دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۰، جلد ۱۹، شماره ۱ (۵۲-۶۱)
https://monadi.isc.org.ir

ارائه‌شده در شانزدهمین کنفرانس بین المللی انجمن رمز ایران در دانشگاه فردوسی مشهد، ۶ و ۷ شهریور ۱۳۹۸

یک طرح تسهیم راز مقاوم در برابر تقلب مبتنی بر گراف★

میثم نوروزی*، ترانه اقلیدس و محمدرضا عارف

دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران، ایران

اطلاعات مقاله

کلمات کلیدی:
تسهیم راز
تسهیم راز مقاوم
شناسایی متقلب
متقلب عجول
گراف جهت‌دار
کد احراز اصالت پیام

dor: 10.0000/000000000

نوع مقاله: پژوهشی

چکیده

طرح تسهیم راز آستانه‌ای امکان تسهیم یک راز را در میان تعدادی از اعضا، به‌نام شرکت‌کنندگان، با ارائه سهم‌هایی به آنان فراهم می‌سازد. بازیابی راز تنها به کمک تعداد مشخص از سهم‌ها امکان‌پذیر است. بازیابی درست راز در این طرح‌ها منوط به رفتار درست شرکت‌کنندگان است. اما در دنیای واقعی ممکن است برخی از شرکت‌کنندگان تلاش کنند سهم‌های نادرستی ارائه دهند، که تقلب نام دارد. یک طرح تسهیم راز مقاوم این امکان را فراهم می‌کند که با حضور تعدادی متقلب هم‌چنان راز به درستی بازیابی شود. در این مقاله طرح تسهیم راز مقاومی ارائه می‌شود که با وجود تعداد بیشینه ممکن از شرکت‌کنندگان متقلب، راز به درستی بازیابی شود. در این طرح برای متقلب‌ها توانایی‌های زیادی در نظر می‌گیریم. آنان می‌توانند سهم‌های خود را متناسب با سهم‌های سایرین تغییر دهند و با یکدیگر ارتباط داشته باشند تا بهترین شیوه را برای تقلب به کار گیرند. این طرح امکان شناسایی و حذف متقلب‌ها را به کمک یک گراف جهت‌دار فراهم می‌سازد و نسبت به طرح‌های پیشین از پیچیدگی کمتری برای بازیابی راز برخوردار است. در عین حال دارای طول سهم کمتری نسبت به طرح‌های موجود است، که به کاهش سربار مخابراتی طرح می‌انجامد. به این ترتیب، طرح تسهیم راز پیشنهادی از دو جنبه پیچیدگی بازیابی راز و طول سهم از کارآیی بیشتری نسب به طرح‌های موجود برخوردار است.

۱ مقدمه

در دنیای امروز در برخی موارد دسترسی یک شخص به تنهایی به اطلاعاتی خاص مطلوب نیست و ما نیازمند آن هستیم که امکان دسترسی در این موارد تنها در صورت وجود مجموعه‌ای از افراد امکان‌پذیر باشد. در بسیاری از طرح‌های رمزنگاری سپردن مالکیت یک راز به یک شخص نامطلوب است. بنابراین، به جای آن مالکیت این راز در بین گروهی از اشخاص تقسیم می‌شود. رمزنگاری آستانه‌ای شامل راهکارهایی است که این امکان را فراهم می‌سازد. ایده اصلی آن توسط شامیر ارائه شده است. یک راز، توسط یک مرجع مورد اعتماد به نام توزیع‌کننده، به سهم‌های مختلف تسهیم می‌شود، به طوری که تنها با دسترسی تعداد معینی، مانند t'، از سهم‌ها، بتوان راز را بازیابی کرد و با تعداد کمتر از t' سهم، نه‌تنها راز قابل بازیابی نباشد بلکه هیچ اطلاعاتی از آن نیز نشت پیدا نکند. چنین طرحی، طرح آستانه‌ای (t', n) نام دارد. در این طرح، n تعداد اعضایی است که در طرح حضور دارند و شرکت‌کنندگان در طرح نامیده می‌شوند و t' نیز آستانه طرح نامیده می‌شود.

در طرح تسهیم راز شامیر فرض بر این است که شرکت‌کنندگان پروتکل

★از کمیته علمی شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول
آدرس‌های رایانامه: meysam_fr7@yahoo.com (میثم نوروزی)، teghlidos@sharif.edu (ترانه اقلیدس)، aref@sharif.edu (محمدرضا عارف)

را به درستی اجرا می‌کنند. حال آنکه در دنیای واقعی امکان به اشتراک گذاشتن سهم نادرست توسط برخی از شرکت‌کنندگان وجود دارد، که فرآیند بازیابی راز را با مشکل روبرو می‌سازد. اگر این عمل به طور عمدی صورت پذیرد آن را تقلب [۱] و شرکت‌کنندگانی که چنین تقلبی را انجام می‌دهند متقلب [۲] می‌نامیم. بنابراین، لازم است طرح‌هایی ارائه شود که بتواند با حضور تعدادی متقلب، راز را به درستی بازیابی کند. در این راستا انواع مختلفی از طرح‌ها معرفی شده‌اند. بر این اساس توزیع کننده سهم و بازیابی‌کننده راز می‌توانند مورد اعتماد یا غیرقابل اعتماد باشند که حالت نخست موضوع این نوشتار است. در این حالت ابتدا تشخیص رخداد تقلب و سپس شناسایی متقلب‌ها مورد نظر است. اما آن‌چه مهمتر به نظر می‌رسد بازیابی راز با حضور متقلب‌هاست که به طرح‌های تسهیم راز مقاوم (RSS [۳]) معروفند. در این پژوهش روی این طرح‌ها تمرکز می‌کنیم. طرح‌هایی که تنها رخداد تقلب را مشخص می‌کنند، طرح‌های تسهیم راز با قابلیت تشخیص تقلب (CDSS [۴]) و طرح‌هایی که متقلب‌ها را نیز معرفی می‌کنند، طرح‌های تسهیم راز با قابلیت شناسایی متقلب (CISS [۵]) نامیده می‌شوند. در این طرح‌ها منظور از سهم تمام اطلاعات منحصر به فردی است که به طور محرمانه به هر شرکت‌کننده داده می‌شود.

نخستین طرحی که در این راستا ارائه شد توسط Topma و Woll [۱] بوده است که به بررسی تشخیص رخداد تقلب پرداخته است. البته پیش از آن McEliece و Sarwate [۲] با برقراری رابطه‌ای میان تسهیم راز شامیر و کدهای Reed-Solomon به شناسایی متقلب‌ها در تسهیم راز پرداخته‌اند. این ایده مبنای بسیاری از طرح‌هایی بوده است که تاکنون ارائه شده است. آنان همچنین نشان دادند در طرحی با n شرکت‌کننده که t عضو آن متقلب است به ازای $t < \frac{n}{۳}$ طرح شامیر مقاوم است. هم‌چنین اگر $t \geq \frac{n}{۲}$، آنگاه امکان بازیابی صحیح راز وجود ندارد و برای $\frac{n}{۳} \leq t < \frac{n}{۲}$ امکان بازیابی درست راز به‌ازای سهم‌های بلندتری نسبت به طول راز وجود دارد. یافتن کران برای اندازه سهم‌ها یکی از موضوعات مهم در سال‌های اخیر بوده است که موضوع مقالات [۳-۶] است. در این کارها کران پایین اندازه سهم‌ها برای تسهیم راز در حضور متقلب اثبات شده‌اند.

تعدادی از طرح‌های ارائه شده به طرح‌های تسهیم راز در حضور متقلب اختصاص یافته است. در این طرح‌ها، هدف بازیابی درست راز در حضور متقلب‌هاست، که موضوع این مقاله است. دو پارامتر در کارآیی این طرح‌ها اثرگذارند؛ طول سهم، که سربار مخابراتی طرح را مشخص می‌کند، و پیچیدگی محاسباتی بازیابی راز، که به نحوی بیانگر سربار محاسباتی طرح است. موضوعی که لازم است به آن توجه شود این است که راز بازیابی شده در این طرح‌ها با احتمال کوچکی نادرست هستند و یکی دیگر از جنبه‌هایی که در این طرح‌ها باید لحاظ شود کاهش این احتمال خطاست.

در سال ۱۹۸۹، Rabin و Ben-Or [۷] از کدهای احراز اصالت پیام برای وارسی سهم‌های تولید شده توسط طرح آستانه‌ای شامیر استفاده کرده‌اند. در طرح ارائه شده، به ازای هر سهم s_i مربوط به شرکت‌کننده P_j، برچسب [۶] τ_{ij} به وسیله کلید k_{ji} تولید و به عضو P_j داده می‌شود. به این ترتیب، به‌ازای یک مقدار دلخواه مثبت η برای آن‌که احتمال خطای بازیابی $۲^{-\eta}$ باشد، باید از کد احراز اصالت پیام با احتمال خطای حداکثر $۲^{-\eta}$ استفاده شود. پس علاوه بر سهم اصلی باید $n\eta$ بیت اضافی به هر شرکت‌کننده داده شود، که منجر به افزایش طول سهم می‌شود. از این رو، طرح‌های بعدی با هدف کاهش این سربار به طرح تسهیم راز معرفی شده‌اند.

Cramer و همکارانش [۶] در سال ۲۰۰۱ طرحی ارائه دادند که در آن برای تسهیم راز اصلی s به کمک مقادیر تصادفی r و $g = s \cdot r$ از سه طرح تسهیم راز مجزا با آستانه t'، برای تسهیم پارامترهای s، r و g استفاده می‌شود. سپس، برای بازیابی s به‌ازای تمام زیرمجموعه‌های $t' + ۱$عضوی، s، r و g بازیابی می‌شوند و با بررسی برقراری تساوی $g = s \cdot r$ صحت بازیابی راز بررسی می‌شود. با فرض این که $\mathbb{F}$ یک میدان با $۲^{\eta+n}$ عضو باشد و $s \in \mathbb{F}$، اگر اندازه سهم از مرتبه $\mathcal{O}(\eta+n)$ باشد، احتمال خطا برابر با $۲^{-\eta}$ خواهد بود. در این طرح چون تمامی زیرمجموعه‌های $t' + ۱$عضوی از n شرکت‌کننده در نظر گرفته می‌شوند، زمان اجرای طرح نمایی خواهد بود. همچنین، Jhanwar و Safavi-Naini [۸] در سال ۲۰۱۳ طرح مشابهی ارائه دادند، که در آن نیز پیچیدگی بازیابی راز نمایی است، اما طول سهم برابر با طول راز است. در این طرح به کمک n پارامتر عمومی، یک تسهیم راز مقاوم در برابر t متقلب، به ازای $\frac{n}{۳} \leq t < \frac{n}{۲} - ۱$، معرفی شده است.

در سال ۲۰۱۲، Cevallos و همکارانش [۹] طرحی با اندازه سهم $\mathcal{O}\left(\eta + n + \log_۲(n) + \log_۲(m)\right)$ و زمان اجرای چندجمله‌ای ارائه دادند که در آن m طول راز است. در این طرح از کدهای احراز اصالت پیام و کدهای تصحیح خطای Reed-Solomon استفاده شده است. ایده‌ی اصلی این طرح تخصیص برچسب به ازای هر سهم به تمام شرکت‌کنندگان است، به نحوی که در مرحله بازیابی راز، وارسی سهم توسط هر شرکت‌کننده جهت به‌کارگیری آن سهم در بازیابی راز تأثیرگذار است. به این منظور در مرحله بازیابی راز، زیرمجموعه‌هایی از شرکت‌کنندگان تشکیل می‌شود که سهم اعضای آن‌ها توسط تمام اعضای دیگرِ آن زیرمجموعه مورد تأیید قرار گرفته باشد. بازیابی راز به کمک سهم‌های بزرگترینِ این زیرمجموعه‌ها انجام می‌شود. این طرح در برابر دسته‌ای از متقلب‌ها که متناسب با سهم سایر اعضا تصمیم به ارائه سهم خود، به صورت درست یا نادرست، می‌گیرند مقاوم است که به آن متقلب عجول [۷] گفته می‌شود.

Adhikari و همکارانش [۱۰] برای بهبود طرح Roy و همکارانش [۱۱] برای کاهش طول سهم از خانواده توابع چکیده‌ساز فراگیر قوی (SU2 [۸]) استفاده کرده‌اند. علاوه بر آن، همچنان بزرگترین زیرمجموعه از شرکت‌کنندگان درستکار برای بازیابی راز تشکیل می‌شود و از سهم آن‌ها

[1] cheating [2] cheater [3] Robust Secret Sharing [4] Cheating Detectable Secret Sharing [5] Cheater Identifiable Secret Sharing

[6] tag [7] rushing [8] Strongly Universal family of hash functions

برای بازیابی راز استفاده می‌شود. در نهایت نیز از قابلیت حذف سهم‌های نادرست به کمک کدهای تصحیح خطای Reed-Solomon بهره برده‌اند. در طرح‌های نام‌برده بین تمام شرکت‌کنندگان وارسی سهم صورت می‌گیرد و تنها روش وارسی متفاوت است و با پیچیده کردن مرحله بازیابی سعی شده است طول سهم‌ها کاهش یابد. Hemenway و Ostrovsky، در رویکردی متفاوت [۱۲] به کمک گراف‌های d–منتظم [۱] تلاش کرده‌اند تا با کاهش تعداد وارسی‌ها سهم کلی هر شرکت‌کننده را کاهش دهند. در این طرح هر شرکت‌کننده به جای وارسی سهم‌های همه شرکت‌کنندگان دیگر، تنها d سهم را وارسی می‌کند و توسط همان d شرکت‌کننده مورد وارسی قرار می‌گیرد. بنا به ادعای نویسندگان، این طرح تنها برای بیشینه تعداد ممکن متقلبان ($t = \lceil \frac{n}{۲} \rceil - ۱$)، دارای طول سهم مناسبی نیست اما به ازای $t = (\frac{۱}{۲} - \varepsilon)n$ که در آن ε مقدار مثبت کوچکی است، نسبت به سایر طرح‌ها طول سهم کمتری دارد. این طرح را در بخش ۳ بررسی خواهیم کرد.

Fehr و Yuan در سال ۲۰۱۹ یک طرح تسهیم راز مقاوم [۱۳] با اندازه سهم $\tilde{\mathcal{O}}(m + \eta n^{\sqrt{\alpha}})$ به ازای مقدار کوچک α پیشنهاد کرده‌اند. این طرح از مدل گرافی برای وارسی سهم‌ها استفاده می‌کند و هر شرکت‌کننده به وارسی تصادفی دو زیرگراف از گراف شرکت‌کنندگان می‌پردازد. در این مقاله، با استفاده از ایده مبتنی بر گراف، به جای وارسی متقابل سهم‌های متناظر با تمامی شرکت‌کنندگان، به دنبال یافتن تعداد کافی وارسی برای دست‌یابی به احتمال خطای موردنظر و طول سهم کوچک هستیم. برای این کار هم‌چنان از وارسی سهم‌ها به کمک کدهای احراز اصالت پیام و بازیابی راز با استفاده از کدهای تصحیح خطا Reed-Solomon استفاده می‌کنیم. اما آنچه طرح پیشنهادی ما را کاراتر می‌کند، مؤثرتر کردن وارسی‌ها و هم‌چنین روش تشخیص متقلب‌ها و حذف آن‌هاست. ما از گراف جهت‌دار d–منتظمی استفاده می‌کنیم که فاقد دور [۲] به طول دو باشد. به این ترتیب امکان تبانی متقابل شرکت‌کنندگان را از میان برمی‌داریم. هم‌چنین با انتخاب بزرگترین زیرگراف از گراف نهایی که رئوس آن ارتباط بیشتری با یکدیگر دارند (دارای کمان‌های بیشتری هستند) و با شرط حاکم بر درجه ورودی هر رأس، که معادل با تعداد تأییدهایی است که برای سهم متناظر دریافت کرده است، احتمال عدم شناسایی متقلب به‌طور معنی‌داری کاهش می‌دهیم. در عین حال، پیچیدگی بازیابی راز را نیز کاهش می‌دهیم. هم‌چنین توانایی‌های قابل توجهی را برای متقلب‌ها در نظر می‌گیریم. در این طرح هر شرکت‌کننده تنها $d < \frac{n}{۲}$ سهم دیگر را وارسی می‌کند. از سوی دیگر ساختار گراف به نحوی است که احتمال خطای بازیابی راز کم است و به این ترتیب به کد احراز اصالت پیام با حداقل طول کلید و برچسب نیاز است، که به کاهش طول سهم منجر می‌شود. بنابراین، با احتمال خطای قابل قبولی، طرح پیشنهادی ما از کارآیی بیشتری نسبت به طرح‌های پیشین برخوردار است.

مهمترین کاربرد تسهیم راز مقاوم، ذخیره‌سازی توزیع شده اطلاعات [۳] مانند ذخیره‌سازی امن در ابر است. این موضوع زمانی اهمیت خود را نشان می‌دهد که با حملات فعالی روبرو هستیم که در آن کارگزاران [۴] ابر عمداً سهم‌های نادرست به بازیابی‌کننده راز ارسال می‌کنند [۱۱]. علاوه بر آن، طرح‌های تسهیم راز مقاوم ارتباط نزدیکی با پروتکل‌های ارسال امن پیام (SMT [۵]) دارد. در این پروتکل‌ها فرستنده و گیرنده به وسیله‌ی n کانال با یکدیگر در ارتباط هستند که t کانال آن در اختیار مهاجمی است که قابلیت تغییر پیام‌های تبادل شده از آن را دارد. اهداف این پروتکل‌ها حفظ حریم خصوصی و مقاوم بودن آن است [۱۱، ۱۲]. بنابراین، از تسهیم راز مقاوم برای پیاده‌سازی این پروتکل نیز می‌توان استفاده کرد. هم‌چنین از روش‌های استفاده شده در طرح‌های تسهیم راز مقاوم می‌توان برای تحقق بخشیدن به تسهیم راز وارسی‌پذیر [۶] و محاسبات امن چند عضوی [۷] استفاده کرد [۷، ۱۱].

۲ پیش‌نیازها

۱.۲ تسهیم راز مقاوم

به طور معمول هر طرح تسهیم راز شامل دو مرحله توزیع سهم‌ها و بازیابی راز است. در مرحله توزیع سهم‌ها توزیع‌کننده D و مجموعه n عضوی از شرکت‌کنندگان $\{P_۱, \ldots, P_n\}$ حضور دارند. در این مرحله D بر اساس مقدار راز انتخاب شده از مجموعه S، یعنی $s \in S$، سهم‌های s_i را به‌ازای $i \in \{۱, \ldots, n\}$ که با $i \in [n]$ نیز آن را نشان می‌دهیم، تولید و به طور امن در اختیار P_iها قرار می‌دهد. هنگام بازیابی راز نیز بازیابی‌کننده راز، R، و شرکت‌کنندگان حضور دارند. در این مرحله هر شرکت‌کننده سهم خود را در اختیار R قرار می‌دهد و R بر اساس سهم‌های دریافتی، راز s' را محاسبه و به عنوان خروجی در اختیار شرکت‌کنندگان قرار می‌دهد، که آن را برابر با s در نظر می‌گیرند. در تسهیم راز مقاوم D و R مورد اعتماد در نظر گرفته می‌شوند و تنها P_iها هستند که ممکن است رفتار خرابکارانه از خود نشان دهند. مهاجم تا قبل از توزیع سهم‌ها و در حین آن غیرفعال است. یک مهاجم عجول می‌تواند مقادیر سهم را پس از مشاهده آنچه شرکت‌کنندگان درستکار برای R می‌فرستند، انتخاب کند. یک مهاجم غیرعجول سهم‌های نادرست را پیش از آغاز مرحله بازیابی راز انتخاب می‌کند [۹].

تعریف ۱ ([۹]). یک طرح تسهیم راز n عضوی را (t, δ)–مقاوم گویند هرگاه به ازای حداکثر t متقلب، پیش از مرحله بازیابی راز هیچ اطلاعاتی در مورد راز به مهاجم نرسد و در پایان مرحله بازیابی راز، بیشینه احتمال خطای بازیابی راز، یعنی $s' \neq s$، برابر با δ باشد.

تعریف ۲ ([۹]). اگر S_i مجموعه تمام سهم‌های ممکن s_i باشد، مقدار $\sigma = \max_i (\log_۲|S_i|) - \log_۲|S|$ را سربار طرح می‌نامند.

هرچقدر سربار یک طرح تسهیم راز مقاوم کمتر باشد کارآیی آن طرح بیشتر است، زیرا سربار مخابراتی کمتری را تحمیل می‌کند.

[1] d-regular [2] cycle [3] distributed information storage

[4] server [5] Secure Message Transmission [6] verifiable secret sharing [7] secure multi party computation

۲.۲ کد احراز اصالت پیام

کدهای احراز اصالت پیام، پیام M را دریافت و تحت یک کلید k، برچسب τ را به عنوان خروجی برمی‌گرداند که برای احراز اصالت پیام مورد استفاده قرار می‌گیرد. برای تسهیم راز مقاوم به کدهای احراز اصالت پیام ساده‌ای نیاز داریم که تنها یک بار استفاده می‌شوند.

تعریف ۳ ([۹]). اگر برای تابع $\text{MAC} : \mathbf{M} \times \mathbf{K} \to \mathbf{T}$، به ازای مجموعه‌های متناهی $\mathbf{M}$، $\mathbf{K}$ و $\mathbf{T}$، رابطه زیر برای تمام $M, \hat{M} \in \mathbf{M}$ و $\tau, \hat{\tau} \in \mathbf{T}$ برقرار باشد، آن را ε-امن[1] می‌گوییم.

$$\Pr\left[\text{MAC}(M,K) = \hat{\tau} | \text{MAC}(M,K) = \tau\right] \leq \varepsilon,$$

که در آن متغیر تصادفی K دارای توزیع یکنواخت روی $\mathbf{K}$ است.

تابع

$$\mathbb{F}^l \times \mathbb{F}^2 \to \mathbb{F},$$
$$((m_1, \ldots, m_l), (k_1, k_2)) \to \sum_{i=1}^{l} m_i k_1^i + k_2$$

در حالت کلی یک کد احراز اصالت پیام با $\varepsilon = l/|\mathbb{F}|$ است که در آن $\mathbb{F}$ میدان محاسبات است [۱۲].

۳.۲ گراف جهت‌دار

هر گراف جهت‌دار $D = (V, A)$ به کمک مجموعه رئوس V و مجموعه کمان‌های[2] A نشان داده می‌شود. در گراف D، به دنباله‌ای یک در میان از رئوس و کمان‌ها که با رئوس آغاز و با کمان پایان می‌پذیرد گام[3] می‌گویند. اگر رأس ابتدایی و انتهایی این گام یکسان باشد آن را دور[4] می‌نامند. اگر $x \in V(D)$ رأسی از گراف D باشد، تعداد کمان‌هایی که از این رأس خارج می‌شود را درجه خروجی می‌نامیم و با $d^+(x)$ نشان می‌دهیم و به طور مشابه تعداد کمان‌هایی که به آن وارد می‌شود را درجه ورودی می‌نامیم و آن را با $d^-(x)$ نشان می‌دهیم. کمینه درجه خروجی و ورودی به ترتیب به صورت زیر تعریف می‌شوند [۱۴]:

$$\delta^+(D) = \min\left\{d^+(x) : x \in V(D)\right\} \quad (۱)$$
$$\delta^-(D) = \min\left\{d^-(x) : x \in V(D)\right\} \quad (۲)$$

همچنین کمینه نیمه‌درجه[5] نیز به صورت زیر تعریف می‌شود:

$$\delta^\circ(D) = \min\left\{\delta^+(D), \delta^-(D)\right\} \quad (۳)$$

برای مقادیر بیشینه نیز به صورت مشابه می‌توان $\Delta^+(D)$، $\Delta^-(D)$ و $\Delta^\circ(D)$ را تعریف کرد.

تعریف ۴ ([۱۴]). اگر برای گراف جهت‌دار D، $\Delta^\circ(D) = \delta^\circ(D) = d$ آنگاه D را d-منتظم می‌گوییم.

ماتریس مجاورت A متناظر با گراف جهت‌دار D به این صورت تعریف می‌شود که اگر کمانی از رأس i به رأس j وجود داشته باشد درایه سطر iاُم و ستون jاُم آن برابر با یک و سایر درایه‌ها برابر با صفر قرار داده می‌شود. این ماتریس توصیفی یکتا از گراف D را به دست می‌دهد.

ما برای ترسیم گراف D از نرم‌افزار MATLAB استفاده می‌کنیم که از الگوریتم ارائه شده در [۱۵] استفاده می‌کند. در این الگوریتم رئوسی که به وسیله یک کمان به یکدیگر متصل هستند نزدیک به هم ترسیم می‌شوند. این الگوریتم به زبان‌های مختلف نرم‌افزاری پیاده‌سازی شده است.

۴.۲ کد تصحیح خطای Reed-Solomon

اگر $C(x) \in \mathbb{F}_p$ چندجمله‌ای با بیشینه درجه t باشد و $i_1, \ldots, i_n$ عناصر متمایز $\mathbb{F}_p$ باشند، در این صورت $(C(i_1), \ldots, C(i_n))$ کلمه‌کدهای کد Reed-Solomon را تشکیل می‌دهند که دارای کمینه فاصله همینگ $n - t$ است. بنابراین، هنگامی که $t < \frac{n}{3}$ باشد، این کد با احتمال یک می‌تواند تا t خطا را تصحیح کند. پس این طرح قابلیت شناسایی متقلب‌ها را تا تعداد $\frac{n-1}{3}$ داراست [۱۰].

۳ بررسی طرح Hemenway و Ostrovsky

در این طرح با در نظر گرفتن شرکت‌کنندگان به عنوان رئوس گراف d-منتظم G، ماتریس مجاورت A تشکیل شده است که با تقسیم درایه‌های آن به d، A' به دست می‌آید. اگر مقادیر ویژه این ماتریس محاسبه و اندازه آن‌ها به ترتیب نزولی مرتب شوند، بزرگترین مقدار برابر با یک خواهد بود و مقدار بعدی را با λ نشان می‌دهیم. ادعا شده است این طرح به ازای مقادیر کوچک ε با وجود $t = (\frac{1}{2} - \varepsilon)n$ متقلب مقاوم است. به ازای هر رأس $i \in [n]$ مجموعه همسایه‌های آن به صورت $\Gamma(i)$ نشان داده می‌شود. مرحله توزیع سهم‌ها در این طرح به این صورت است [۱۲]:

(۱) تولید سهم‌های s_i برای راز s به ازای هر $i \in [n]$ با طرح تسهیم راز $(\frac{2}{3}\varepsilon_\circ n, \circ)$-مقاوم

(۲) تولید برچسب‌های $\tau_{ij} = \text{MAC}(k_{ij}, s_j)$ برای هر $i \in [n]$ و $j \in \Gamma(i)$

(۳) ارسال s_i و $\{k_{ij}, \tau_{ji}\}_{j \in \Gamma(i)}$ به عنوان سهم هر شرکت‌کننده

بازیابی راز نیز با داشتن $\{s_i, \{k_{ij}, \tau_{ji}\}_{j \in \Gamma(i)}\}_i$ به صورت زیر انجام می‌شود [۱۲]:

(۱) مقداردهی اولیه گراف $G = \emptyset$

(۲) برای هر $i \in [n]$ اگر

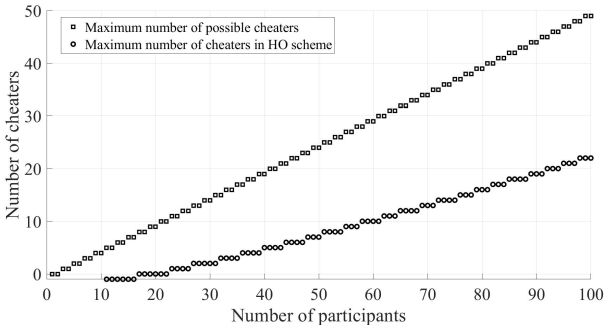
$$|\{j = \text{MAC}(k_{ij}, s_j) = \tau_{ij}\}| > \frac{d}{2}$$

در این صورت $G = G \cup \{i\}$

(۳) اعمال الگوریتم بازیابی راز طرح تسهیم راز $(\frac{2}{3}\varepsilon_\circ n, \circ)$-مقاوم برای سهم‌های G

Hemenway و Ostrovsky ثابت کرده‌اند برای آن که طرح آنان مقاوم باشد باید شرط زیر برقرار باشد:

[1] ε-secure [2] arc [3] walk [4] cycle [5] semi-degree



شکل ۱. مقایسه بیشینه تعداد متقلب در طرح Hemenway و Ostrovsky با کران بالای تعداد ممکن متقلب

$$\lambda < \sqrt{\frac{\varepsilon^{۳}\varepsilon_{۰}}{(\frac{۱}{۲}-\varepsilon)(۱-\varepsilon_{۰})}} \qquad (۴)$$

سپس از آن جایی $\lambda < ۲/\sqrt{d}$، لذا در نهایت درجه رأسی گراف G باید در شرط زیر صدق کند:

$$d > \frac{۴(\frac{۱}{۲}-\varepsilon)(۱-\varepsilon_{۰})}{\varepsilon^{۳}\varepsilon_{۰}} \qquad (۵)$$

و در نهایت با در نظر گرفتن مقدار حدی $\varepsilon_{۰} = \frac{۱}{۲}$ به شرط نهایی زیر برای داشتن طرح تسهیم راز مقاوم می‌رسند:

$$d > \frac{۴(\frac{۱}{۲}-\varepsilon)}{\varepsilon^{۳}} \qquad (۶)$$

و نتیجه می‌گیرند که کافی است $d > ۲/\varepsilon^{۳}$ [۱۲]. اما نویسندگان از این نکته بدیهی غافل شده‌اند که باید $d < n$، زیرا d درجه رأسی گراف است و نمی‌تواند از $n-۱$ تجاوز کند. به این ترتیب، با به‌دست آوردن ε از رابطه $t = (\frac{۱}{۲}-\varepsilon)n$ و جایگذاری آن در شرط فوق داریم:

$$n-۱ \geq d > \frac{۲}{\varepsilon^{۳}} \Rightarrow n-۱ > \frac{۲}{(\frac{۱}{۲}-\frac{t}{n})^{۳}}$$
$$\Rightarrow t \leq n\left(\frac{۱}{۲} - \sqrt[۳]{\frac{۲}{n-۱}}\right) \qquad (۷)$$

پس بیشینه تعداد متقلب‌ها که با حضور آنان این طرح همچنان قابلیت بازیابی راز را دارد برابر خواهد بود با:

$$t = \left\lfloor n\left(\frac{۱}{۲} - \sqrt[۳]{\frac{۲}{n-۱}}\right)\right\rfloor \qquad (۸)$$

با مقایسه این تعداد با حد بالای تعداد متقلب‌ها در شکل ۱ واضح است که مقدار ε کوچک نیست و این طرح در حضور تعداد زیاد متقلب‌ها دچار مشکل است.

۴ طرح پیشنهادی

در بخش ۳ مشاهده کردیم که طرح Hemenway و Ostrovsky نمی‌تواند اهداف یک طرح تسهیم راز مقاوم را برآورده سازد. اما همچنان ایده کاهش تعداد وارسی‌های هر شرکت‌کننده می‌تواند مورد توجه باشد. ما نیز با بهره‌گیری از همین ایده و با تغییراتی که در مدل نویسندگان ایجاد می‌کنیم و همچنین استفاده از شیوه متفاوتی برای محاسبه خطا طرح تسهیم راز مقاومی با احتمال خطای ناچیز و طول سهم کوتاهتر ارائه می‌دهیم.

در طرح پیشنهادی از مدل گراف جهت‌دار d-منتظم برای وارسی سهم‌ها استفاده می‌کنیم که فاقد دوری به طول دو باشد. به این ترتیب امکان تبانی متقابل بین شرکت‌کنندگان از بین می‌رود. در این مدل، هر کمان نشان‌دهنده یک عمل وارسی است. رأسی که کمانی از آن خارج شده، سهم رأسی را که کمان به آن وارد شده است وارسی می‌کند. واضح است که گراف مورد نظر باید فاقد حلقه روی هر رأس نیز باشد.

۱.۴ الگوریتم پیشنهادی تسهیم راز مقاوم

طرح پیشنهادی همانند سایر طرح‌ها شامل دو مرحله توزیع سهم‌ها و بازیابی راز است. برای توزیع سهم‌ها عملیات زیر انجام می‌شود:

(۱) تولید گراف n رأسی جهت‌دار d-منتظم D با ویژگی‌های بیان‌شده که درجه ورودی و خروجی هر رأس آن $d = \lfloor \frac{n-۱}{۲} \rfloor$ است.

(۲) نگاشت تصادفی هر یک از رئوس به هر یک از شرکت‌کنندگان

(۳) تولید سهم‌های s_i برای راز s به ازای هر $i \in [n]$ به کمک تسهیم راز آستانه‌ای شامیر با آستانه t' که $t' = \lceil \frac{n+۳}{۴} \rceil$

(۴) انتخاب کلیدهای کدهای احراز اصالت $k_{ij} \in \mathbb{F}_q^{۲}$ برای وارسی سهم P_j توسط P_i و تولید برچسب‌های $\tau_{ij} = \mathrm{MAC}(k_{ij}, s_j)$ برای هر $i \in [n]$ و $j \in \Gamma^{-}(i)$ که در آن $\Gamma^{-}(i)$ مجموعه تمام رئوسی از D است که از رأس i کمانی به آن وارد شده است.

(۵) ارسال امن سهم‌های s_i و $\{k_{ij}, \tau_{ji}\}_{j\in\Gamma^{-}(i)}$ به P_iها.

برای بازیابی راز، عملیات زیر با استفاده از $\{s_i, \{k_{ij}, \tau_{ji}\}_{j\in\Gamma^{-}(i)}\}_i$ توسط بازیابی کننده انجام می‌گیرد:

(۱) وارسی تمامی سهم‌ها به کمک برچسب‌های داده شده به هر شرکت‌کننده بر اساس کمان‌های گراف D و حذف کمان‌هایی از گراف D که در وارسی رد می‌شوند.

(۲) رسم گراف D حاصل‌شده و انتخاب بزرگترین مجموعه از رئوس که دارای ارتباط بیشتری با یکدیگر هستند.

(۳) حذف رئوسی از مجموعه انتخاب‌شده که $d^{-}(x) < d_{\Lambda}$ به ازای $d_{\Lambda} \geq ۲$.

(۴) بازیابی راز به کمک سهم‌های متناظر با اعضای باقیمانده در مجموعه و با استفاده از کد تصحیح خطای Reed-Solomon

مجموعه‌ای را، که از سهم‌های اعضای آن برای بازیابی نهایی راز استفاده می‌شود، مجموعه نهایی قابل قبول می‌نامیم و با Λ نشان می‌دهیم.

۲.۴ مدل متقلب

متقلب‌ها سعی دارند که عضو مجموعه Λ شوند تا بازیابی راز را با مشکل مواجه سازند. از این پس، مجموعه شرکت‌کنندگانی که سهم‌های خود را به درستی ارائه می‌کنند و تلاشی برای فریب سایر شرکت‌کنندگان ندارند،

مجموعه درستکارها می‌نامیم و آن را با H نشان می‌دهیم. همچنین، مجموعه‌ای را که در تلاش برای گرفتن تأیید از سایر شرکت‌کنندگان برای سهم‌های نادرست خود هستند متقلب می‌نامیم و با T نمایش می‌دهیم. بر اساس الگوریتم فوق، اگر $t_i \in T$ متقلب دلخواهی باشد، برای آن‌که t_i بتواند وارد Λ شود اعضای T به صورت زیر عمل می‌کنند:

- متقلب t_i سعی می‌کند با وجود ارائه سهم نادرست، تأیید اعضای H را جلب کند تا به آن نزدیک شود که این کار را فریب می‌نامیم.
- در صورتی که t_i بتواند عضو $h_j \in H$ را فریب دهد، تمام اعضای T که وظیفه وارسی سهم h_j را دارند، سهم او را تأیید می‌کنند تا با بیشتر شدن ارتباط بین h_j و T بتوانند h_j را به خود نزدیک و از Λ خارج کنند.
- متقلب t_i که موفق به فریب حداقل یک عضو درستکار شده باشد سایر متقلب‌ها را که موفق به این کار نشده‌اند تأیید نمی‌کند تا از T فاصله بگیرد و به H نزدیکتر شود.
- از آن‌جایی که درجه ورودی t_i باید حداقل d_Λ باشد، نیازمند گرفتن تأییدهایی از سوی متقلب‌هاست و به این ترتیب سایر اعضای T به تأیید t_i می‌پردازند تا درجه‌ی ورودی آن به d_Λ برسد.
- به ازای تمامی اعضای T عملیات فوق تکرار می‌شود.

پس متقلب‌ها در طرح پیشنهادی از توانایی بالایی برخوردارند و از نوع عجول به حساب می‌آیند.

۳.۴ محاسبه خطای طرح

برای آن‌که بتوانیم احتمال خطای طرح را مشخص کنیم لازم است برخی نمادگذاری‌ها را انجام دهیم تا در نهایت احتمال خطای بازیابی راز را مشخص کنیم. به این منظور، متقلب دلخواه t_i را در نظر می‌گیریم و نتایج را به سایر متقلب‌ها تعمیم می‌دهیم. به ازای n شرکت‌کننده درجه رأسی گراف را $d = \lfloor \frac{n-1}{2} \rfloor$ در نظر می‌گیریم.

اگر فرض کنیم طرح پیشنهادی در برابر بیشینه تعداد ممکن متقلب، مقاوم است در این صورت در طرحی با n شرکت‌کننده، $t = \lfloor \frac{n-1}{2} \rfloor$ متقلب خواهیم داشت. تعداد کمان‌های مربوط به گراف جهت‌دار d-منتظم D که از t_i به H می‌رود را با a و تعداد کمان‌های اولیه از H به t_i را نیز با b نشان می‌دهیم. اگر $T' = T \backslash \{t_i\}$، در این صورت تعداد کمان‌ها از t_i به T' برابر با $d-a$ و تعداد کمان‌ها از T' به t_i برابر با $d-b$ خواهد بود.

چون $|T'| = t - 1 = \lfloor \frac{n-3}{2} \rfloor$ پس کمینه مجموع تعداد کمان‌ها بین H و t_i، یعنی $a+b$، از رابطه زیر به دست می‌آید:

$$2d - |T'| = 2\left\lfloor \frac{n-1}{2} \right\rfloor - \left\lfloor \frac{n-3}{2} \right\rfloor = \left\lfloor \frac{n+1}{2} \right\rfloor = d+1 \quad (9)$$

به این ترتیب کران پایین تعداد این کمان‌ها به‌صورت زیر است:

$$a+b \geq d+1 \quad (10)$$

با استدلال مشابه، کران بالای تعداد کمان‌ها نیز به تعداد اعضای H است:

$$a+b \leq n-t = n-d \quad (11)$$

برای آن‌که متقلب t_i بتواند به مجموعه Λ وارد شود باید حداقل یک عضو از H را فریب دهد. اگر تعداد اعضایی از H را که t_i آن‌ها را فریب داده است با c نمایش دهیم، باید داشته باشیم: $1 \leq c \leq b$. بنابراین باید $b \geq 1$.

در نخستین گام برای آن‌که t_i در Λ قرار گیرد لازم است ارتباط t_i با H، حداقل برابر با ارتباط آن با T' باشد. پس از آن، t_i باید شرط حداقل درجه ورودی d_Λ را نیز داشته باشد تا در Λ قرار گیرد. از این‌رو، اگر تعداد تأییدهایی را که t_i از T' دریافت می‌کند f بنامیم، آن‌گاه

$$c+f \geq d_\Lambda \quad (12)$$

که در رابطه (۱۲) پارامتر f نمی‌تواند از تعداد کل کمان‌هایی که از T' به t_i وارد می‌شود، بیشتر باشد، یعنی

$$f \leq d-b \quad (13)$$

در این طرح احتمال فریب برابر با احتمال موفقیت متقلب به منظور دریافت یک تأیید برای سهم نادرست خود است که همان احتمال خطای کد احراز اصالت پیام در نظر گرفته می‌شود. معمولا لازم است این احتمال مقدار ناچیزی باشد، بنابراین، برای متقلب‌ها حالت مطلوب حالتی است که تنها با یک فریب بتوانند به مجموعه Λ راه یابند، پس می‌توان از احتمال $c > 1$ در محاسبه خطا چشم‌پوشی کرد. با قرار دادن $c = 1$ در (۱۲) داریم:

$$d_\Lambda - 1 \leq f \quad (14)$$

بدین ترتیب، کافی است که متقلب به تعداد $f = d_\Lambda - 1$ تأیید از T' دریافت کند. با جایگذاری f در (۱۳) داریم:

$$b \leq d - d_\Lambda + 1 \quad (15)$$

از سوی دیگر، اگر تعداد کمان‌های خروجی از t_i به سایر متقلب‌هایی که موفق به فریب عضوی از H شده‌اند را با e نمایش دهیم، در این صورت $0 \leq e \leq d-a$ و برای برقراری شرط ارتباط بیشتر با H باید داشته باشیم:

$$c+a \geq f+e \quad (16)$$

که با قرار دادن $c = 1$ و $f = d_\Lambda - 1$ به نامساوی زیر تبدیل می‌شود:

$$a \geq d_\Lambda - 2 + e \quad (17)$$

بنابراین، چهار شرط (۱۰)، (۱۱)، (۱۵) و (۱۷) باید به‌طور هم‌زمان برقرار باشند تا t_i به Λ راه یابد. پس برای محاسبه احتمال خطای بازیابی راز، تمام حالت‌های مختلف a و b را، که در شروط چهارگانه فوق صدق می‌کنند به همراه احتمال هر یک از آن‌ها در نظر می‌گیریم. با

ضرب مجموع این احتمال‌ها در احتمال خطای کد احراز اصالت، احتمال $P_\Lambda(t_i)$ به دست می‌آید که آن را احتمال موفقیت t_i برای حضور در Λ می‌نامیم. چون $|T'|=\lfloor\frac{n-۳}{۲}\rfloor$ پس کمینه مقدار a و b برابر با یک است. در این محاسبات برای اولین متقلب، $t_۱$، قرار می‌دهیم $e=۰$ و برای سایر متقلب‌ها، بسته به وجود کمان بین متقلب جدید و متقلب‌های پیشین مقدار e را مشخص می‌کنیم. مثلا برای متقلب $t_۲$ با احتمال $\frac{d}{n-۱}$، $e=۱$ است.

اکنون، توزیع احتمال a و b را به دست می‌آوریم. از آن‌جایی که پیش از اجرای بازیابی راز نمی‌دانیم کدام شرکت‌کننده درستکار و کدام یک متقلب هستند، با انتخاب تصادفی یکی از رئوس به عنوان متقلب t_i به دنبال تعداد کمان‌های بین این رأس و مجموعه تصادفی $n-t$ عضوی به عنوان درستکارها هستیم. در واقع از $n-۱$ رأس دیگر گراف، $n-t$ رأس را انتخاب کرده‌ایم و می‌خواهیم بدانیم احتمال آن که a رأس از این مجموعه دارای کمانی از t_i یا b رأس از آن دارای کمانی به t_i باشد، چقدر است. این احتمال از توزیع فوق هندسی پیروی می‌کند:

$$P(b=i)=P(a=i)==\frac{\binom{d}{i}\binom{(n-۱)-d}{(n-t)-i}}{\binom{n-۱}{n-t}} \qquad (۱۸)$$

برای آن‌که متقلب‌ها مانع بازیابی درست راز شوند، لازم است $\frac{(n-t)}{۲}$ متقلب به مجموعه Λ راه یابند. پس احتمال موفقیت متقلب‌ها برای بازیابی نادرست راز با حضور در Λ، که آن را احتمال خطای حالت اول $\delta_۱$ می‌نامیم، از رابطه زیر به‌دست می‌آید:

$$\delta_۱=\prod_{i=۱}^{\frac{(n-t)}{۲}} P_\Lambda(t_i) \qquad (۱۹)$$

اما برای آن‌که راز به درستی بازیابی نشود امکان دیگری نیز وجود دارد که آن را با احتمال خطای حالت دوم $\delta_۲$ نشان می‌دهیم. امکان دارد تعدادی از رئوس درستکار به دلیل دارا نبودن حداقل درجه ورودی حذف شوند، به نحوی که تعداد درستکارهای باقی‌مانده از آستانه t' کمتر شود. احتمال این رخداد همان $\delta_۲$ است.

با فرض $h_j\in H$ و $H'=H\backslash\{h_j\}$، اگر تعداد کمان‌های خروجی از h_j به H' را با a' و تعداد کمان‌های ورودی به h_j از H' را با b' نشان دهیم، h_j زمانی از Λ حذف می‌شود که اولا داشته باشیم: $b'<d_\Lambda$ و ثانیا فریب نخورده باشد، زیرا در این صورت متقلب‌ها به تأیید h_j می‌پردازند. بنابراین، احتمال آنکه h_j در Λ نباشد برابر است با

$$P_{\Lambda'}(h_j)=[۱-(d-a')\varepsilon]\,P(b'<d_\Lambda) \qquad (۲۰)$$

که در آن ε احتمال خطای کد احراز اصالت پیام است. بیشینه مقدار این احتمال برای $h_۱$، به ازای $a'=d$ به‌دست می‌آید و برای $h_۲$ بیشینه مقدار a' که به بیشینه احتمال عدم حضور آن در Λ می‌انجامد برابر است با $a'=d-۱$. پس، احتمال آنکه h_j در Λ نباشد برابر است با

$$P_{\Lambda'}(h_j)=[۱-(j-۱)\varepsilon]\,P(b'<d_\Lambda) \qquad (۲۱)$$

به این ترتیب، احتمال خطای حالت دوم برابر است با

$$\delta_۲=\prod_{j=۱}^{n-t-(t'-۱)} P_{\Lambda'}(h_j) \qquad (۲۲)$$

گزاره ۱. هیچ درستکاری با اعمال شرط ارتباط بیشتر با متقلب‌ها از مجموعه Λ حذف نمی‌شود.

اثبات. با فرض $h_j\in H$ برای آن که h_j با شرط ارتباط بیشتر با متقلب‌ها حذف شود باید ارتباط آن با مجموعه متقلب‌ها، T، بیشتر از ارتباط آن با مجموعه H' باشد، یعنی

$$c+(d-b')>a'+b' \qquad (۲۳)$$

که در آن

$$۱\le c\le d-a' \qquad (۲۴)$$

از طرفی نیز تعداد کل کمان‌ها بین h_j و T نمی‌تواند از $|T|=t=d$ بیشتر باشد. پس

$$(d-a')+(d-b')\le d \qquad (۲۵)$$

$$a'+b'\ge d \qquad (۲۶)$$

با جایگذاری کران پایین $a'+b'=d$ در (۲۳) داریم

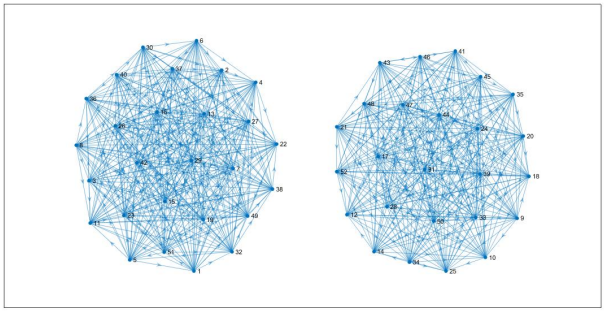
$$c>b' \qquad (۲۷)$$

که با جایگذاری $b'=d-a'$ در رابطه (۲۷) با رابطه (۲۳) در تناقض است. پس هیچ درستکاری با شرط ارتباط بیشتر با متقلب‌ها حذف نمی‌شود. □

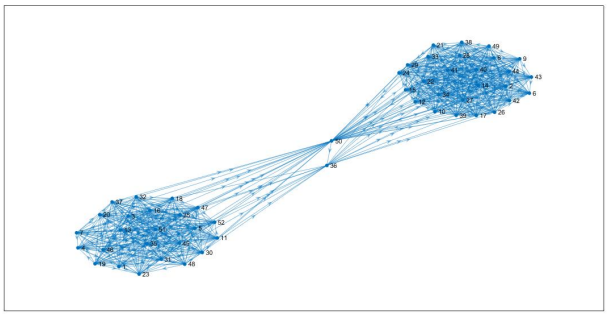
احتمال خطای کل طرح $\delta=۲^{-\eta}=\delta_۱+\delta_۲$ است. پس، لازم است این دو خطا تا حد امکان به یک‌دیگر نزدیک باشند که این امر با حداقل درجه‌ی ورودی d_Λ قابل کنترل است. با توجه به این‌که خطای کد احراز اصالت پیام مقدار ناچیز ε است، بنابراین احتمال فریب دو درستکار توسط یک متقلب تقریبا برابر با صفر است لذا قرار می‌دهیم $d_\Lambda=۲$. نتایج به دست آمده در بخش ۴.۴ نیز بر این اساس است.

۴.۴ مقایسه با سایر طرح‌ها

همان‌گونه که در الگوریتم بازیابی راز طرح پیشنهادی در بخش ۱.۴ بیان شد، پس از رسم گراف نهایی با انتخاب بزرگترین مجموعه از رئوس که ارتباط بیشتری با هم دارند متقلب‌ها را حذف می‌کنیم. این تمایز بین درستکارها و متقلب‌ها پس از رسم گراف به سادگی ممکن است. برای مثال شکل ۲ گراف نهایی طرحی شامل ۵۲ شرکت‌کننده با ۲۵ متقلب است. رئوس به وضوح به دو دسته تفکیک شده‌اند که هر یک مجموعه درستکارها و متقلب‌ها را نشان می‌دهد. مجموعه‌ای که تعداد رئوس کمتری دارد نشان‌دهنده مجموعه متقلب‌ها است. بنابراین شناسایی و حذف متقلب‌ها در این طرح به سادگی امکان‌پذیر است و بر خلاف سایر طرح‌ها نیازی به انجام محاسبات پیچیده نیست. بنابراین، بازیابی راز



شکل ۲. گراف نهایی تسهیم راز میان ۵۲ شرکت‌کننده با ۲۵ متقلب با کمترین احتمال خطا. زیرگراف سمت راست متقلب‌ها هستند.



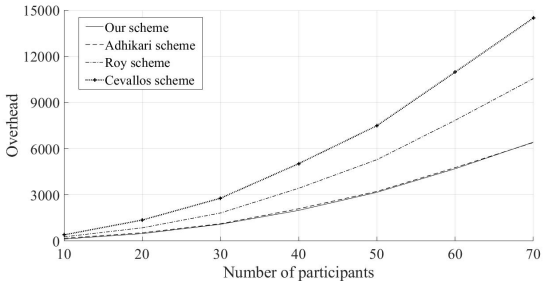
شکل ۳. گراف نهایی تسهیم راز میان ۵۲ شرکت‌کننده با ۲۵ متقلب با سربار کمتر. زیرگراف سمت راست درستکارها هستند.

ساده‌تر و سریعتر از سایر طرح‌ها انجام می‌شود و از این نظر کارآیی بیشتری دارد. در این مثال راز $s \in_R \mathbb{F}_q^m$ به ازای $m = ۲۵۶$ تسهیم شده است که با سربار $\sigma = ۲۴۰۰$ بیت به احتمال خطای $۲^{-۳۵۸۸۸۹۲}$ منجر می‌شود. با استفاده از کد احراز اصالت پیام با احتمال خطای بیشتر، سربار طرح تسهیم راز به $\sigma = ۱۲۰۰$ می‌رسد که شکل ۳ بیانگر گراف نهایی برای این حالت است. شناسایی متقلب‌ها همچنان در این حالت ساده است. دو رأس میانی موفق به فریب شده‌اند اما نتوانسته‌اند خود را درستکار جا بزنند. احتمال خطا در این حالت $۲^{-۱۳۴۸۸۹۲}$ است.

مجموعه $\{s_i, \{k_{ij}, \tau_{ji}\}_{j\in\Gamma^-(i)}\}$ سهم هر شرکت‌کننده در طرح پیشنهادی است. بنا به آن‌چه در بخش ۲.۲ بیان شد، برای پیام $M \in \mathbb{F}_q^m$، کد احراز اصالتی با خطای $\varepsilon = \frac{m}{q}$ خواهیم داشت. با قرار دادن $q = ۲^p$، سربار طرح بر اساس تعریف ۲ به دست می‌آید:

$$\sigma = d\,(|\mathbf{K}|+|\mathbf{T}|) = ۳d\log_۲ q = ۳dp \qquad (۲۸)$$

به منظور مقایسه سربار طرح‌ها، از آن‌جایی که در طرح پیشنهادی احتمال خطا در مدل گراف جهت‌دار محاسبه شده است و متفاوت از طرح‌های پیشین است، انجام مقایسه به صورت پارامتری بین طرح پیشنهادی و سایر طرح‌ها امکان‌پذیر نیست. از این‌رو، در شکل ۴ سربار طرح پیشنهادی به ازای یک راز به طول $m = ۲۵۶$ بیت با طرح‌های موجودی که دارای کمترین سربار هستند، مقایسه شده است. در این طرح‌ها احتمال خطا برابر با $\delta = ۲^{-\eta}$ است، که مقادیر η برای تعداد شرکت‌کنندگان مختلف در جدول ۱ داده شده است. همان‌طور که در شکل ۴ مشاهده می‌کنیم، طرح پیشنهادی دارای سربار کمتری نسبت به



شکل ۴. مقایسه سربار طرح پیشنهادی با سایر طرح‌های موجود

جدول ۱. مقدار η برای تعداد شرکت‌کنندگان مختلف

n	۱۰	۲۰	۳۰	۴۰	۵۰	۶۰	۷۰
η	۷٫۳۱	۵۸٫۹۷	۱۴۵٫۷۱	۳۰۰٫۷۴	۴۷۴٫۹۸	۷۳۴٫۱۷	۹۹۵٫۹۶

سایر طرح‌هاست که این موضوع به ازای رازهایی به طول‌های مختلف نیز صادق است. هم‌چنین، از آن‌جایی که در طرح Fehr و Yuan [۱۳] مقدار دقیق طول سهم مشخص نشده است، با طرح پیشنهادی در این مقاله قابل مقایسه نیست. اما همان‌طور که در ادامه نشان می‌دهیم، به نظر می‌رسد این طرح در مقایسه با طرح Adhikari و همکارانش سربار بیشتری داشته باشد و به این ترتیب طرح پیشنهادی از طرح [۱۳] نیز سربار کمتری خواهد داشت. برای این کار طول سهم را در طرح [۱۰] که از رابطه (۲۹) به دست می‌آید، با جایگذاری مقدار t بر حسب n به صورت رابطه (۳۰) بازنویسی می‌کنیم. در این رابطه، N درجه چندجمله‌ای تابع چکیده‌ساز مورد استفاده و مقدار e نیز عدد نپر است.

$$|s_i| = m + (۲n - t - ۱)\left(\log(n-t) + \log(N) + \frac{۲}{n-t}(\eta + \log(e))\right) \qquad (۲۹)$$

$$|s_i| = m + \mathcal{O}(n\log n + \eta) = m + \tilde{\mathcal{O}}(n+\eta) \qquad (۳۰)$$

رابطه (۳۰) با توجه به تساوی $\mathcal{O}(N) = \mathcal{O}(n)$ نوشته شده است. از طرفی طول سهم طرح Fehr و Yuan، از مرتبه $|s_i| = \tilde{\mathcal{O}}(m+\eta n^{\sqrt{\alpha}})$ است، به نظر می‌رسد با انتخاب مقادیر بسیار کوچک α پیچیدگی بازیابی راز در طرح نام‌برده، که از مرتبه $poly\left(\eta, m, n, \left(\frac{۱}{\alpha}\right)^{\tilde{\mathcal{O}}(\frac{۱}{\alpha})}\right)$ است [۱۳]، به صورت نمایی درمی‌آید. بنابراین، مقدار α را نمی‌توان به حدی کوچک انتخاب کرد که طول سهم متناظر با آن کمتر از طول سهم در طرح [۱۰] باشد.

با توجه به این مقایسه‌های انجام شده، تحت شرایط یکسان، طرح پیشنهادی نسبت به سایر طرح‌ها علاوه بر سادگی بازیابی درست راز دارای سربار کمتر و کارآیی بیشتری است.

۵ نتیجه‌گیری

در این مقاله یک طرح تسهیم راز مقاوم در حضور بیشینه تعداد ممکن متقلب مبتنی بر مدل گراف جهت‌دار ارائه شده است، که شناسایی و حذف

متقلب‌ها را به سادگی با مشاهده گراف نهایی طرح فراهم می‌آورد. به این ترتیب، بنا بر اطلاعات ما تاکنون، بازیابی صحیح راز بسیار ساده‌تر از طرح‌های موجود انجام پذیر است و دیگر نیازی به محاسبات پیچیده برای بازیابی درست راز وجود ندارد. هم‌چنین این طرح امکان بازیابی درست راز را با طول سهم‌های کوتاهتری نسبت به طرح‌های موجود فراهم کرده است که سربار مخابراتی طرح را کاهش می‌دهد. پس طرح پیشنهادی در شرایط یکسان دارای کارآیی بهتر از هردو جنبه پیچیدگی محاسباتی بازیابی راز و سربار طرح است.

سپاسگزاری

این پژوهش از حمایت مالی صندوق حمایت از پژوهشگران طبق قرارداد شماره ۵۳۹۷۹/ص/۹۶ بهره‌مند شده است که بدین وسیله از حمایت آن صندوق تشکر می‌شود. همچنین، از راهنمایی آقای دکتر کسری علیشاهی تشکر و قدردانی به عمل می‌آید.

مراجع

[1] Martin Tompa and Heather Woll. How to share a secret with cheaters. *journal of Cryptology*, 1(3):133–138, 1989.

[2] Robert J. McEliece and Dilip V. Sarwate. On sharing secrets and reed-solomon codes. *Communications of the ACM*, 24(9):583–584, 1981.

[3] Marco Carpentieri, Alfredo De Santis, and Ugo Vaccaro. Size of shares and probability of cheating in threshold schemes. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 118–125. Springer, 1993.

[4] Wakaha Ogata, Kaoru Kurosawa, and Douglas R Stinson. Optimum secret sharing scheme secure against cheating. *SIAM Journal on Discrete Mathematics*, 20(1):79–95, 2006.

[5] Carlo Blundo and Alfredo De Santis. Lower bounds for robust secret sharing schemes. *Information Processing Letters*, 63(6):317–321, 1997.

[6] Ronald Cramer, Ivan Damgård, and Serge Fehr. On the cost of reconstructing a secret, or vss with optimal reconstruction phase. In *Annual International Cryptology Conference*, pages 503–523. Springer, 2001.

[7] Tal Rabin and Michael Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 73–85, 1989.

[8] Mahabir Prasad Jhanwar and Reihaneh Safavi-Naini. Unconditionally-secure robust secret sharing with minimum share size. In *International conference on financial cryptography and data security*, pages 96–110. Springer, 2013.

[9] Alfonso Cevallos, Serge Fehr, Rafail Ostrovsky, and Yuval Rabani. Unconditionally-secure robust secret sharing with compact shares. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 195–208. Springer, 2012.

[10] Avishek Adhikari, Kirill Morozov, Satoshi Obana, Partha Sarathi Roy, Kouichi Sakurai, and Rui Xu. Efficient threshold secret sharing schemes secure against rushing cheaters. In *International Conference on Information Theoretic Security*, pages 3–23. Springer, 2016.

[11] Partha Sarathi Roy, Avishek Adhikari, Rui Xu, Kirill Morozov, and Kouichi Sakurai. An efficient robust secret sharing scheme with optimal cheater resiliency. In *International Conference on Security, Privacy, and Applied Cryptography Engineering*, pages 47–58. Springer, 2014.

[12] Brett Hemenway and Rafail Ostrovsky. Efficient robust secret sharing from expander graphs. *Cryptography and Communications*, 10(1):79–99, 2018.

[13] Serge Fehr and Chen Yuan. Towards optimal robust secret sharing with security against a rushing adversary. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 472–499. Springer, 2019.

[14] Jørgen Bang-Jensen and Gregory Z Gutin. *Digraphs: theory, algorithms and applications*. Springer Science & Business Media, 2008.

[15] Thomas MJ Fruchterman and Edward M Reingold. Graph drawing by force-directed placement. *Software: Practice and experience*, 21(11):1129–1164, 1991.