مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال ششم، شماره ۳، پاییز ۱۳۹۷، ص ۱۱۵-۱۰۷

طرح تسهیم راز چندگامی چنداستفاده براساس تابع چکیده‌ساز با ساختار دسترسی عمومی

مجید فرهادی[1*]، حمیده بای‌پور[2]، رضا مرتضوی[3]

۱- استادیار، ۲- کارشناسی ارشد، ۳- استادیار، دانشگاه دامغان

(دریافت: ۹۶/۰۸/۲۲، پذیرش: ۹۷/۰۱/۱۸)

چکیده

در طرح تسهیم راز چندگامی چنداستفاده واسطه قادر است چند راز را بین گروهی از شرکت‌کنندگان به اشتراک بگذارد و در مرحله بازسازی راز، این رازها گام به گام بازسازی شوند طوری‌که با بازسازی یک راز، بقیه رازها آشکار نمی‌شود یا امنیت آن‌ها به خطر نمی‌افتد. ما در این مقاله یک طرح تسهیم راز چندگامی چنداستفاده براساس تابع چکیده‌ساز پیشنهاد می‌کنیم، چون توابع چکیده‌ساز دارای محاسبات سریع و آسان هستند. این طرح در برابر تقلب شرکت‌کنندگان مقاوم است. همچنین، در این طرح با استفاده از پروتکل تبادل کلید دفی- هلمن واسطه و شرکت‌کنندگان از طریق کانال عمومی با هم ارتباط برقرار می‌کنند. ساختار طرح پیشنهادی در برابر حمله یک راز شناخته‌شده امن است.

واژگان کلیدی: طرح تسهیم راز، چندگامی، چنداستفاده، تابع چکیده‌ساز، ساختار دسترسی عمومی، حمله راز شناخته‌شده

۱- مقدمه

طرح تسهیم راز یک انگیزه قوی برای حفاظت از اطلاعات در برابر از بین رفتن، آسیب‌دیدن و یا افتادن اطلاعات به‌دست دیگری است. اگر تنها یک شخص کل راز را نگهداری کند، آن‌گاه خطر از دست‌دادن راز توسط شخص وجود دارد. یا زمانی‌که راز مورد نیاز است، ممکن است شخص در دسترس نباشد. برای حل این موضوع، طرح تسهیم راز طراحی شده است. طرح تسهیم راز باعث می‌شود که یک راز میان مجموعه‌ای از شرکت‌کنندگان طوری تسهیم شود که تنها زیرمجموعه‌های از پیش‌تعیین‌شده بتوانند راز را بازسازی کنند.

طرح‌های تسهیم راز در ابتدا برای حفاظت از کلیدهای رمزنگاری و دسترسی به منابع به اشتراک گذاشته شده و سپس برای سایر کاربردها نیز استفاده شدند. برخی از این کاربردها، محاسبات چندبخشی [۱]، مدیریت کلید در شبکه‌های موردی (ad-hoc) [۲]، رمزنگاری آستانه [۳] و رأی‌گیری الکترونیکی [۴] است.

در سال ۱۹۷۹ میلادی، طرح تسهیم راز آستانه‌ای (t,n) توسط بلاکلی[1] [۵] و شامیر[2] [۶] به‌طور مستقل پیشنهاد شد. طرح آستانه طرحی است که در آن، تعداد شرکت‌کنندگان هر زیرمجموعه مجاز بزرگتر یا مساوی حد آستانه t است. درواقع، راز بین n شرکت‌کننده طوری به اشتراک گذاشته می‌شود که هر زیرمجموعه شامل t شرکت‌کننده یا بیشتر بتوانند راز را بازسازی کنند، اما زیرمجموعه‌های کمتر از t شرکت‌کننده نتوانند هیچ اطلاعاتی از راز به‌دست آورند. طرح بلاکلی براساس هندسه متناهی و طرح شامیر براساس درون‌یابی لاگرانژ است. از دیگر طرح‌های تسهیم راز در موضوعاتی چون به اشتراک‌گذاری تصویر [۹-۷]، تسهیم راز بصری [۱۲-۱۰] و برون‌سپاری داده‌ها [۱۳] می‌توان اشاره کرد.

فرض کنید $\mathcal{P}$ مجموعه همه شرکت‌کنندگان باشد. گروهی از شرکت‌کنندگان که با ترکیب سهم‌هایشان بتوانند راز را بازسازی کنند، یک زیرمجموعه مجاز نامیده می‌شود. مجموعه همه زیرمجموعه‌های مجاز، ساختار دسترسی نام دارد که با رابطه (۱) نمایش داده می‌شود.

$$\Gamma = \{A \mid A \subseteq \mathcal{P}, \mid A \mid \geq t\} \qquad (۱)$$

1- Blakley
2- Shamir

* رایانامه نویسنده مسئول: farhadi@du.ac.ir

اگر k راز وجود داشته باشد و با استفاده از تسهیم راز شامیر میان n شرکت‌کننده به اشتراک گذاشته شود، واسطه باید طرح تسهیم راز (t,n) را k دفعه اجرا کند که این باعث پایین‌آمدن کارایی طرح می‌شود. برای حل این مشکل، در سال ۱۹۹۴ میلادی، هی[1] و داوسون[2] [۱۴] طرح تسهیم چندراز براساس طرح شامیر، تابع یک‌طرفه و مقادیر انتقال پیشنهاد دادند. در سال ۱۹۹۸ میلادی، تومپا[3] و وول[4] [۱۵] بیان کردند که در طرح تسهیم راز شامیر تقلب امکان‌پذیر است. آن‌ها مسئله خاصی از تسهیم راز در حضور واسطه قابل اعتماد و شرکت‌کنندگان بداندیش که برای تقلب در بازسازی راز تلاش می‌کنند، مورد مطالعه قرار دادند. در مرحله بازسازی راز شرکت‌کنندگان بداندیش می‌توانند با ارایه سایه راز جعلی از بازسازی راز واقعی جلوگیری کنند. برای حل این مشکل، طرح‌های [۱۹-۱۶] پیشنهاد شدند. پاپیریک[5] و ژانگ[6] [۱۷] روی تسهیم راز امن بلاشرط متمرکز شدند. در طرح آن‌ها، همه سهم‌های نادرست در مرحله تأییدپذیری توسط ترکیب‌کننده شناسایی شده و حذف می‌شوند. همچنین، شرکت‌کنندگان بداندیش هیچ مزیتی در ارسال سهم‌های نادرست (برای تقلب‌کردن) به ترکیب‌کننده یا نسبت به شرکت‌کنندگان قابل اعتماد ندارند. به‌طور دقیق‌تر، یک گروه از شرکت‌کنندگان بداندیش با استفاده از سهم‌های معتبر خودشان و راز نامعتبر بازسازی‌شده، شانس خوبی در به‌دست‌آوردن راز معتبر ندارند.

دس[7] و ادهیکاری[8] [۲۰] و چام[9] و ژانگ [۲۲-۲۱]، طرح‌های تسهیم راز براساس تابع چکیده‌ساز را پیشنهاد دادند. این طرح‌ها به‌دلیل نداشتن محاسبات توان‌رسانی پیمانه‌ای و استفاده از تابع چکیده‌ساز سرعت اجرایی بالایی دارد. در [۲۱]، چام و ژانگ طرح خود را به نسخه تاییدپذیر شرکت‌کنندگان در مرحله بازسازی راز گسترش دادند. یک ویژگی عملکردی طرح دس و ادهیکاری (طرح DA) و نسخه تاییدپذیر طرح چام و ژانگ (طرح CZ) این است که از ارایه سایه راز جعلی توسط شرکت‌کنندگان در مرحله بازسازی راز جلوگیری می‌کند. در طرح DA، چون مقدار چکیده سایه راز به‌صورت عمومی منتشر می‌شود پس از بازسازی راز و محاسبه مقدار چکیده راز بازسازی شده و مقایسه آن با مقدار چکیده راز منتشرشده، می‌توان از درست‌بودن مقدار راز بازسازی‌شده اطمینان حاصل کرد. اگر دو مقدار چکیده با هم برابر نباشند واضح است که واسطه تقلب کرده است. درواقع، تقلب واسطه پس از بازسازی راز قابل شناسایی است. طرح‌ها در [۲۲-۲۰] از کانال خصوصی برای ارتباط بین واسطه و شرکت‌کنندگان استفاده می‌کنند. همچنین، در طرح [۲۲]، سهام شرکت‌کنندگان زیرمجموعه مجاز در مرحله بازسازی راز برای ترکیب‌کننده (یا شرکت‌کنندگانی که با هم راز را بازسازی می‌کنند) آشکار می‌شود. بنابراین، اگر شرکت‌کننده P_i در چند زیرمجموعه مجاز برای بازسازی رازهای مختلف حضور داشته باشد، ترکیب‌کننده می‌تواند یک راز را با حضور این شرکت‌کننده بازسازی کرده و باقی رازها را بدون حضور این شرکت‌کننده (با استفاده از سهم P_i که در بازسازی راز قبلی در اختیار ترکیب‌کننده قرار داده بود) بازسازی کند.

برای برطرف‌کردن مسئله استفاده از کانال خصوصی برای ارتباط بین واسطه و شرکت‌کنندگان، طرح‌هایی مطرح شدند [۲۴-۲۳]. در این طرح‌ها برای برطرف‌کردن این مشکل از سیستم رمزگذاری کلید عمومی مانند RSA[10] استفاده می‌کنند.

در این مقاله، یک طرح تسهیم راز چندگامی[11] چنداستفاده[12] براساس تابع چکیده‌ساز پیشنهاد می‌شود. در طرح پیشنهادی تقلب شرکت‌کنندگان در مرحله بازسازی راز توسط ترکیب‌کننده قابل شناسایی است. این طرح به‌دلیل استفاده از پروتکل تبادل کلید دفی- هلمن[13] مسئله استفاده از کانال خصوصی برای ارتباط بین واسطه و شرکت‌کنندگان را برطرف می‌کند. همچنین، ساختار این طرح پیشنهادی طوری است که در برابر حمله یک راز شناخته شده مقاوم است. یعنی، دشمن با استفاده از یک راز شناخته‌شده و اطلاعات عمومی دیگر، نمی‌تواند رازهای باقی‌مانده را بازسازی کند.

بقیه ساختار این مقاله به این صورت است: در بخش دوم، چند تعریف، پروتکل تبادل کلید دفی- هلمن و ویژگی‌های تابع چکیده‌ساز مورد استفاده در طرح پیشنهادی ارایه می‌شود. در بخش سوم، یک طرح تسهیم راز چندگامی چنداستفاده جدید براساس تابع چکیده‌ساز پیشنهاد می‌شود که در بخش چهارم، امنیت این طرح پیشنهادی مورد بررسی قرار می‌گیرد. در بخش پنجم، ویژگی‌های عملکردی طرح پیشنهادی با چند طرح دیگر مقایسه می‌شود. درنهایت، بخش ششم نتایج به‌دست‌آمده از مقاله بیان می‌گردد.

۲- پیش‌نیازها

در این بخش ابتدا برخی تعاریف موجود در طرح‌های تسهیم راز آورده می‌شود. سپس به پرتکل تبادل کلید دفی-هلمن و ویژگی‌های یک تابع چکیده‌ساز امن اشاره می‌شود که در طرح

1- He
2- Dawson
3- Tompa
4- Woll
5- Pieprzyk
6- Zhang
7- Das
8- Adhikari
9- Chum
10- Rivest Shamir Adleman
11- Multi-step
12- Multi-use
13- Diffie-Hellman

پیشنهادی مورد استفاده هستند.

۲-۱- تعاریف

با فرض قابل اعتماد[1]بودن واسطه، دو تعریف زیر برای یک طرح تسهیم راز چندگامی وجود دارد.

تعریف ۲-۱ (درستی[2]): اگر t شرکت‌کننده یا بیشتر بتوانند با ترکیب سهم‌هایشان راز را بازسازی کنند، آن‌گاه طرح تسهیم راز چندگامی در شرط درستی صدق می‌کند.

تعریف ۲-۲ (محرمانگی[3]): اگر کمتر از t شرکت‌کننده با ترکیب سهم‌هایشان نتوانند راز را بازسازی کنند، آن‌گاه طرح تسهیم راز چندگامی دارای شرط محرمانگی است.

تعریف زیر در مورد جلوگیری از تقلب شرکت‌کنندگان در مرحله بازسازی راز از طرح تسهیم راز چندگامی است.

تعریف ۲-۳ (قابلیت ردیابی[4]): اگر برخی شرکت‌کنندگان بداندیش در مرحله بازسازی راز به‌منظور تقلب سهم نامعتبر به ترکیب‌کننده ارایه کنند و این تقلب توسط ترکیب‌کننده با استفاده از تعهدات یا مقادیر عمومی قابل شناسایی باشد، آن‌گاه طرح تسهیم راز چندگامی دارای شرط قابلیت ردیابی است.

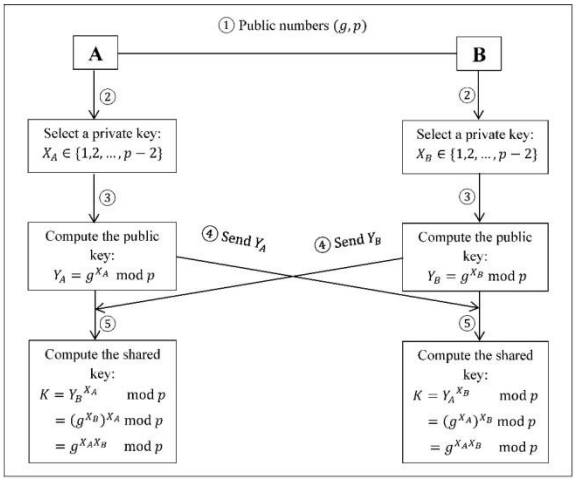
در اینجا دو تعریف حمله یک راز شناخته‌شده و $(k-1)$- ایمن را مطرح می‌کنیم.

تعریف ۲-۴ (حمله یک راز شناخته‌شده[5]): در یک طرح تسهیم راز چندگامی، یک دشمن با استفاده از یک راز شناخته شده تلاش می‌کند تا بقیه رازها را بازسازی کند.

تعریف ۲-۵ ($(k-1)$- ایمن): اگر ساختار طرح تسهیم راز چندگامی طوری باشد که در برابر حمله یک راز شناخته‌شده مقاوم باشد، آن‌گاه طرح تسهیم راز چندگامی $(k-1)$- ایمن است. (یعنی، اگر در یک طرح تسهیم راز، k راز برای به اشتراک‌گذاری وجود داشته باشد و مقدار یکی از رازها در اختیار دشمن باشد، در این صورت، دشمن با استفاده از این راز شناخته شده نتواند هیچ اطلاعاتی از $k-1$ راز باقی‌مانده به‌دست آورد.)

۲-۲- پروتکل تبادل کلید دفی-هلمن (DH)

دفی و هلمن یک روش جدید براساس سختی مسئله لگاریتم گسسته[6] (DLP) روی یک میدان متناهی pعضوی (p عددی اول است) پیشنهاد دادند [۲۵]. در این روش، دو طرف A و B می‌خواهند توافقی روی یک کلید مخفی داشته باشند. پروتکل تبادل کلید DH این امکان را به A و B می‌دهد تا از کانال ناامن (کانال عمومی) برای تبادل کلید استفاده کنند (شکل ۱).



شکل (۱): پروتکل تبادل کلید دفی- هلمن

هر بخشی می‌تواند در تبادل کلید برای به‌دست‌آوردن اطلاعات تلاش کند، اما اطلاعات به‌دست آمده را نمی‌تواند در تشخیص کلید خصوصی به‌کار ببرد. پروتکل تبادل کلید DH را می‌توان همچون سنگ‌بنایی برای رمزنگاری کلید عمومی درنظر گرفت. امنیت پروتکل تبادل کلید DH برپایه مسئله لگاریتم گسسته (DLP) می‌باشد.

دو طرف A و B با استفاده از پروتکل تبادل کلید DH برای تولید کلید مخفی مشترک، ابتدا روی عدد اول بزرگ p و یک عنصر g متعلق به $\mathbb{Z}_p^*$ توافق می‌کنند که g یک زیرگروه دوری با مرتبه بزرگ از گروه ضربی $\mathbb{Z}_p^*$ تولید می‌کند. زوج (g,p) به‌صورت عمومی منتشر می‌شوند. این زوج اعداد ممکن است برای اجراهای متعدد از پروتکل به‌کار رود و یا حتی ممکن است برای تعداد زیادی از کاربران برای دوره زمانی طولانی یکسان باشد.

۲-۳- تابع چکیده‌ساز رمزنگارانه

تابع چکیده‌ساز، یک نگاشت $H:\{0,1\}^* \to \{0,1\}^q$، چنان‌که حداقل دارای دو ویژگی زیر باشد.

۱- فشرده‌سازی: نگاشت H یک ورودی m از طول متناهی را به یک خروجی مانند y که $y=H(m)$ و از طول ثابت q می‌نگارد، طوری‌که با تغییرات در ورودی نتوان خروجی را کنترل کرد. یعنی، تغییرات کوچک در ورودی باعث تغییرات بزرگ در خروجی می‌شود.

۲- سهولت محاسبات: برای H داده شده و یک ورودی m محاسبه $y=H(m)$ آسان باشد.

تابع چکیده‌ساز رمزنگارانه باید در شرایط زیر صدق کند [۲۶]:

1- Honest
2- Correctness
3- Confidentiality
4- Traceability
5- One-Known-Secret attack
6- Discrete Logarithm Problem

۱- پیام m از ورودی با طول بیت دلخواه و خروجی با طول بیت ثابت است.
۲- تابع چکیده‌ساز باید مقاوم در برابر پیش‌تصویر باشد. یعنی، برای یک y به‌دست‌آمده با استفاده از تابع چکیده‌ساز H، یافتن پیام m طوری‌که $y = H(m)$ دشوار باشد.
۳- تابع چکیده‌ساز باید مقاوم در برابر پیش‌تصویر دوم باشد. یعنی، برای یک m_1 داده شده، یافتن $m_2 \neq m_1$ طوری‌که $H(m_2) = H(m_1)$ دشوار باشد.
۴- تابع چکیده‌ساز باید مقاوم در برابر تصادم باشد. یعنی، یافتن دو پیام $m_1 \neq m_2$ طوری‌که $H(m_1) = H(m_2)$ دشوار باشد.

دشواری یافتن یک تصادم به اندازه مقدار چکیده بستگی دارد.

۲-۴- مقاومت در برابر پیش‌تصویر پیشوند اجباری هدف منتخب

مقاومت در برابر پیش‌تصویر پیشوند اجباری هدف منتخب که به اختصار مقاومت در برابر پیش‌تصویر CTFP[1] می‌نویسند، توسط کلسی[2] و کانو[3] به‌عنوان یک ویژگی ضروری و قابل توجه برای کاربردهای خاص توابع چکیده‌ساز معرفی شد [۲۷]. فرض کنید H یک تابع چکیده‌ساز باشد. مقاومت در برابر پیش‌تصویر CTFP برای یک دشمن به‌صورت زیر تعریف می‌شود.

۱- دشمن ابتدا تعدادی پیش‌محاسبات را انجام داده و به یک مقدار چکیده h متعهد می‌شود. مقدار h "هدف منتخب" نام دارد.
۲- حریف یک پیشوند P را انتخاب کرده و در اختیار دشمن قرار می‌دهد. پیشوند P "پیشوند اجباری" نام دارد.
۳- دشمن باید پسوند $\mathcal{S}$ را طوری پیدا کند که $h = H(P \| \mathcal{S})$.

۳- طرح پیشنهادی

در این بخش، یک طرح تسهیم راز چندگامی چنداستفاده براساس تابع چکیده‌ساز پیشنهاد می‌شود. این طرح دارای سه مرحله است: مرحله آغازین، مرحله ساخت و مرحله تاییدپذیری و بازسازی راز. در مرحله آغازین، ما برای حذف کانال خصوصی از پروتکل تبادل کلید دفی- هلمن برای انتقال اطلاعات بین واسطه و شرکت‌کنندگان استفاده می‌کنیم. دلیل این‌که مرحله تاییدپذیری و بازسازی راز را یک مرحله درنظر گرفته‌شده این است که هم تایید درستی سهام شرکت‌کنندگان (قبل از بازسازی راز) و هم بازسازی راز توسط ترکیب‌کننده انجام می‌شود. مراحل طرح به‌صورت زیر است:

۳-۱- مرحله آغازین

فرض کنید $\mathcal{P} = \{P_1, P_2, ..., P_n\}$ مجموعه همه شرکت‌کنندگان و $S = \{S_1, S_2, ..., S_k\}$، k راز برای به اشتراک‌گذاری باشد. واسطه گروه ضربی $\mathbb{Z}_p^*$ و تابع چکیده‌ساز رمزنگارانه $H : \{0,1\}^* \to \{0,1\}^q$ دارای ویژگی یک‌طرفه، مقاوم در برابر پیش‌تصویر، مقاوم در برابر پیش‌تصویر پیشوند اجباری هدف منتخب را انتخاب می‌کند که p عدد اول بزرگ، $\alpha \in \mathbb{Z}_p^*$ عنصر اولیه و $\{0,1\}^q$ نشان‌دهنده همه رشته‌های دودویی به‌طول q است. سپس واسطه مقادیر (g, p) و تابع چکیده‌ساز H را به‌صورت عمومی منتشر می‌کند. واسطه تمام زیرمجموعه‌های مجاز را تعیین می‌کند. فرض کنید مشخصه زیرمجموعه مجاز l بوده و $1 \leq l \leq r$. واسطه ساختار دسترسی عمومی را منتشر می‌کند.

- **تبادل کلید دفی-هلمن**

۱- واسطه کلید خصوصی خود را از مجموعه $\{1, 2, ..., p-2\}$ انتخاب می‌کند. فرض کنید s_i کلید خصوصی واسطه (متناظر با شرکت‌کننده P_i) باشد.
۲- واسطه کلید عمومی

$$X_i = g^{s_i} \bmod p, i = 1, 2, ..., n \quad (۲)$$

را محاسبه کرده و مقدار X_i را روی تابلو اعلانات منتشر می‌کند. توجه داشته باشید که تنها واسطه به تابلو اعلانات دسترسی دارد و بخش دیگری نمی‌تواند مقادیرش را تغییر دهد.
۳- هر شرکت‌کننده p_i مقدار $s_i' \in \{1, 2, ..., p-2\}$ را به‌عنوان کلید خصوصی خودش درنظر می‌گیرد و کلید عمومی خود را به‌صورت:

$$Y_i = g^{s_i'} \bmod p, i = 1, 2, ..., n \quad (۳)$$

محاسبه کرده و مقدار Y_i را روی تابلو اعلانات مربوط به خودش منتشر می‌کند. توجه داشته باشید که بخش دیگری نمی‌تواند مقادیرش را تغییر دهد.
۴- واسطه مقدار کلید

$$K_i = Y_i^{s_i} \bmod p, i = 1, 2, ..., n \quad (۴)$$

را محاسبه می‌کند.
۵- واسطه مقادیر $h_i = H(K_i)$ و $h_i' = H(h_i)$ را

1- Chosen Target Forced Prefix
2- Kelsey
3- Kohno

محاسبه کرده و مقدار $h_i^{'}$ را به‌صورت عمومی منتشر می‌کند.

۶- هر شرکت‌کننده p_i مقدار کلید

$$K_i = X_i^{s_i^{'}} \bmod p, i = 1,2,...,n \quad (۵)$$

را محاسبه می‌کند.

هر شرکت‌کننده p_i مقادیر $h_i = H(K_i)$ و $h_i^{'} = H(h_i)$ را محاسبه کرده و مقدار $h_i^{'}$ محاسبه شده توسط خودش را با مقدار $h_i^{'}$ منتشرشده توسط واسطه مقایسه می‌کند. اگر دو مقدار باهم برابر باشند، آن‌گاه مقدار کلید K_i توسط واسطه و شرکت‌کنندگان به‌درستی محاسبه شده است.

شبه‌کد این مرحله در شکل (۲) نشان داده است.

Algorithm 1 Initialization phase

Require: No. participants n, threshold t and secrets $S_1, S_2, \ldots, S_k$.

Ensure: n quasi-shares such that t suffice to reconstruct secrets $S_1, S_2, \ldots, S_k$.

1: **If** the k secrets are fixed, input and store them in $S_1, S_2, \ldots, S_k$
2: **Otherwise**, generate randomly k secrets and store them in $S_1, S_2, \ldots, S_k$
3: $r \leftarrow \binom{n}{t}$ ▷ {minimal authorized subsets}
4: Publish $\Gamma_{0j} = \{A_{j1}, A_{j2}, \ldots, A_{jr}\}$ on the notice board
5: Select and publish hash function $H : \{0,1\}^* \rightarrow \{0,1\}^q$ on the notice board (H is one-way, second preimage resistant and chosen target forced prefix resistant)
6: Select large prime number p
7: $g \longleftarrow$ primary root of $\mathbb{Z}_p^*$
8: Write (g, p) on the notice board
9: **for** $i \leftarrow 1$ **to** n **do**
10: The dealer generates randomly s_i as her/his private key
11: $X_i \leftarrow g^{s_i} \bmod p$
12: Write X_i on the notice board
13: **end for**
14: **for** $i \leftarrow 1$ **to** n **do**
15: Each P_i generates randomly $s_i^{'}$ as her/his private key
16: $Y_i \leftarrow \alpha^{s_i^{'}} \bmod p$
17: Write Y_i on the notice board
18: **end for**
19: **for** $i \leftarrow 1$ **to** n **do**
20: $\{K_i\}_D \leftarrow Y_i^{s_i} \bmod p$
21: $\{h_i\}_D \leftarrow \text{Hash}(\{K_i\}_D)$
22: $\{h_i^{'}\}_D \leftarrow \text{Hash}\{(h_i\}_D)$
23: Write $\{h_i^{'}\}_D$ on the notice board
24: **end for**
25: **for** $i \leftarrow 1$ **to** n **do**
26: $\{K_i\}_{P_i} \leftarrow X_i^{s_i^{'}} \bmod p$
27: $\{h_i\}_{P_i} \leftarrow \text{Hash}(\{K_i\}_{P_i})$
28: $\{h_i^{'}\}_{P_i} \leftarrow \text{Hash}(\{h_i\}_{P_i})$
29: Read $\{h_i^{'}\}_D$ from the notice board
30: **if** $\{h_i^{'}\}_{P_i} = \{h_i^{'}\}_D$ **then**
31: Write "True"
32: **else**
33: Write "False"
34: **end if**
35: **end for**

شکل (۲): شبه‌کد مرحله آغازین

۳-۲- مرحله ساخت

۱- واسطه شبه‌سهم‌های شرکت‌کنندگان را به دو حالت زیر محاسبه می‌کند:

- حالت اول: واسطه زیرمجموعه مجاز A_I ($1 \le I \le r$) را به‌دلخواه انتخاب کرده و برای زیرمجموعه مجاز A_J ($1 \le J \le r, J \ne I$)، $A_I \cap A_J = \varnothing$، شبه‌سهم‌ها را به‌صورت

$$h_{lj}^{(i)} = H(h_i \parallel j) \quad (۶)$$

محاسبه می‌کند که j در واقع رشته دودویی j است. سپس مقدار

$$d_{lj} = h_{lj}^{(1)} \parallel h_{lj}^{(2)} \parallel ... \parallel h_{lj}^{(t)}, 2 \le t \le n \quad (۷)$$

$$d_i^{'} = H(h_{lj}^{(1)} \parallel h_{lj}^{(2)} \parallel ... \parallel h_{lj}^{(t)}) \quad (۸)$$

را به‌دست می‌آورد. (به‌عنوان مثال برای این حالت، برای یک مجموعه ۴ عضوی، دو زیرمجموعه ۲ عضوی وجود دارد که اشتراک آن‌ها تهی است. همچنین، برای یک مجموعه ۶ عضوی نیز ۳ زیرمجموعه ۲ عضوی یا ۲ زیرمجموعه ۳ عضوی وجود دارند که اشتراک آن‌ها تهی است و به‌همین ترتیب می‌توان ادامه داد.)

- حالت دوم: برای زیرمجموعه‌های مجاز باقی‌مانده که $A_I \cap A_J \ne \varnothing$ شبه‌سهم‌ها را به‌صورت

$$h_{lj}^{(i)} = H(h_i \parallel l \parallel j) \quad (۹)$$

محاسبه می‌کند. سپس مقادیر d_i و $d_i^{'}$ را همانند (۷) و (۸) به‌دست می‌آورد.

۲- واسطه مقادیر $H(h_{lj}^{(i)})$ را محاسبه کرده و به صورت عمومی منتشر می‌کند.

۳- واسطه مقدار کنترل عمومی C_{lj} را به‌صورت زیر تولید و منتشر می‌کند.

$$C_{lj} = S_j \oplus d_{lj} \quad (۱۰)$$

۴- واسطه مقدار $S_j^{'} = H(S_j)$ را محاسبه کرده و به‌صورت عمومی منتشر می‌کند.

شبه‌کد این مرحله در شکل (۳) نشان داده شده است.

Algorithm 2 Construction phase

// The lines are performed by the dealer D:
for $I \leftarrow 1$ **to** r **do**
  for $J \leftarrow 1$ **to** r **do**
    for $I \neq J$ **do**
      if $A_I \cap A_J = \emptyset$ **then**
        $h_{lj}^{(i)} \leftarrow \mathrm{Hash}(h_i||j)$ ▷ {|| means concatenation}
      else
        $h_{lj}^{(i)} \leftarrow \mathrm{Hash}(h_i||l||j)$
      end if
      $h_{lj}^{(i)'} \leftarrow \mathrm{Hash}(h_{lj}^{(i)})$
      Write $\{h_{lj}^{(i)'}\}_D$ on the notice board
      $d_{lj} \leftarrow h_{lj}^{(1)}||h_{lj}^{(2)}||\ldots||h_{lj}^{(t)}$
      $d'_{lj} \leftarrow \mathrm{Hash}(h_{lj}^{(1)}||h_{lj}^{(2)}||\ldots||h_{lj}^{(t)})$
      $C_{lj} \leftarrow S_j \oplus d'_{lj}$ ▷ {$\oplus$ means XOR}
      Write C_{lj} on the notice board
    end for
  end for
end for
for $j \leftarrow 1$ **to** k **do**
  $S'_j \leftarrow \mathrm{Hash}(S_j)$
  Write $\{S'_j\}_D$ on the notice board
end for

شکل (۳): شبه‌کد مرحله ساخت

۳-۳- مرحله تاییدپذیری و بازسازی راز

۱- شرکت‌کنندگان زیرمجموعه مجاز شبه‌سهم خود را با توجه به حالت اول یا حالت دوم تولید شبه‌سهم‌ها محاسبه کرده و برای ترکیب‌کننده ارایه می‌دهد.

۲- ترکیب‌کننده پس از دریافت شبه‌سهم‌های شرکت‌کنندگان، مقدار چکیده آن‌ها را محاسبه کرده و با مقدار چکیده‌ای که واسطه در مرحله ساخت به‌صورت عمومی منتشر کرده بود، مقایسه می‌کند. اگر مقادیر چکیده‌ای که ترکیب‌کننده از شبه‌سهم‌های ارایه‌شده به‌دست می‌آورد با مقدار چکیده شبه‌سهم‌هایی که واسطه در مرحله ساخت منتشر کرده است، برابر باشد، در این‌صورت، ترکیب‌کننده این شبه‌سهم‌ها را می‌پذیرد؛ درغیر این‌صورت، از شرکت‌کنندگان درخواست می‌کند که دوباره شبه‌سهم خود را ارایه دهند.

۳- ترکیب‌کننده مقدار $d_{lj}^{(i)}$ را همانند (۷) یا (۹) محاسبه می‌کند.

۴- ترکیب‌کننده با استفاده از مقدار $d_{lj}^{(i)}$ و مقادیر عمومی C_{lj}ها، رازهای $S_1, S_2, \ldots, S_k$ را به‌صورت زیر بازسازی می‌کند.

$$S_j = C_{lj} \oplus d_{lj} \qquad (۱۱)$$

۵- ترکیب‌کننده مقدار $S'_j = H(S_j)$ را محاسبه کرده و با مقدار چکیده راز منتشرشده توسط واسطه در مرحله ساخت مقایسه می‌کند. اگر دو مقدار چکیده با هم برابر باشند، در این‌صورت، راز به‌درستی بازسازی شده است. اما اگر دو مقدار چکیده با هم برابر نباشند، در این صورت، واضح است که واسطه متقلب بوده و مقادیر عمومی جعلی منتشر کرده است.

شبه‌کد این مرحله در شکل (۴) نشان داده شده است.

Algorithm 3 Verification and secret recovery phases

Require: quasi-shares and public controls
Ensure: The secrets $S_1, S_2, \ldots, S_k$
for $l \leftarrow 1$ **to** r **do**
  for $j \leftarrow 1$ **to** k **do**
    for $i \leftarrow 1$ **to** t **do**
      Provide quasi-share $\{h_{lj}^{(i)}\}_{p_i}$ to the combiner C
    end for
  end for
end for
// The next lines are performed by the combiner C:
for $l \leftarrow 1$ **to** r **do**
  for $j \leftarrow 1$ **to** k **do**
    for $i \leftarrow 1$ **to** t **do**
      $\{h_{lj}^{(i)'}\}_C \leftarrow H\left(\{h^{(i)}\}_{P_i}\right)$
      Read $\{h_{lj}^{(i)'}\}_D$ from the notice board
      if $\{h_{lj}^{(i)'}\}_C = \{h_{lj}^{(i)'}\}_D$ **then**
        Write "quasi-share $\{h_{lj}^{(i)}\}_{P_i}$ is Valid"
      else
        Write "quasi-share $\{h_{lj}^{(i)}\}_{P_i}$ is Invalid"
      end if
    end for
  end for
end for
for $l \leftarrow 1$ **to** r **do**
  for $j \leftarrow 1$ **to** k **do**
    for $i \leftarrow 1$ **to** t **do**
      $d_{lj} \leftarrow h_{lj}^{(1)}||h_{lj}^{(2)}||\ldots||h_{lj}^{(t)}$
      $d'_{lj} \leftarrow \mathrm{Hash}(h_{lj}^{(1)}||h_{lj}^{(1)}||\ldots||h_{lj}^{(t)})$
      Read C_{lj} from the notice board
      $S_j \leftarrow C_{lj} \oplus d'_{lj}$
      $\{S_j\}_C \leftarrow \mathrm{Hash}(S_j)$
      Read $\{S'_j\}_D$ on the notice board
      if $\{S_j\}_C = \{S'_j\}_D$ **then**
        Write "the reconstructed secret is Valid"
      else
        Write "the reconstructed secret is Invalid"
      end if
    end for
  end for
end for

شکل (۴): شبه‌کد مرحله تأییدپذیری و بازسازی راز

۴- تحلیل طرح پیشنهادی

قضیه ۴-۱- (محرمانگی): دشمن با همکاری $t-1$ شرکت‌کننده نمی‌تواند سهام شرکت‌کنندگان دیگر را به‌دست

آورده و رازها را بازسازی کند.

اثبات: بدون کاستن از کلیت، فرض کنید شرکت‌کنندگان $P_1,P_2,...,P_{t-1}$ به‌ترتیب با سهم‌های $h_1,h_2,...,h_{t-1}$ قصد داشته باشند با ترکیب سهم‌هایشان و همچنین، اطلاعات عمومی منتشرشده، راز را بازسازی کنند. برای انجام این‌کار، $t-1$ شرکت‌کننده می‌توانند برای به‌دست‌آوردن شبه‌سهم شرکت‌کننده P_t با استفاده از

$$d_{lj} = H(h_{lj}^1 \| h_{lj}^2 \| ... \| h_{lj}^t) \quad (۱۲)$$

تلاش کنند. اما از آن‌جا که تابع‌چکیده‌ساز H دارای ویژگی مقاومت در برابر پیش‌تصویر CTFP است، درنتیجه، $t-1$ شرکت‌کننده نمی‌توانند با این روش مقدار شبه‌سهم h_{lj}^t را به‌دست آورند.

قضیه۴-۲- (تأیید شرکت‌کنندگان): شرکت‌کنندگان بداندیش در مرحله بازسازی راز با ارایه سهم جعلی نمی‌توانند از بازسازی راز اصلی جلوگیری کنند و تقلب آن‌ها توسط ترکیب‌کننده قابل شناسایی است.

اثبات: فرض کنید برخی شرکت‌کنندگان بداندیش قصد تقلب داشته باشند. این شرکت‌کنندگان در مرحله بازسازی راز برای ترکیب‌کننده شبه‌سهم جعلی $\overline{h_{lj}^{(i)}}$ ارایه می‌دهند. ترکیب‌کننده پس از دریافت این شبه‌سهم‌ها، مقدار چکیده آن‌ها را به‌دست آورده و با مقدار چکیده منتشرشده توسط واسطه مقایسه می‌کند. از آن‌جا که تابع چکیده‌ساز H مقاوم در برابر پیش‌تصویر است، بنابراین، شرکت‌کنندگان بداندیش نمی‌توانند سهم‌های $\overline{h_{lj}^{(i)}}$ را طوری پیدا کنند که $H(\overline{h_{lj}^{(i)}}) = H(h_{lj}^{(i)})$. درنتیجه، این تقلب توسط ترکیب‌کننده قبل از بازسازی راز قابل شناسایی است.

قضیه ۴-۳- (امنیت سهام و رازها): یک دشمن بیرونی با استفاده از اطلاعات عمومی منتشرشده از سهام و رازها نمی‌تواند هیچ اطلاعاتی مفیدی برای بازسازی راز به‌دست آورد.

اثبات: فرض کنید دشمن بیرونی قصد دارد تا با استفاده از اطلاعات عمومی منتشرشده، رازها را بازسازی کند. دشمن بیرونی می‌تواند با استفاده از مقادیر (g,p) و X_i منتشرشده در مرحله تبادل کلید برای به‌دست‌آوردن سهام شرکت‌کنندگان تلاش کند. اما از آن‌جا که فرض کردیم محاسبه لگاریتم گسسته دشوار است، دشمن بیرونی با استفاده از این اطلاعات عمومی نمی‌تواند هیچ اطلاعاتی از سهام شرکت‌کنندگان به‌دست آورده و رازها را بازسازی کند. همچنین، دشمن بیرونی می‌تواند با استفاده از مقادیر h_i' و S_j' برای به‌دست‌آوردن سهام و رازها تلاش کند. برای انجام این‌کار، دشمن بیرونی باید توانایی این را داشته باشد که معکوس مقادیر h_i' و S_j' را به‌دست آورد. اما از آن‌جا که تابع چکیده‌ساز H یک‌طرفه است، دشمن بیرونی نمی‌تواند هیچ اطلاعاتی از این مقادیر عمومی به‌دست آورد.

قضیه ۴-۴- ($(k-1)$ - ایمن): ساختار طرح پیشنهادی در برابر حمله یک راز شناخته‌شده مقاوم است.

اثبات: فرض کنید دشمن بیرونی یکی از رازها، به‌عنوان مثال، راز S_j را در اختیار داشته و قصد داشته باشد بقیه رازها را با استفاده از این راز شناخته‌شده، بازسازی کند. دشمن با استفاده از مقدار عمومی C_{lj} و راز شناخته شده S_j، مقدار

$$d_{lj} = S_j \oplus C_{lj} \quad (۱۳)$$

را محاسبه می‌کند، اما با به‌دست‌آوردن این مقدار نمی‌تواند در مورد سهام شرکت‌کنندگان اطلاعاتی کسب کند. از آن‌جا که شبه‌سهم شرکت‌کنندگان برای بازسازی هر راز تغییر می‌کند، بنابراین، لازم است که دشمن سهم شرکت‌کنندگان را به‌دست آورد. اما چون تابع چکیده‌ساز یک‌طرفه است، دشمن نمی‌تواند معکوس مقادیر عمومی h_i' را محاسبه کرده و سهم شرکت‌کنندگان را به‌دست آورد. در واقع می‌توان گفت که با آشکارشدن یک راز، امنیت باقی رازها به خطر نمی‌افتد. بنابراین، ساختار طرح پیشنهادی در برابر حمله یک راز شناخته‌شده امن است.

نتیجه ۴-۱- (چندبار استفاده): طرح پیشنهادی یک طرح چنداستفاده است. در این طرح، در مرحله بازسازی راز، به‌جای این‌که سهم‌ها به ترکیب‌کننده ارایه شود، شبه‌سهم‌های تولیدشده از سهم‌ها برای ترکیب‌کننده ارسال می‌شود. دلیل آن این است که اگر شرکت‌کنندگان در مرحله بازسازی راز سهم خودشان را ارسال کنند، آن‌گاه ترکیب‌کننده می‌تواند بدون حضور شرکت‌کنندگان رازهای دیگر را بازسازی کند. به‌عنوان مثال، در طرح [۲۱]، در مرحله بازسازی راز سهم همه شرکت‌کنندگان زیرمجموعه مجاز برای بازسازی راز آشکار می‌شود. همچنین، در طرح [۱۴]، پس از بازسازی رازها، سهم شرکت‌کنندگان قابل استفاده مجدد نخواهد بود و این امنیت رازهای بازسازی‌نشده را به‌خطر می‌اندازد. لذا در طرح پیشنهادی ما سعی کردیم این مشکل را برطرف کنیم. به این صورت که هر شرکت‌کننده در این طرح فقط یک سهم دارد و با استفاده از سهمش شبه‌سهم‌های مربوط به هر راز محاسبه کرده و در مرحله بازسازی راز برای ترکیب‌کننده ارسال می‌کند. بنابراین، ترکیب‌کننده برای بازسازی هر راز باید شبه‌سهم‌های شرکت‌کنندگان را درخواست کند و بدون حضور حتی یک شرکت‌کننده هم نمی‌تواند راز را بازسازی

کند. حال چون مقدار سهم‌های شرکت‌کنندگان آشکار نمی‌شود، بنابراین، سهم‌ها قابل استفاده مجدد هستند.

نتیجه ۴-۲- (به‌روزرسانی طرح پیشنهادی): در طرح‌های تسهیم راز ممکن است که لازم باشد راز عوض شده و راز دیگری جایگزین شود. به‌علاوه، ممکن است نیاز باشد که زیرمجموعه شرکت‌کنندگان یا ساختار دسترسی تغییر یابد. در طرح پیشنهادی، برای جایگزینی راز جدید می توان سهم‌ها را ثابت نگه داشت اما برای جلوگیری از حمله ردیابی [۲۸] باید مقدار شبه‌سهم‌ها هم تغییر یابد که درنهایت، کنترل‌های عمومی نیز با تغییر راز و شبه‌سهم‌ها تغییر می‌یابد.

۵- مقایسه عملکردها

در این بخش، ویژگی‌های عملکردی در جدول (۱) و هزینه محاسباتی در جدول (۲) طرح پیشنهادی با چند طرح دیگر مورد مقایسه قرار می‌گیرد.

ویژگی ۱) مقاومت در برابر تقلب شرکت‌کنندگان؛

ویژگی ۲) مقاومت در برابر حمله یک راز شناخته‌شده؛

ویژگی۳) قابلیت استفاده مجدد از سهم؛

ویژگی ۴) بدون کانال خصوصی.

توجه کنید که در جدول (۲)، برای هزینه محاسباتی، تنها توان‌رسانی پیمانه‌ای درنظر گرفته شده است.

جدول (۱): مقایسه ویژگی‌های عملکردی

ویژگی	HD [۱۴]	ZZZ [۲۳]	DM [۲۴]	DA [۲۰]	CZ [۲۱]	طرح پیشنهادی
۱	خیر	بله	بله	بله	بله	بله
۲	بله	_	_	بله	خیر	بله
۳	خیر	بله	بله	بله	خیر	بله
۴	خیر	بله	بله	خیر	خیر	بله

جدول (۲): هزینه محاسباتی

طرح	مرحله آغازین		ساخت	بازسازی راز
	واسطه	P_i	واسطه	C یا P_i
HD [۱۴]	0	0	0	0
ZZZ [۲۳]	0	1	$n+1$	t
DM [۲۴]	$2n$	1	0	$t-1$
DA [۲۰]	0	0	0	0
CZ [۲۱]	0	0	0	0
طرح‌جدید	$2n$	2	0	0

C همان ترکیب‌کننده است.

۶- کارهای آینده

در این مقاله، در طرح پیشنهادی هنوز مشکل تقلب واسطه وجود دارد. لذا نویسندگان این مقاله دنبال راه‌حلی برای برطرف این مشکل هستند. همچنین، نویسندگان در تلاش هستند تا طرح تسهیم راز تاییدپذیر عمومی (PVSS[1]) براساس تابع چکیده‌ساز و کاربرد آن در محاسبات ابری مطرح کنند که دارای پیچیدگی محاسباتی کمتری نسبت به طرح‌های PVSS مطرح‌شده باشد. در طرح PVSS، مراحل تاییدپذیری واسطه و شرکت‌کنندگان به‌صورت عمومی انجام می‌شود. یعنی هر تاییدکننده‌ای می‌تواند درستی مقادیر ارایه‌شده از طرف واسطه و شرکت‌کنندگان و همین‌طور مقادیر منتشرشده را مورد بررسی قرار دهد.

۷- نتیجه‌گیری

در این مقاله، یک طرح تسهیم راز چندگامی چنداستفاده براساس تابع چکیده‌ساز پیشنهاد شد. در این طرح، رازها گام به گام بازسازی می‌شوند. هر شرکت‌کننده تنها یک سهم دارد، اما رازها با استفاده از شبه‌سهم‌های متفاوت بازسازی می‌شوند. بنابراین، با بازسازی یک راز امنیت دیگر رازها به‌خطر نمی‌افتد. لذا، ساختار طرح جدید در برابر حمله یک راز شناخته‌شده امن است. همچنین، در این طرح، با استفاده از پروتکل تبادل کلید دفی- هلمن، ارتباط بین واسطه و شرکت‌کنندگان از طریق کانال خصوصی امکان‌پذیر است. به‌دلیل استفاده از تابع چکیده‌ساز، طرح پیشنهادی در مقایسه با برخی طرح‌های دیگر دارای محاسبات سریع و آسان بوده و لذا کارایی آن بیشتر است.

۸- منابع

[1] R. Cramer and I. Damgard, "Multiparty computation, an introduction," Contemporary cryptology, 2005.

[2] K. Fokine, "Key management in ad hoc networks," Student thesis, ISRN LITH-ISY-EX-3322, Linköping University, Department of Electrical Engineering, 2002, Available from: http://www.ep.liu.se/exjobb/isy/2002/3322/.

[3] S. Iftene, "Secret sharing schemes with applications in security protocols," Technical report, University Alexandru Ioan Cuza of Iasi, Faculty of Computer Science, 2006.

[4] B. Schoenmaker "A simple publicly verifiable secret sharing scheme and its application to electronic voting," Lecture Notes in Computer Science, pp. 148-164, 1999.

[5] G. R. Blakley, "Safeguarding cryptographic keys," In: Proc. AFIPS'79 Nat. Computer Conf., vol. 48, pp. 313-317, AFIPS Press, 1979.

[6] A. Shamir "How to share a secret," Comm. ACM, vol. 22, pp. 612-613, 1979.

[7] C. C. Thien and J. C. Lin, "Secret image sharing," Comput. Graph., vol. 26, pp. 765-770, 2002.

1- Publicly Verifiable Secret Sharing

[8] S. J. Shyu and Y. R. Chen, "Threshold secret image sharing by Chinese remainder theorem," Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE, 2008.

[9] T. H. Chen and C. S. Wu, "Efficient multi-secret image sharing based on Boolean operations," Signal Process, vol. 91, pp. 90-97, 2011.

[10] E. R. Verheul and H. C. Van Tilborg, "Constructions and properties of k out of n visual secret sharing schemes," Designs, Codes and Cryptogr., vol. 11, pp. 179-196, 1997.

[11] J. B. Feng, H. C. Wu, S. C. Tsai, F. y. Chang, and Y. P. Chu, "Visual secret sharing for multiple secrets," Pattern Recognit., vol. 41, pp. 3572-3581, 2008.

[12] A. R. Mirghadri and F. Sheikh Sangtajan, "An efficient visual multi-secret sharing scheme," Journal of Electronic and Syber defence, vol. 3, pp. 1-9, 2016. (In Persian)

[13] M. R. Azariun, M. haghjoo, and M. ghayoori, "Privacy and soundness of outsourced data based on threshold secret sharing," Journal of electronic and syber defence vol. 3, pp. 63-72, 2013. (In Persian)

[14] J. He and E. Dawson, "Multistage secret sharing based on one-way function," Electron. Lett., vol. 30, pp. 1591-1592, 1994.

[15] M. Tompa and H. Woll, "How to share a secret with cheaters," J. Cryptology, vol. 1, pp. 133-138, 1998.

[16] J. Pieprzyk and X. M. Zhang, "Constructions of cheating immune secret sharing," ICICS 2001, Springer, Verlag, (LNCS, 2288), pp. 226-243, 2001.

[17] J. Pieprzyk and X. M. Zhang, "On cheating immune secret sharing," Discrete Math. Theor. Comput. Sci., vol. 6, pp. 253-264, 2004.

[18] R. D. Prisco and A. Santis, "Cheating immune (2, n)-threshold visual secret sharing," SCN 2006, Springer, Berlin, (LNCS, 4116), pp. 216-228, 2006.

[19] X. M. Zhang and J. Pieprzyk, "Cheating immune secret sharing," ICICS, LNCS, 2229, Springer, Verlag, pp. 144-149, 2001.

[20] A. Das and A. Adhikari, "An efficient multi-use multi-secret sharing scheme based on hash function," Appl. Math. Lett., vol. 23, pp. 993-996, 2010.

[21] C. S. Chum and X. Zhang, "Hash function-based secret sharing scheme designs," Secur. Commun. Netw., vol. 6, pp. 584-592, 2013.

[22] C. S. Chum, and X. Zhang, "Implementations of a Hash Function Based Secret Sharing Scheme," Appl. Secur. Res., vol. 10, pp. 525-542, 2015.

[23] J. Zhao, j. Zhang, and R. Zhao, "A practical multi-secret sharing scheme," Comput. Stand. Inter., vol. 29, pp. 138-141, 2007.

[24] M. H Dehkordy and S. Mashhadi, "An efficient threshold verifiable multi-secret sharing,'' Comput. Stand. Inter., vol. 30, pp. 187-190, 2008.

[25] W. Diffie and M. Hellman, "New direction in cryptography," IEEE Trans. Inf. Theory, vol. 22, pp. 644-454, 1976.

[26] P. Rogaway and T. Shrimpton, "Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance," In International Workshop on Fast Software Encryption, pp. 371-388. Springer, Berlin, Heidelberg, 2004.

[27] J. Kelsey and T. Kohno, "Herding hash functions and the Nostradamus attack," In Serge Vaudenay, editor, Advanes in Cryptology-EUROCRYPT 2006, volume 4004 of Lecture Notes in Computer Science, pages, pp. 183–200, Springer, 2006.

[28] S. Bahrami and A. Payandeh, "Traceability attack to LY 2-way authentication protocol in the RFID systems," The 7th National Conference of Command, Control, Communications, Computer & Intelligence, 2013. (In Persian)

Journal of Electronical & Cyber Defence
Vol. 6, No. 3, 2018, Serial No. 23

A Hash-Based Multi-Use Multi-Stage Secret Sharing Scheme with General Access Structure

M. Farhadi*, H. Bypour, R. Mortazavi

*Damghan University

(Received: 13/11/2017, Accepted: 07/04/2018)

ABSTRACT

In the multi-use multi-stage secret sharing scheme, the dealer is able to share several secrets among a group of participants, and the secrets are reconstructed stage by stage such that the reconstruction of secrets at earlier stages does not reveal or weaken the secrecy of the remaining secrets. Since the hash functions are quick and easy to calculate, in this paper, we propose a multi-use multi-secret sharing scheme based on a hash function that makes the method very efficient. This scheme is resistant to the cheating of participants. Also, by using the Diffie-Hellman key exchange protocol, the dealer and participants communicate with each other through a public channel. The structure of the proposed scheme is safe against one-known-secret attack.

Keywords: Secret Sharing Scheme, Multi-stage, Multi-use, Hash Function, General Access Structure, One-knownsecret Attack

* Corresponding Author Email: farhadi@du.ac.ir