریزدانه ایجاد کند. اگر فرستنده بتواند مقدار آستانه را به ۳ افزایش دهد، می‌تواند دسترسی این کاربر را ممنوع کند. این سهم مقاله ما

۱ Key escrow

۲ Key Policy Attribute Based Encryption

است. این بدان معنی است که اگر مرجع آستانه را ۲ انتخاب کرده باشد و فرستنده ۱ را انتخاب کند، مقدار آستانه کل ۳ خواهد بود. در واقع، در طرح‌های قبلی FIBE، مقدار آستانه (برای یک کاربر) یک بار برای همیشه انتخاب شده و ثابت باقی می‌ماند. عدم انعطاف در انتخاب آستانه باعث بروز مشکل فوق می‌شود. بنابراین، ما می‌خواهیم این مشکلات را در طرح خود با استفاده از تکنیک ضرب چند جمله‌ای تسهیم راز که از مقاله [29] اقتباس شده است، حل کنیم. طرح ما همچنین می‌تواند ABE دو سیاستی باشد. زیرا مرجع و فرستنده مقدار آستانه را با هم انتخاب می‌کنند. همانطور که قبلاً ادعا کردیم، تکنیک پیشنهادی می‌تواند در اکثر طرح‌های KP-ABE مانند [5] و [30] استفاده شود. درواقع، اگر تکنیک ما در طرح‌های KP-ABE استفاده شود، فرستنده می‌تواند تمام مقادیر آستانه را در گیت‌های شروع مدار (گره‌های برگ درخت دسترسی) افزایش دهد.

در طرح ما، مقدار آستانه به دو بخش تقسیم می‌شود. یک قسمت توسط مرجع روی کلید قرار می‌گیرد و قسمت دیگر توسط فرستنده انتخاب شده و در متن رمزی قرار می‌گیرد. در نهایت، آستانه کل مجموع دو آستانه اولیه خواهد بود. بنابراین، مقدار آستانه دیگر ثابت نخواهد بود و ممکن است در هنگام رمزگذاری افزایش یابد. بنابراین، مقدار آستانه انعطاف پذیر خواهد بود. برای این منظور از روشی به نام ضرب سهام در تسهیم راز شامیر[1] استفاده کردیم. این تکنیک را می‌توان در طرح‌های KP-ABE مانند [5] و [30] نیز به کار برد.

۳- مفاهیم اولیه

در این بخش، تعاریف و مقدماتی که در طرح پیشنهادی استفاده خواهیم کرد، ارائه شده است. این بخش شامل تعریف FIBE انعطاف‌پذیر (به عنوان یک طرح ABE)، مدل امنیتی انتخابی برای KP-ABE، طرح‌های تسهیم راز، زوج‌نگار دوخطی و فرض مشکل سخت است.

۳-۱- رمزگذاری مبتنی بر شناسه فازی آستانه انعطاف پذیر

هر طرح FIBE و ABE دارای چهار الگوریتم است: الگوریتم‌های راه اندازی، تولید کلید، رمزگذاری و رمزگشایی. ما این الگوریتم‌ها را به ترتیب به صورت Set، KGen، Enc و Dec نشان می‌دهیم. الگوریتم‌های راه‌اندازی و تولید کلید توسط مرجع اجرا می‌شود. الگوریتم رمزگذاری توسط فرستنده (مالک داده) و الگوریتم رمزگشایی توسط گیرنده (کاربر داده) اجرا می‌شود. اکنون این الگوریتم‌ها را برای طرح خود تعریف می‌کنیم.

Set(λ,U) : این الگوریتم پارامتر امنیتی λ و مجموعه تمام ویژگی‌های U را دریافت می‌کند، سپس شاه‌کلید خصوصی (MSK) و کلیدهای عمومی (PK) را تولید می‌کند. MSK باید ایمن نگه داشته شود و PK برای همه اعضای شبکه اعلام شود. تعداد تمام ویژگی‌ها $n = |U|$ است.

KGen $(\boldsymbol{MSK}, \boldsymbol{d_1}, \boldsymbol{\omega})$: این الگوریتم شاه‌کلید خصوصی MSK، مقدار آستانه اول d_1 و مجموعه ویژگی $\omega \subseteq U$ را به عنوان ورودی دریافت می‌کند و کلید خصوصی کاربر (SK) را تولید می‌کند.

$\boldsymbol{Enc}\ (\boldsymbol{M}, \boldsymbol{PK}, \boldsymbol{d_2}, \boldsymbol{\omega'})$: این الگوریتم کلید عمومی PK، مقدار آستانه دوم d_2، پیام مورد نظر (M) و مجموعه ویژگی $\omega' \subseteq U$ را به عنوان ورودی دریافت می‌کند و متن رمزی E که مربوطه به ω' و پیام M. است ، را تولید می‌کند.

$\boldsymbol{Dec}\ (\boldsymbol{E}, \boldsymbol{SK})$: این الگوریتم کلید مخفی SK که مربوط به مجموعه ویژگی ω و همچنین متن رمز E مربوط به مجموعه ویژگی ω'، را دریافت می‌کند. اگر $|\omega \cap \omega'| < d_1 + d_2$ برقرار باشد، الگوریتم $\perp$ را خروجی می‌دهد، در غیر این صورت، این الگوریتم پیام M را بازیابی می‌کند و آن را به عنوان خروجی اعلام می‌کند.

[1] Secret Sharing

۳-۲- مدل امنیت انتخابی

با توجه به اینکه امنیت طرح خود را در مدل امنیتی انتخابی اثبات خواهیم کرد، در این قسمت به توضیح این مدل می‌پردازیم. این مدل شامل مراحل متعددی است که بین مهاجم و چالشگر به صورت یک بازی اجرا می‌شود. در ادامه این بازی توضیح داده خواهد شد.

مقداردهی اولیه: مهاجم ابتدا یک مجموعه ویژگی چالش α و مقدار d_2 را مشخص می‌کند و آنها را به چالشگر می‌فرستد.

راه اندازی: چالشگر الگوریتم راه اندازی را اجرا می‌کند و کلیدهای عمومی را برای مهاجم ارسال می‌کند.

فاز ۱: مهاجم مجاز است مجموعه ویژگی γ_j را انتخاب کند و درخواستی برای کلیدهای خصوصی γ_j بفرستد تا زمانی که $|\alpha \cap \gamma_j| < d_1 + d_2$ برای همه jها برقرار باشد.

چالش: مهاجم دو پیام M_0 و M_1 را انتخاب می‌کند و آنها را به مهاجم ارسال می‌کند. سپس چالشگر یک بیت تصادفی b را انتخاب کرده و M_b را با مجموعه ویژگی چالش α رمزگذاری می‌کند.

فاز ۲: فاز ۱ تکرار می‌شود.

حدس: مهاجم حدس می‌زند کدام پیام رمزگذاری شده است. حدس مهاجم را با b' نشان می‌دهیم. اگر مهاجم بیت مورد نظر را با احتمال بیش از $\frac{1}{2}$ تشخیص دهد، برنده این بازی خواهد بود.

۳-۳- تسهیم راز

فرض کنید که ما می‌خواهیم یک راز را بین چندین نهاد به اشتراک بگذاریم. به هر موجودیت یک سهم مخفی داده می‌شود که هیچ یک از آنها نمی‌توانند مقدار راز را محاسبه کنند. این در صورتی امکان‌پذیر است که تعداد کافی از موجودیت‌ها با یکدیگر همکاری کنند. مهمترین طرح تسهیم راز، طرح شامیر است که مانند یک گیت آستانه عمل می‌کند [31]. در این طرح، اگر یک راز بین n موجودیت به اشتراک گذاشته شود و اگر t یا بیشتر از این موجودیت‌ها وجود داشته باشد، راز می‌تواند بازیابی شود. این طرح را می‌توان به هر ساختار دسترسی تعمیم داد. در این طرح، برای بازیابی آن باید حداقل t نقطه از یک چندجمله‌ای درجه $t-1$ داشته باشیم. برای به اشتراک گذاشتن راز s بین n موجودیت با آستانه t (به آن طرح t از n می‌گویند و $t \leq n$) ابتدا یک چند جمله‌ای تصادفی $q(x)$ درجه $t-1$ انتخاب می‌شود که $q(0) = s$. هر نهاد i، که $1 \leq i \leq n$، دوتایی $(i, q(i))$ داده می‌شود. برای بازیابی مقدار s از ضرایب لاگرانژ استفاده می‌شود. تابع ضریب لاگرانژ را می‌توان به صورت زیر محاسبه کرد.

$$\Delta_{i.S}(x) = \prod_{j \in S \,.\, j \neq i} \frac{x-j}{i-j} \qquad ,\forall\, i \in S \tag{۱}$$

$$\Delta_{i.S}(0) = \prod_{j \in S \,.\, j \neq i} \frac{-j}{i-j} \tag{۲}$$

که در آن S مجموعه مورد نظر از t سهام موجودیت‌های مختلف است. از فرمول زیر برای بازیابی مقدار سهم q(0)=s استفاده می‌شود.

$$q(0) = \sum_{i \in S} q(i) \cdot \Delta_{i,S}(0) \qquad (۳)$$

این یک تابع آستانه است. توجه داشته باشید که گیت‌های AND و OR را نیز می‌توان با استفاده از این تابع تولید کرد.

۳-۳-۱ ضرب چند جمله ای در تسهیم راز

در این بخش، روابط ضرب سهام مربوط به دو طرح تسهیم راز شامیر را که از [29] اقتباس شده است، بحث خواهیم کرد. یعنی دو چند جمله‌ای متفاوت برای دو راز متفاوت داریم. نتیجه می‌گیریم که ضرب سهم‌ها معادل ضرب این دو چند جمله‌ای است. در ادامه به بررسی این روش می‌پردازیم. فرض کنید n موجودیت $P_1, \dots, P_n$ داریم. چند جمله‌ای $q(x)$ درجه $d_1 - 1$ داریم که $d_1 < n$ و راز این چند جمله ای $q(0) = s_1$ است. برخی از سهام مخفی به عنوان $P_i \leftarrow (i, q(i)); 1 \leq i \leq n$ به نهادهای فوق اختصاص داده می‌شود. این رابطه نشان می‌دهد که موجودیت P_i دوتایی $(i, q(i))$ را دریافت می‌کند. بنابراین، با d_1 شرکت کننده از n موجودیت موجود، راز s_1 می‌تواند بازیابی شود. حال فرض کنید یک چند جمله ای $p(x)$ با درجه d_2 داریم که راز آن $p(0) = s_2$ است. برخی از سهام مخفی به صورت $P_i \leftarrow (i, p(i)) ; 1 \leq i \leq n$ به نهادهای فوق اختصاص داده می‌شود. حال اگر سهم‌های قبلی را ضرب کنیم (یعنی $P_i \leftarrow (i, q(i).p(i)) ; 1 \leq i \leq n$) سپس درونیابی کنیم، برابر است با حاصل‌ضرب چندجمله‌ای $h(x) = q(x).p(x)$ با راز $h(0) = q(0)p(0) = s_1 s_2$. درجه چندجمله‌ای به دست آمده $d_1 + d_2 - 1$ است. اگر شرط $d_1 + d_2 < n$ برقرار باشد، می‌توان در نظر گرفت که تسهیم راز برای $h(x)$ انجام شده است. بنابراین، راز حاصلضرب چندجمله‌ای با حداقل $d_1 + d_2$ شرکت‌کننده بازیابی خواهد شد. لازم به ذکر است که درجه چندجمله‌ای اول $d_1 - 1$، دومی d_2 و مقدار آستانه برای حاصل‌ضرب آنها $d_1 + d_2$ است.

۳-۴- زوج‌نگار دوخطی

زوج‌نگار دوخطی متقارن، نگاشت از دو عنصر یک گروه به عنصری از گروه دوم است. بنابراین زوج‌نگار دوخطی که با e نشان داده می‌شود را می‌توان به صورت $e: G_1 \times G_1 \rightarrow G_T$ تعریف کرد. مسئله لگاریتم گسسته باید در هر گروه سخت باشد تا امنیت در کاربردهای رمزگذاری تضمین شود. ویژگی اصلی این نگاشت حالت دوخطی آن است. بنابراین، اگر g مولد گروه G_1 باشد و اندازه گروه q یک عدد اول بزرگ و همچنین $a, b \in Z_q$ باشد، داریم:

$$e(g^a, g^b) = e(g, g)^{ab} \qquad (۴)$$

با این تعریف، عنصر $e(g,g)$ مولد گروه G_T خواهد بود. بنابراین، رابطه $e(g,g) \neq 1$ باید برقرار باشد تا تابع به درستی کار کند.

۳-۵- مسئله تصمیم دیفی-هلمن دوخطی اصلاح شده

فرض کنید که زوج‌نگار دوخطی $e: G_1 \times G_1 \to G_T$ وجود دارد. اگر بردار $(g^a, g^b, g^c, e(g,g)^z)$ داده شود، تشخیص اینکه z برابر با ab/c است یا خیر، مسئله تصمیم دیفی-هلمن دوخطی اصلاح شده (MDBDH) شناخته می‌شود. فرض می‌کنیم که این مسئله سخت است و مهاجم به طور معمول با احتمال $\frac{1}{2} + negl$ قادر به حل این مشکل است. در اینجا $negl$ به معنای ناچیز است.

۴- طرح پیشنهادی

همانطور که قبلا ذکر شد، طرحی را در این بخش ارائه خواهیم کرد که برای ساختار دسترسی آستانه استفاده می‌شود. این مقدار آستانه به طور مشترک توسط مرجع در الگوریتم تولید کلید و فرستنده در الگوریتم رمزگذاری انتخاب می‌شود. آستانه تعریف شده توسط مرجع، آستانه اول d_1 و آستانه تعریف شده توسط فرستنده، آستانه دوم d_2 نامیده می‌شود. آستانه اول ثابت است و تغییر نمی‌کند اما آستانه دوم برای هر رمزگذاری انتخاب می‌شود. این اجازه می‌دهد تا آستانه انعطاف‌پذیر باشد. در رابطه با ABE، اینگونه تفسیر می‌شود که هر کاربر با مجموعه‌ای از ویژگی‌ها ω تعریف می‌شود و دارای کلیدهای خصوصی مربوط به این ویژگی‌ها است. فرستنده پیام را با استفاده از تعدادی ویژگی که به صورت ω' نشان داده می‌شود، رمزگذاری می‌کند. حال اگر گیرنده پیام به اندازه کافی به مجموعه ویژگی متن رمزی نزدیک باشد، می‌تواند رمزگشایی کند. ملاک نزدیک بودن به ویژگی‌های متن رمز شده، مقدار آستانه است. به عبارت دیگر، اگر شرط $|\omega \cap \omega'| \geq d_1 + d_2$ برقرار باشد، کاربر گیرنده قادر به رمزگشایی خواهد بود. روش پیشنهادی ما برای افزایش مقدار آستانه می‌تواند در بسیاری از طرح‌های KP-ABE مانند [5] و [30] نیز اجرا شود. الگوریتم‌های این طرح را در ادامه توضیح می‌دهیم.

طرح FIBE ما دارای چهار الگوریتم راه‌اندازی، تولید کلید، رمزگذاری و رمزگشایی است که به ترتیب با Set، KGen، Enc و Dec نشان می‌دهیم.

Set(λ, U): گروه G_1 که از مرتبه p است با مولد g انتخاب می‌شود. همچنین یک زوج‌نگار دوخطی e به صورت $G_1 \times G_1 \to G_T$ انتخاب می‌شود. مجموعه $\{G_1, G_T, g, e\}$ به عنوان پارامترهای عمومی pp شناخته می‌شود. فرض بر این است که این پارامترها در کلید عمومی PK موجود هستند. پارامتر امنیتی λ ورودی این الگوریتم است. این الگوریتم به صورت تصادفی مقادیر $t_1, \dots, t_{|U|}$ را از مجموعه Z_p انتخاب می‌کند. سپس به صورت تصادفی مقدار y را از مجموعه Z_p^* انتخاب می‌کند. کلید مخفی اصلی به شرح زیر است.

$$MSK: t_1, \dots, t_{|U|}, y$$

علاوه بر این، کلیدهای عمومی به شرح زیر منتشر می‌شوند.

$$PK: T_1 = g^{t_1}, \dots, T_{|U|} = g^{t_{|U|}}, Y = e(g,g)^y$$

KGen(MSK,d_1,ω): این الگوریتم تابع چند جمله ای $q(x)$ را با یک درجه کمتر از مقدار آستانه d_1 انتخاب می‌کند. بنابراین، این چند جمله‌ای از درجه $d_1 - 1$ است و این چند جمله‌ای به طور تصادفی انتخاب می‌شود بگونه‌ای که $q(0) = y$. کلید مخفی کاربر به صورت زیر خواهد بود.

$$SK: D_i = g^{\frac{q(i)}{t_i}}; i \in \omega \quad (۵)$$

$Enc\ (M, PK, d_2$ و $\omega')$: این الگوریتم یک مقدار تصادفی s را از مجموعه Z_p^* انتخاب می‌کند. سپس چندجمله‌ای $p(x)$ از درجه d_2 انتخاب می‌شود بگونه‌ای که $p(0) = s$ برقرار باشد. متن رمز شده به صورت زیر خواهد بود.

$$E = \left\{d_2, \omega', E' = M.Y^s, \left\{E_i = T_i^{p(i)}\right\}_{i \in \omega'}\right\} \quad (۶)$$

$Dec\ (E, SK)$: فرض کنید که کاربر گیرنده کلید مخفی SK را با مجموعه صفات ω دارد. اگر شرط $|\omega \cap \omega'| \geq d_1 +$ d_2 برقرار باشد، این گیرنده می‌تواند E را رمزگشایی کند. اگر برقرار نباشد، الگوریتم خروجی $\perp$. برای رمزگشایی، گیرنده مجموعه S شامل $d_1 + d_2$ عضو از $|\omega \cap \omega'|$ را انتخاب می‌کند. رمزگشایی به شرح زیر خواهد بود.

$$M = \frac{E'}{\prod_{i \in S}\left(e(D_i, E_i)\right)^{\Delta_{i,S}(0)}} \quad (۷)$$

در رابطه فوق، $\Delta_{i,S}\ (0)$ ضریب لاگرانژ است. صحت رابطه (۷) برای بازیابی پیام M را می‌توان به صورت زیر ثابت کرد.

$$\frac{E'}{\prod_{i \in S}\left(e(D_i, E_i)\right)^{\Delta_{i,S}(0)}} = \frac{M.e(g,g)^{ys}}{\prod_{i \in S}\left(e\left(g^{\frac{q(i)}{t_i}}, g^{p(i).t_i}\right)\right)^{\Delta_{i,S}(0)}}$$

$$= \frac{M.e(g,g)^{ys}}{\prod_{i \in S}(e(g,g)^{q(i).p(i)})^{\Delta_{i,S}(0)}} = \frac{M.e(g,g)^{ys}}{e(g,g)^{\sum_{i \in S} q(i).p(i)\Delta_{i,S}(0)}}$$

$$= \frac{M.e(g,g)^{ys}}{e(g,g)^{ys}} = M$$

همانطور که ملاحظه می‌شود، اگر شرط $|\omega \cap \omega'| \leq d_1 + d_2$ برقرار نباشد، مجموعه S قابل تعریف نیست. بنابراین، بازیابی پیام با استفاده از رابطه (۷) امکان پذیر نیست.

۵- ارزیابی امنیتی و کارایی

در این بخش، امنیت طرح خود را با استفاده از مدل امنیتی انتخابی و با فرض سختی مسئله تصمیم دیفی-هلمن دوخطی اصلاح شده اثبات خواهیم کرد. همچنین، ما طرح خود را با طرح [1] مقایسه می‌کنیم و به این نتیجه می‌رسیم که پیچیدگی محاسباتی و سربار ارتباط طرح ما تقریباً مشابه [1] است.

۵-۱- اثبات امنیتی

ما فرض می‌کنیم که چالشگر می‌خواهد با داشتن پارامترهای $(A, B, C, Z) = (g^a, g^b, g^c, e(g,g)^z)$ به مسئله تصمیم دیفی-هلمن دوخطی اصلاح شده پاسخ دهد. همچنین فرض می‌کنیم که یک مهاجم وجود دارد که می‌تواند طرح ما را با احتمال $\varepsilon + \frac{1}{2}$ بشکند که ε غیر قابل اغماض است. چالشگر باید از پاسخ مهاجم برای حل مسئله تصمیم دوخطی اصلاح شده دیفی-هلمن استفاده کند. اگر این امکان وجود داشته باشد، با توجه به اینکه مسئله DMBDH سخت است و قابل حل نیست، به این نتیجه می‌رسیم که دشمنی مانند $\mathcal{A}$ وجود ندارد که طرح ما را بشکند. برای این منظور، ما مراحل مدل امنیتی انتخابی را اجرا می‌کنیم.

مقداردهی اولیه: مهاجم $\mathcal{A}$ ابتدا مجموعه ویژگی چالش α و مقدار d_2 را مشخص می‌کند.

راه‌اندازی: چالشگر الگوریتم راه‌اندازی را برای مهاجم شبیه‌سازی می‌کند و $Y = e(g, A) = e(g,g)^a$ را تنظیم می‌کند. علاوه بر این، مقدار تصادفی $\beta_i \in Z_p$ را برای هر $i \in \alpha$ انتخاب می‌کند و $T_i = C^{\beta_i} = g^{c\beta_i}$ را قرار می‌دهد. مقادیر تصادفی $\omega_i \in Z_p$ را برای هر $i \in U - \alpha$ انتخاب می‌کند و $T_i = g^{\omega_i}$ را تنظیم می‌کند. بنابراین، پارامترهای عمومی انتخاب شده و به مهاجم داده می‌شود.

فاز ۱: مهاجم مجموعه ویژگی γ را انتخاب می‌کند که $|\alpha \cap \gamma| < d_1 + d_2$ است و آن را برای چالشگر ارسال می‌کند. رقیب باید کلیدهای مخفی مربوط به γ را تولید کند. ابتدا مجموعه‌های Γ, Γ' و S را برای هر مجموعه ویژگی γ که $|\alpha \cap \gamma| < d_1 + d_2$ به صورت زیر تعریف می‌کنیم:

$$\Gamma = \gamma \cap \alpha \,,\, S = \Gamma' \cup \{0\} \,,\, \Gamma \subseteq \Gamma' \subseteq \gamma;\ \ |\Gamma'| = d_1 - 1$$

چالشگر کلیدهای خصوصی D_i را برای همه $i \in \Gamma'$ به صورت زیر تولید می‌کند:

اگر $i \in \Gamma$: مقدار تصادفی $s_i \in Z_p$ انتخاب شده و $D_i = g^{s_i}$ تنظیم می‌شود.

اگر $i \in \Gamma' - \Gamma$: مقدار تصادفی $\lambda_i \in Z_p$ انتخاب شده و $D_i = g^{\frac{\lambda_i}{\omega_i}}$ تنظیم می شود.

برای انتخاب یک چند جمله‌ای $q(x)$ درجه، $d_1 - 1$ می‌توانیم به طور تصادفی نقاط $d_1 - 1$ را انتخاب کنیم و $q(0) = a$ نیز تنظیم شود. طبق طرح ما و موارد فوق، برای $i \in \Gamma$ داریم $q(i) = c\beta\_i\, s\_i$ و برای $i \in \Gamma - \Gamma'$ داریم $q(i) = \lambda_i$.

چالشگر، با توجه به اینکه لگاریتم گسسته مرتبط با $T_i\,; i \notin \alpha$ (یعنی ω_i) را می‌داند، می‌تواند برای محاسبه کلید $D_i; i \notin \Gamma'$ این کار را انجام دهد.

$$i \notin \Gamma' : D_i = \left(\prod_{j \in \Gamma} C^{\frac{\beta_i s_i \Delta_{j,S}(i)}{\omega_i}} \right) \left(\prod_{j \in \Gamma' - \Gamma} g^{\frac{\lambda_i . \Delta_{j,S}(i)}{\omega_i}} \right) A^{\frac{\Delta_{0,S}(i)}{\omega_i}}$$

رقیب با استفاده از درونیابی قادر به محاسبه $D_i = g^{\frac{q(i)}{t_i}} : i \notin \Gamma'$ (که $q(x)$ با استفاده از $d_1 - 1$ مقدار از $i \notin \Gamma'$ و یک مقدار $A = g^a$ ایجاد شد.. بنابراین، کلیدهای خصوصی مربوط به γ تولید شدند.

چالش: مهاجم دو پیام M_0 و M_1 را انتخاب کرده و برای چالشگر می‌فرستد. چالشگر بیت تصادفی v را انتخاب می کند و پیام M_v را با ویژگی‌های چالش α به صورت زیر رمزگذاری می‌کند.

برای رمزگذاری، ابتدا چند جمله‌ای $p'(x)$ درجه d_2 را انتخاب می‌کند که $p'(0) = 1$ برقرار است. متن رمز به صورت زیر تولید می شود.

$$E = \left\{ d_2, \omega', E' = M_v . Z, \left\{ E_i = B^{p'(i)\beta_i} \right\}_{i \in \omega'} \right\}$$

اگر $z = ab/c$ باشد، فرض کنیم که $r' = b/c$ و داریم $E' = M_v . e(g,g)^{\frac{ab}{c}} = M_v . e(g,g)^{ar'} = M_v . Y^{r'}$ و نیز $E_i = B^{p'(i)\beta_i} = g^{p'(i)b\beta_i} = g^{p'(i)\frac{b}{c}c\beta_i} = g^{p(i)c\beta_i} = T_i^{p(i)}$.

در رابطه فوق، $p(x) = \frac{b}{c} p'(x)$=r'p'(x) برقرار است که در آن $p(x)$ چند جمله ای d_2 درجه و $p(0) = r'$ است. بنابراین، چالشگر توانسته است متن رمز شده را برای M_v شبیه‌سازی کند.

حال اگر z یک مقدار تصادفی باشد، E' کاملا تصادفی خواهد بود.

فاز ۲: فاز ۱ تکرار می شود.

حدس: در این مرحله، مهاجم بیت v' را حدس می‌زند. اگر $z = ab/c$، احتمال موفقیت مهاجم (یعنی $v' = v$) $\frac{1}{2} + \epsilon$ خواهد بود زیرا ما فرض کردیم که مهاجم با احتمال $\frac{1}{2} + \epsilon$ و غیر قابل اغماض می‌تواند بیت رمزگذاری شده v برای طرح ما را شناسایی کند. اگر z تصادفی باشد، احتمال موفقیت مهاجم (یعنی $v' = v$)) $\frac{1}{2}$ خواهد بود.

با توجه به اینکه چالشگر مقدار v' را دریافت می‌کند، اگر $v' = v$، فرض می‌شود که $z = ab/c$ برقرار است و اگر $v' \neq v$ باشد، z تصادفی است. بنابراین، چالشگر می‌تواند مسئله BDMDH را حل کند. اکنون احتمال موفقیت چالشگر را محاسبه می کنیم (P(Ch)).

$$P(Ch) = \frac{1}{2}P\left(v' = v \middle| z = \frac{ab}{c}\right) + \frac{1}{2}Pr\left(v' = v \middle| z \in_r \mathbb{Z}_p\right)$$

$$= \frac{1}{2}\left(\frac{1}{2} + \epsilon\right) + \frac{1}{2}\left(\frac{1}{2}\right) = \frac{1}{2} + \frac{\epsilon}{2}$$

از آنجایی که فرض می کنیم ϵ غیر قابل اغماض است، $\epsilon/2$ نیز غیر قابل اغماض خواهد بود. بنابراین چالشگر می‌تواند مسئله BDMDH را حل کند. اما این با فرض ما در تضاد است زیرا فرض کرده‌ایم هیچ الگوریتمی نمی‌تواند این مسئله را حل کند. بنابراین، مهاجمی مانند $\mathcal{A}$ نیز وجود ندارد که بتواند طرح ما را بشکند.

۵-۲- مقایسه و ارزیابی کارایی

در طرح پیشنهادی، فرستنده برخلاف طرح‌های قبلی (به عنوان مثال، [1]، [5] و [30]) می‌تواند در انتخاب مقدار آستانه یا خط‌مشی دسترسی مداخله کند. طرح پیشنهادی این خاصیت را بدون اعمال پیچیدگی بیشتر در مقایسه با طرح‌های قبلی به تصویر می‌کشد. در این بخش، نشان می‌دهیم که استفاده از تکنیک ضرب چندجمله‌ای در تسهیم راز، هیچ گونه محاسبات و سربار ارتباط اضافی را نسبت به نسخه اصلی تحمیل نمی‌کند.

ما طرح خود را با [1] (و همچنین [5] و [30] با فرض اینکه تکنیک ما برای آنها اعمال می‌شود) در چهار الگوریتم، یعنی راه‌اندازی، تولید کلید، رمزگذاری و رمزگشایی مقایسه می‌کنیم. ما پیچیدگی محاسباتی و اندازه متن رمزنگاری شده را که مستقیماً با سربار ارتباط مرتبط است، در مقایسه خود در نظر می‌گیریم.

راه‌اندازی: الگوریتم راه‌اندازی در طرح ما دقیقاً مشابه الگوریتم راه‌اندازی در [1] و [5] است (و بسیار شبیه به [30]). بنابراین، پیچیدگی محاسبات و اندازه کلید عمومی یکسان است. کلید عمومی در [30] همچنین شامل دو تابع هش H_1 و H_2 اضافی است.

تولید کلید: الگوریتم تولید کلید در طرح ما دقیقاً مشابه الگوریتم تولید کلید در [1] است (و [5] و [30] با برخی تفاوت‌های جزئی). بنابراین، پیچیدگی محاسبات و اندازه کلید مخفی یکسان است.

Enc: تفاوت بین الگوریتم رمزگذاری در طرح ما با طرح‌های [1]، [5] و [30] این است که d_2 اضافی در رابطه (۴) وجود دارد و همچنین $\{E_i = T_i^{p(i)}) \}_{i\in\omega'}$ به جای $\{E_i = T_i^{s} \}_{i\in\omega'}$ محاسبه می‌شود. این به این معنی است که سربار ارتباط (اندازه متن رمز شده) طرح ما دارای یک عنصر اضافی به نام d_2 است. این را می‌توان با افزودن حداکثر ۴ بیت در متن رمزی مدیریت کرد. زیرا این عنصر دومین مقدار آستانه را نشان می‌دهد که عدد کمی است. بنابراین، ما می‌توانیم آن را نادیده بگیریم. همچنین پیچیدگی محاسباتی الگوریتم رمزگذاری در طرح ما همانند طرح‌های ذکر شده است. توجه داشته باشید که در طرح ما الگوریتم Enc باید یک چند جمله ای $p(x)$ را انتخاب کند و همچنین $\{p(i)\}_{i\in\omega'}$ را محاسبه کند که این محاسبات ناچیز هستند. بنابراین، می‌توان ادعا کرد که پیچیدگی محاسباتی و سربار ارتباط تقریباً مشابه طرح‌های ذکر شده است. در حالی که در [30] فرستنده $E' = H_2\ (Y^{s.H_1(m)})$ را به جای $E' = M.Y^s$ محاسبه می‌کند، اما پیچیدگی محاسبات و اندازه متن رمزی مشابه متن پیشنهادی طرح ما است.

Dec: الگوریتم رمزگشایی طرح ما دقیقاً مشابه الگوریتم رمزگشایی [1] و الگوریتم گره رمزگشایی در [5] و [30] است، با فرض اینکه $d = d_1 + d_2$ باشد. این بر انتخاب مجموعه اشتراکات S تأثیر می‌گذارد. با این حال، عملیات رمزگشایی یکسان است.

بنابراین، می‌توان نتیجه گرفت که استفاده از تکنیک ضرب چندجمله‌ای در تسهیم راز، پیچیدگی محاسباتی، اندازه کلیدها و متن رمزی را مجبور نمی‌کند.

۶- نتیجه‌گیری

در این مقاله، ایده ضرب سهم‌های مرتبط با طرح تسهیم راز شامیر برای انعطاف‌پذیر کردن مقدار آستانه در طرح‌های FIBE و KP-ABE پیشنهاد شده است. در این راستا، یک طرح جدید FIBE با آستانه انعطاف‌پذیر ارائه شد. با توجه به اینکه در طرح پیشنهادی ساختار دسترسی (دروازه آستانه) هم برای کلید و هم برای متن رمز اعمال می‌شود، می‌توان آن را DP-ABE نیز در نظر گرفت. در واقع، یک مقدار آستانه در کلیدها اعمال می‌شود و یک مقدار دیگر در متن رمزگذاری شده اعمال می‌شود. به عبارت دیگر، بخشی از مقدار آستانه توسط مرجع در الگوریتم تولید کلید و بخشی دیگر توسط فرستنده در الگوریتم رمزگذاری تعیین می‌شود. آستانه انتخاب شده توسط مرجع همیشه ثابت است، اما آستانه مرتبط با فرستنده برای هر رمزگذاری قابل تغییر است. بنابراین، طرح ما نسبت به طرح ساهای و واترز [1] انعطاف‌پذیرتر است. مقدار آستانه کل در طرح پیشنهادی با مجموع دو آستانه انتخاب شده توسط مرجع و فرستنده برابر است. برای ایجاد چنین طرحی، از ایده ضرب سهام مرتبط با طرح تسهیم راز استفاده کرده‌ایم. این انعطاف‌پذیری به هیچ‌گونه سربار محاسباتی و ارتباطی اضافی (غیر از مقدار d_2 در متن رمزی) در مقایسه با طرح [1] منجر نمی‌شود. به عبارت دیگر، طرح پیشنهادی ضمن ارائه یک طرح انعطاف‌پذیر، دارای سربار محاسباتی و ارتباطی مشابه قبلی است [1]. در این مقاله، همچنین به اشکالات طرح [1] که ممکن است در یک شبکه رخ دهد، اشاره شد. طرح پیشنهادی این مشکلات را حل کرد. این تکنیک‌های انعطاف‌پذیری و سیاست دوگانه را می‌توان برای بهبود طرح KP-ABE موجود به‌عنوان مثال [5]، [30] یا موارد دیگر به کار برد. علاوه بر این، پیچیدگی محاسباتی، اندازه کلیدها و اندازه

متن رمزی طرح پیشنهادی با [1] و همچنین با [5] و [30] (با این فرض که ایده ضرب سهم‌ها بر روی آنها اعمال شود) مقایسه شد.

با توجه به اینکه رایانه‌های کوانتومی رشد چشمگیری در سال‌های اخیر داشته است، ارائه طرح‌هایی که در برابر این رایانه‌ها امن باشند، ضروری به نظر می‌رسد. در همین راستا می‌توان ایده ضرب سهم‌ها را برای طرح‌های پساکوانتومی مانند [26] نیز اعمال کرد. در اینصورت، ضمن اینکه طرح از ساختار دسترسی قوی‌تری برخوردار خواهد بود، می‌تواند در برابر حملات رایانه‌های کوانتومی مقاوم باشد.

۷- مراجع

[1] Amit Sahai and Brent Waters, "Fuzzy Identity-Based Encryption," EUROCRYPT, Vols. Fuzzy Identity-Based Encryption, no. EUROCRYPT, 2005.

[2] Sana Belguith, Nesrine kaaniche, Giovanni Russello, "PU-ABE: Lightweight Attribute-Based Encryption Supporting Access Policy Update for Cloud Assisted IoT," International Conference on Cloud Computing, 2018.

[3] Syh-Yuan Tan , Kin-Woon Yeow, and Seong Oun Hwang, "Enhancement of a Lightweight Attribute-Based Encryption Scheme for the Internet of Things," IEEE INTERNET OF THINGS JOURNAL, 2019.

[4] Hang Li , Keping Yu , Bin Liu , Chaosheng Feng , Zhiguang Qin , and Gautam Srivastava, "An efficient ciphertext-policy weighted attribute-based encryption for the internet of health things," IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, vol. 26, 2022.

[5] Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," ACM conference on Computer and communications security, 2006.

[6] John Bethencourt, Amit Sahai, Brent Waters, "Ciphertext-Policy Attribute-Based Encryption," IEEE symposium on security and privacy (SP'07), 2007.

[7] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," International Workshop on Public Key Cryptography, 2011.

[8] Ali Mohammad, Javad Mohajeri, Mohammad-RezaSadeghi, Ximeng Liu, "A fully distributed hierarchical attribute-based encryption scheme," Theoretical Computer Science, vol. 815, pp. 25-46, 2020.

[9] Nuttapong Attrapadung, Hideki Imai, "Dual-Policy Attribute Based Encryption," International Conference on Applied Cryptography and Network Security, 2009.

[10] Ostrovsky, Sahai, Waters, "Attribute-based encryption with non-monotonic access structures," Proceedings of the 14th ACM conference on Computer and communications security, 2007.

[11] Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan, Dhinakaran Vinayagamurthy, "Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits," Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2014.

[12] MahdaviOliaee, Mahdi and Ahmadian, Zahra, "Fine-grained flexible access control: ciphertext policy attribute based encryption for arithmetic circuits," Journal of Computer Virology and Hacking Techniques, pp. 1-14, 2022.

[13] Green,Matthew , Susan Hohenberger, Brent Waters, "Outsourcing the decryption of abe ciphertexts," USENIX security symposium , vol. 2011, 2011.

[14] M. Chase, "Multi-authority Attribute Based Encryption," Theory of cryptography conference, 2007.

[15] Ruyuan Zhanga, Jiguo Li, Yang Lu, Jinguang Han, and Yichen Zhang, "Key escrow-free attribute based encryption with user revocation," Information Sciences, vol. 600, 2022.

[16] Er-Shuo Zhuang; Chun-I Fan; and I-Hua Kuo, "Multi-Authority Attribute-Based Encryption with Dynamic Membership from Lattices," IEEE Access, 2022.

[17] Xiao Zhang, Faguo Wu, Wang Yao, Zhao Wang, and Wenhua Wang, "Multi-authority attribute-based encryption scheme with constant-size ciphertexts and user revocation," Concurrency and Computation: Practice and Experience, vol. 31, 2019.

[18] Nuttapong Attrapadung, Benoˆıt Libert,, and Elie de Panafieu, Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts, 2011.

[19] Attrapadung, Nuttapong, Javier Herranz, Fabien Laguillaumie, Benoît Libert, Elie De Panafieu, and Carla Ràfols, "Attribute-based encryption schemes with constant-size ciphertexts," Theoretical computer science, 2012.

[20] Junbeom Hur; and Dong Kun Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, 2010.

[21] Priyanka Dutta, Willy Susilo, Dung Hoang Duong, Partha Sarathi Roy, "Puncturable identity-based and attribute-based encryption from lattices," Theoretical Computer Science, vol. 929, pp. 18-38, 2022.

[22] Chunpeng Ge , Willy Susilo , Joonsang Baek, Zhe Liu, Jinyue Xia, and Liming Fang, "Revocable attribute-based encryption with data integrity in clouds," IEEE Transactions on Dependable and Secure Computing, vol. 19, 2021.

[23] Shijie Deng, Gaobo Yang, Wen Dong, and Ming Xia, "Flexible revocation in ciphertext-policy attribute-based encryption with verifiable ciphertext delegation," Multimedia Tools and Applications, 2022.

[24] Zhen Liu, and Duncan S. Wong, "Practical attribute-based encryption: traitor tracing, revocation and large universe," The Computer Journal, vol. 59, 2016.

[25] Marloes Venema, Greg Alpár, and Jaap-Henk Hoepman, "Systematizing core properties of pairing-based attribute-based encryption to uncover remaining challenges in enforcing access control in practice," Designs, Codes and Cryptography, 2022.

[26] Shweta Agrawal, Xavier Boyen, Vinod Vaikuntanathan, Panagiotis Voulgaris, "Fuzzy Identity Based Encryption from Lattices," IACR Cryptol. ePrint Arch., 2011.

[27] Sergey Gorbunov, Vinod Vaikuntanathan, Hoeteck Wee, "Attribute-Based Encryption for Circuits," Journal of the ACM (Association for Computing Machinery), May 2013.

[28] Y. Sreenivasa Rao, Ratna Dutta, "Computational friendly attribute-based encryptions with short ciphertext," Theoretical Computer Science, vol. 668, 2017.

[29] Mehdi Mahdavi Oliaee, Mahshid Delavar, Mohammad Hassan Ameri, Javad Mohajeri, and Mohammad Reza Aref, "On the Security of O-PSI a Delegated Private Set Intersection on Outsourced Datasets," The ISC International Journal of Information Security (ISeCure), vol. 10, no. 2, pp. 117-127, 2018.

[30] Yong Yu , Junbin Shi, Huilin Li, Yannan Li, Xiaojiang Du, and Mohsen Guizani, "Key-Policy Attribute-Based Encryption With Keyword Search in Virtualized Environments," IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, vol. 38, 2020.

[31] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612-613, 1979.