۱۳۶۵
دانشگاه جامع امام حسین(ع)
دانشکده و پژوهشکده فنی و مهندسی

مجله علمی-پژوهشی «علوم و فناوری‌های پدافند غیرعامل»
سال اول، شماره ۲، زمستان ۱۳۸۹: ص ۱۲-۵

Available online:
www.adst.ir

تشخیص و تصحیح تقلب در طرح‌های تسهیم محرمانه با استفاده از کدهای سه‌سه‌یی

زین‌العابدین نوروزی[۱*]، ابراهیم محمدی[۲]

۱- مربی، ۲- کارشناس ارشد، دانشگاه جامع امام حسین(ع)، دانشکده فناوری اطلاعات و ارتباطات، گروه ریاضی و رمز
E-mail: znorozi@ihu.ac.ir

(دریافت ۱۳۸۹/۲/۱۰ ، پذیرش ۱۳۸۹/۸/۱۷)

چکیده

طرح‌های تسهیم محرمانه در مدیریت کلید رمزنگاری و سیستم‌های امن چندگانه بسیار مورد استفاده قرار می‌گیرند. طرح‌های تسهیم روش‌هایی هستند که در آنها یک کلید محرمانه به عنوان راز بین شرکاء طوری تسهیم می‌گردد که فقط زیرمجموعه‌های مجاز قادر به بازسازی کلید محرمانه بوده و افراد غیرمجاز قادر به بازسازی راز نیستند. مجموعه همه زیرمجموعه‌های مجاز را ساختار دسترسی طرح گوییم. ساختارهای گوناگونی از طرح‌های تسهیم محرمانه وجود دارند که یکی ازآن‌ها بر مبنای تئوری کدینگ است. در اصل هر کد خطی می‌تواند به عنوان ساختار یک طرح تسهیم محرمانه مورد استفاده قرار گیرد. یکی از مسائل مهم در طرح‌های تسهیم محرمانه، تشخیص و تصحیح متقلب می‌باشد. در این مقاله با ارائه دو فرضیه جدید چگونگی تشخیص و تصحیح متقلبین را مورد بررسی قرار داده و به نتایج مطلوبی دست یافتیم.

کلیدواژه‌ها: طرح‌های تسهیم محرمانه؛ کدهای سه‌سه‌یی؛ تقلب؛ ساختار دسترسی؛ ساختار دسترسی مینیمال

Detection and Correction of Cheat in the Secret Sharing Schemes with Ternary Codes

Z. Noroozi*, E. Mohamady
Faculty and Research Center of Communication and Information Technology, Imam Hossein University
E-mail: znorozi@ihu.ac.ir

Abstract

Secret sharing schemes are useful in the management of cryptographic keys and in multiparty secure protocols. A secret sharing scheme permits a secret to be shared among participants in such a way that only authorized subsets of participants can recover the secret, but any unauthorized has absolutely no information on the secret. The set of all authorized subset defines the access structure to the secret. There are several approaches to the construction of secret sharing schemes. One of them is based on coding theory. It is to note that every linear code can be used to construct secret sharing schemes. On of the important problems of the secret sharing schemes is detection and correction of cheat. In this paper we present two hypotheses for detection and correction of cheat.

Keywords: Secret Sharing Schemes; Ternary Codes; Cheating; Minimal Access Structure

۱. مقدمه

طرح‌های تسهیم محرمانه در سیستم‌هایی که به‌صورت شبکه‌ای عمل می‌کنند نقش مهمی ایفاء می‌نمایند. در علومی مانند پدافند نوین که نیاز به رعایت سلسله مراتب با وزن‌های متفاوت هستیم، این طرح‌ها بسیار مفید و کارا هستند. در طرح تسهیم محرمانه، واگذارکننده[1] یک مقدار محرمانه را به‌عنوان راز بین شرکاء طوری تسهیم می‌کند، که یک زیرمجموعه مجاز[2] از شرکاء با روی هم قرار دادن سهام جزیی خویش قادر به بازسازی کلید محرمانه باشند، لیکن هر زیرمجموعه غیرمجاز[3] با به اشتراک گذاشتن سهام جزیی خویش قادر به بازسازی کلید محرمانه نباشند[۱]. اگر شرکاء غیرمجاز با به اشتراک گذاشتن سهام جزیی خویش، هیچ‌گونه اطلاعاتی در خصوص راز بدست نیاورند، در این صورت طرح را یک طرح تسهیم محرمانه کامل[4] گفته و زیرمجموعه‌های مجاز یک طرح را ساختار دسترسی[5] طرح گوییم. اولین طرح‌های تسهیم محرمانه ارائه شده، روش تسهیم محرمانه آستانه‌ای[6] بوده است که همزمان توسط شامیر[۲] بر مبنای چندجمله‌ای‌های لاگرانژ و بلکلی[۳] بر پایه هندسه تصویری در سال ۱۹۷۹ ارائه شد. یک طرح آستانه‌ای (k,n) عبارت است از طرح تسهیم محرمانه‌ای که واگذارکننده کلید محرمانه را طوری تسهیم می‌کند که هر k شریک یا بیشتر از n نفر قادر به بازسازی کلید محرمانه باشند ولی اگر کم‌تر از k شریک سهام خویش را به اشتراک بگذارند، قادر به بازسازی کلید محرمانه نباشند[۴]. طرح‌های مهم دیگر، طرح‌های خطی بر مبنای ساختار *فضای برداری*[7] بوده است[۶و۵]. در ادامه طرح‌های اثبات‌پذیر[8] ابتدا توسط کوهر و همکارانش معرفی گردید[۷]. ارتباط بین طرح‌های تسهیم محرمانه و کد توسط دانگ و همکارانش[۹و۸] در سال ۱۹۹۶ که مبنای آن بر اساس قضیه باقی‌مانده چینی بوده است مطرح گردید. ساختار دسترسی طرح‌های تسهیم محرمانه بر اساس کدهای تصحیح خطا[۱۰]، مربوط به توزیع وزن کدهای دوگان است[۱۲و۱۱و۵]. در حقیقت تعیین ساختار دسترسی طرح‌های تسهیم محرمانه بیشتر نیازمند داشتن توزیع وزن می‌باشد(تعیین توزیع وزن کدها عموما یک مسئله‌ی بسیار سخت است). در اصل، هر کد خطی تصحیح خطا می‌تواند برای ساختار طرح تسهیم راز مورد استفاده قرارگیرد. چگونگی تشخیص و تصحیح متقلب (متقلبین) در این طرح‌ها یک مساله باز می‌باشد[۱۶و۱۵و۱۴و۱۳]. در این مقاله روشی جدید را برای یافتن متقلب در طرح‌های تسهیم محرمانه بر اساس کدهای سه‌سه‌یی ارائه می‌شود.

ساختار مقاله به شرح زیر است: طرح‌های تسهیم محرمانه در بخش ۲ و مفاهیمی از کلاس کدهای سه‌سه‌یی در بخش ۳ بیان می‌شود. تقلب و تصحیح خطا در کدهای سه‌سه‌یی در بخش ۴، تحلیل تشخیص و تصحیح تقلب در بخش ۵ و در بخش پایانی نتیجه‌گیری ارائه می‌شود.

۲. طرح‌های تسهیم محرمانه

تعریف: فرض کنیم X یک مجموعه نقاط متناهی، R مجموعه‌ای از ورودی‌های تصادفی متناهی و $\Gamma: R \to [0,1]$ یک توزیع احتمال روی ورودی‌های R باشد. یک طرح تسهیم محرمانه مانند Σ نگاشتی از حاصل‌ضرب دو ورودی تصادفی به توی یک مجموعه $n-$تایی می‌باشد،

$$\Sigma : X \times R \to S_1 \times S_2 \times \cdots \times S_n \qquad (۱)$$

به‌طوری که مجموعه $n-$تایی را سهام و برای هر $r \in R$ و هر $x \in X$ مقدار $\Sigma(x,r)$ را سهم شریک p_i ; $i = 1,2,\ldots,n$ گفته و با $\Sigma_i(x,r)=\Sigma(x_i,r_i)$ نشان می‌دهیم که در آن S_i دامنه سهم p_i می‌باشد.

Σ در دست واگذارکننده می‌باشد، آن را طوری بین شرکاء تسهیم می‌کند که برای مقدار ورودی $x \in X$، او مقدار تصادفی $r \in R$ انتخاب شده از توزیع Σ را اختیار نموده و بردار تصادفی به‌صورت $(\Sigma_1(x,r),\ldots,\Sigma_n(x,r))$ را تولید می‌کند. سپس با یک روش امن از کانال خصوصی و به‌طور محرمانه مقدار $\Sigma_i(x,r)$ را به‌عنوان سهم شریک $i-$ام ارسال می‌دارد، با این نگرش که شرکاء دیگر هیچ‌گونه اطلاعاتی راجع به این مقدار ندارند.

تعریف: گردایه $\Gamma \subseteq 2^{|P|}$ یکنوا[9] است هرگاه اگر $B \in \Gamma$ و $B \subseteq C$ آنگاه $C \in \Gamma$.

1. Dealer
2. Qualified Subset
3. Non Qualified Subset
4. Perfect Secret Sharing Scheme
5. Access structure
6. Threshold Secret Sharing Scheme
7. Vector Space
8. Verifiable Secret Sharing Schemes
9. Monotone

گردایه یکنوا Γ از زیرمجموعه‌های غیرتهی $\{p_1,\ldots,p_n\}$ را یک ساختار دسترسی گوییم.

مجموعه‌های در Γ را مجموعه‌های مجاز و مجموعه‌هایی که در Γ نباشند را مجموعه‌های غیرمجاز گوییم.

تعریف: فرض کنیم S با دامنه متناهی از فضای محرمانه‌ها باشد. یک طرح تسهیم محرمانه با ساختار دسترسی Γ، عبارت است از طرحی که یک واگذارکننده مقدار محرمانه $s \in S$ را به‌عنوان ورودی طرح انتخاب نموده، به‌طوری که دو شرط زیر برقرار باشند:

الف) لزوم بازسازی[1]

کلید محرمانه s توسط هر مجموعه مجاز از شرکاء وقتی که سهام خویش را روی هم قرار دهند قابل بازسازی باشد (با فرض آن‌که هیچ‌کدام از شرکاء سهم تقلبی وارد بازی نکنند و سهم واقعی خویش را به اشتراک بگذارند). بدین مفهوم که برای هر مجموعه دلخواه $A \in \Gamma\ ;\ A=\{i_1,\ldots,i_{|A|}\}$، وجود دارد تابع بازسازی مانند f_A به‌صورت زیر:

$$f_A : S_{i_1} \times S_{i_2} \times \cdots \times S_{i_{|A|}} \to S \qquad (۲)$$

طوری که برای هر کلید محرمانه S و هر ورودی تصادفی r، اگر برای $i = 1,\ldots,n$ داشته باشیم $s_i \in S_i$ و $\Sigma(s,r)=(s_1,\ldots,s_n)$، آنگاه:

$$f_A(s_{i_1} \times s_{i_2} \times \cdots \times s_{i_{|A|}}) = s\ ;\ s_{i_j} \in S_{i_j}\ ,1 \le j \le |A| \qquad (۳)$$

ب) لزوم امنیت[2]

هر مجموعه غیرمجاز از شرکاء هیچ اطلاعات جزیی در کمک کردنشان به بازسازی کلید نداشته باشند. بدین مفهوم که برای هر مجموعه $B \notin \Gamma$ و هر دو کلید متفاوت $\omega_1, \omega_2 \in S$ و برای هر بردار $\{s_i\}_{i\in B}$ از سهام، آنگاه تساوی زیر همواره برقرار باشد،

$$p[\underset{p_i \in B}{\wedge} \Sigma_i(\omega_1,r)=s_i] = p[\underset{p_i \in B}{\wedge} \Sigma_i(\omega_2,r)=s_i] \qquad (۴)$$

نتیجه این که انتخاب یک مقدار تصادفی دلخواه از فضای کلید و مقدار دلخواه محاسبه شده از فضای مجموعه غیرمجاز، هم‌شانس هستند و برای رسیدن به کلید محرمانه هیچ مزیتی بر هم ندارند.

تعریف: فرض کنیم P یک مجموعه از شرکاء و Γ یک ساختار دسترسی روی P باشد. مجموعه $A \in \Gamma$ یک مجموعه مینیمال[3] می‌باشد، هرگاه اگر $B \in \Gamma$ و $B \subseteq A$ آنگاه $B = A$. گردایه همه مجموعه‌های مینیمال از Γ را با Γ^- نمایش می‌دهیم.

مثال: فرض کنیم $P=\{a,b,c\}$ یک مجموعه از شرکاء و $\Gamma=\{X \subseteq P\ ;\ |X| \ge 2\}$ یک ساختار دسترسی روی P باشد، آنگاه $\Gamma^- = \{ab, bc, ac\}$.

۳. کلاس کدهای سه‌سه‌یی

فرض کنیم $\left(GF(2)^n, +\right)$ یک گروه جمعی آبلی با مرتبه‌ی $N=2^n$، همراه با عضو خنثی باشد و $n \ge 2$ یک عدد صحیح باشد، با فرض آن‌که M یک گروه ضربی با مشخصه‌یی از $GF(2)^n$ به $GF(3)^*$ باشد که $|M| = \left|GF(2)^n\right| = N$.

مجموعه‌ی $GF(2)^n$ می‌تواند با مجموعه‌ای از اعداد صحیح $\{i : 0 \le i \le 2^n-1\}$ نمایش داده شود.

اعضاء $(i_0,i_1,\ldots,i_{n-1})$ از $GF(2)^n$ با $i = i_0 + i_1 2 + \ldots + i_{n-1}2^{n-1}$ مشخص می‌گردند، طوری‌که هر i_j، برابر با صفر یا یک است. عبارت $(i_0,i_1,\ldots,i_{n-1})$ نمایش دودویی عدد i می‌باشد.

تعریف می‌کنیم

$$f_i = f_i(y) = (-1)^{i_0y_0+i_1y_1+\ldots+i_{n-1}y_{n-1}}\ ;\ 0 \le i \le 2^n-1 \qquad (۵)$$

که در آن $y=(y_0,y_1,\ldots,y_{n-1})$ و $i=(i_0,i_1,\ldots,i_{n-1})$ به ترتیب نمایش دودویی اعداد y و i هستند.

برای هر i، $(0 \le i \le 2^n-1)$ مقادیر 2^n مشخصه از $GF(2)^n$ به $GF(3)^*$ معلوم هستند. بنابراین $M=\{f_0,f_1,\ldots,f_{2^n-1}\}$ یک ماتریس شناخته شده است، که در آن f_0 مشخصه‌ی بدیهی است. چون i و y با نمایش دودویی مربوطه‌شان، همانی هستند، لذا $f_i(y) = f_y(i)$.

برای هر زیرمجموعه‌ی X از $GF(2)^n$، کد مشخصه‌ی گروه C_x، بر روی $GF(3)$ توسط دانگ به‌صورت زیر توصیف شده است:

1. Reconstruction Requirement
2. Security Requirement
3. Minimal Set

$$C_X = \{\forall x \in X \ : \sum_{i=0}^{N-1} c_i f_i(x) = 0 \ ; \ (c_0, c_1, ..., c_{N-1}) \in GF(3)^N \ \} \quad (۶)$$

با فرض آن‌که $X = \{x_0, x_1, ..., x_{t-1}\}$ یک زیرمجموعه از فضای $GF(2)^n$ و X^c مکمل X در $GF(2)^n$ باشد. قضیه مهم زیر را در خصوص مولفه‌های کد سه‌سه‌یی داریم؛

قضیه: فرض کنید X یک زیرمجموعه از فضای $GF(2)^n$ باشد. برای $0 \le i \le N-1$، اگر بردار v_i به‌صورت زیر نمایش داده شود،

$$v_i = \left(f_0(x_i), f_1(x_i), ..., f_{N-1}(x_i)\right) \quad (۷)$$

آنگاه مجموعه $\{v_0, v_1, ..., v_{N-1}\}$ مستقل خطی بوده و ماتریس $H = \left[f_{j-1}(x_{i-1})\right]_{1 \le i \le t \ , \ 1 \le j \le N}$ دارای مرتبه t و یک ماتریس کنترل مشابهت برای C_X است. هم‌چنین ماتریس $G = \left[f_{j-1}(x_{t-1+i})\right]_{1 \le i \le N-t \ , \ 1 \le j \le N}$ دارای مرتبه‌ی $N-t$ و یک ماتریس مولد برای C_X است، بنابراین C_X یک کدخطی $[N, N-t]$ بر روی $GF(3)$ می‌باشد. به علاوه H یک ماتریس مولد برای C_{X^c} و $C_X \oplus C_{X^c} = GF(3)^N$ است [۱۷و۸].

وزن همینگ یک بردار a از $GF(2)^n$، نمایش داده شده به‌صورت $wt(a)$، با تعداد مختصات غیرصفر آن تعیین می‌شود.

برای $1 \le r \le n$ فرض کنیم $X(r,n) = \left\{a \in GF(2)^n : wt(a) > r\right\}$ و $C_3(r,n)$ نمایش کد $C_{X(r,n)}$ بر روی $GF(3)$ باشد. فرض کنیم $c = (c_0, ..., c_{2^n-1})$ در فضای $GF(3)^{2^n}$ باشد، محمل[1] c را با $Supp(c)$ نمایش داده و عبارت است از:

$$Supp(c) = \{i \ ; \ 0 \le i < 2^n \ , \ c_i \ne 0\}$$

گوییم کدکلمه a توسط کدکلمه b پوشش داده می‌شود، هرگاه $Supp(a)$ شامل $Supp(b)$ باشد.

قضیه: خواص زیر برای کدهای $C_3(r,n)$ برقرار است:

الف) $C_3(r,n)$ یک کد سه‌سه‌یی $\left[2^n, \sum_{j=0}^{r} \binom{n}{j}, 2^{n-r}\right]$ می‌باشد.

ب) کدکلمه‌هایی که دارای حداقل وزن غیرصفر هستند، کد $C_3(r,n)$ را تولید می‌کنند.

ج) کد دوگان $C_3(r,n)^{\perp}$ معادل با کد $C_3(n-r-1,n)$ است[۷].

قضیه: برای هر عدد صحیح $1 \le m \le n$ در کد $C_3(r,n)$، به تعداد $\binom{n+1}{m} 2^m$ کدکلمه به شکل $\sum_{j=0}^{m-1} a_j v_{i_j}$ وجود دارند که دارای وزن همینگ یکسان به‌صورت زیر می‌باشند:

$$w(m) = 2^n - 2^{n-m} \frac{2^m + (-1)^{(m+2r)/3} 2}{3} \quad (۸)$$

که در آن برای هر j، $a_j \in GF(3)^*$ و $r = m \pmod 3$ باقی‌مانده‌ی منحصر به فرد با $0 \le r \le 2$ و $0 \le i_0 < i_1 < ... < i_{m-1} \le n$ است [۱۲و۹و۷و۴].

۴. تقلب و تصحیح خطا در کدهای سه‌سه‌یی

در کدهای سه‌سه‌یی با توجه به n، تعداد شرکاء $2^n - 1$ می‌باشند و با در نظر گرفتن مؤلفه r، کد $C_3(r,n)$ یک کد سه‌سه‌یی با پارامترهای $[N, K, d] = \left[2^n, \sum_{j=0}^{r} \binom{n}{j}, 2^{n-r}\right]$ است.

در کدهای سه‌سه‌یی با توجه به K به دست آمده و در نتیجه زیرمجموعه‌ی دلخواه انتخابی از میدان $GF(2)^n$ یعنی $\left(X \in GF(2)^n\right)$ تمام مختص‌های ماتریس کنترل مشابهت H از روی تابع زیر به دست می‌آید:

$$f_i(y) = (-1)^{i_0 y_0 + i_1 y_1 + ... + i_{n-1} y_{n-1}} \quad (۹)$$

از رابطه (۹) مشخص است که تمام درآیه‌های G و H مقادیر غیرصفر دارند و در واقع ماتریس‌های G و H به شکل ماتریس‌های استاندارد در نمی‌آیند و در نتیجه ماتریس H^T نیز به شکل استاندارد قابل نمایش نیست. با توجه به توضیحات فوق مشخص می‌گردد که تصحیح خطا همانند مواقعی که تمام مختصات یک و صفر بودند به راحتی انجام نمی‌گیرد. بنابراین تصحیح خطا در کدهای سه سه‌یی را به طریق زیر انجام می‌دهیم؛

برای تشخیص و تصحیح متقلب در یک طرح، شرط لازم در روش ما عبارت است از این‌که باید تعداد افراد متقلب در بازیابی راز از نصف کم‌ترین فاصله‌ی همینگ، کم‌تر باشند. یعنی اگر به تعداد e متقلب در بین k نفر شریک در بازیابی راز حضور

1. Support

داشته باشند، آنگاه برای بازیابی درست راز باید شرط $e \le \left\lfloor \frac{d}{2} \right\rfloor$ برقرار باشد. بدین مفهوم که باید به ازای هر فرد متقلب تقریبا دو نفر درست‌کار بیشتر از سطح آستانه‌ای حضور داشته باشند و در صورتی که تعداد افراد متقلب از کران رابطه‌ی فوق بیشتر باشد، این روش کارآیی ندارد. در ضمن اضافه کردن عدد یک به ابتدای سمت چپ مجموعه دلخواه ورودی به معنی اضافه کردن یک نفر درست‌کار به مجموعه می‌باشد که این هم کمک موثری در تشخیص و تصحیح خطا مخصوصا برای مجموعه‌های بیش از یک متقلب دارد. در واقع شرط فوق و اضافه کردن عدد یک به ابتدای سمت چپ مجموعه دلخواه ورودی، در پیدا کردن متقلب و تصحیح آن ما را به سمت کدکلمه‌های مینیمال که مجموعه‌های دسترسی مجاز و مینیمال از روی آن‌ها بدست می‌آیند سوق می‌دهد.

فرضیه‌ی ۱ (جهت تشخیص متقلب)

در کدهای سه‌سه‌یی با n مشخص و با تعداد 2^n-1 سهام‌دار، اگر کدکلمه را به‌صورت $V_1=a_1,a_2,...,a_i,...,a_{2^n}$ و مجموعه‌ی دلخواه ورودی از سهام‌داران (به تعداد 2^n-1) را بعد از اضافه کردن عدد یک به ابتدای سمت چپ آن به صورت $V_2=1,b_2,...,b_i,...,b_{2^n-1}$ نشان داده $(b_i,a_i \in F_3)$ و عمل‌گر زیر را تعریف می‌کنیم:

$$W = V_1 * V_2 = \begin{cases} 0 & if \quad a_i = b_i \\ 1 & if \quad a_i \neq b_i \end{cases}. \qquad (۱۰)$$

با توجه به W های به دست آمده ناشی از عمل‌گر فوق برای V_2 با تمام کدکلمه‌ها، اگر W با حداقل مولفه‌ی ۱ موجود را در نظر بگیریم، آنگاه تعداد ۱ ها نشان‌دهنده تعداد خطا یا تعداد متقلب در طرح تسهیم محرمانه است.

فرضیه‌ی ۲ (جهت تشخیص و تصحیح متقلب)

در کدهای سه‌سه‌یی با n مشخص و با تعداد 2^n-1 سهام‌دار، در این روش تصحیح خطا به‌صورت زیر انجام می‌پذیرد: برای هر کدکلمه دلخواه (به‌عنوان شرکایی که برای بازسازی کلید محرمانه سهام خویش را به اشتراک گذاشته‌اند)، فرضیه ۱ از سمت چپ، بیت به بیت به آن‌ها اعمال شده و سپس خروجی دو بیت دو بیت جدا می‌شود که در نتیجه تعداد دو بیتی‌های غیرصفر نشان‌دهنده‌ی تعداد خطاست و با در نظر گرفتن کم‌ترین تعداد دو بیتی غیرصفر مربوط به کدکلمه خاص، تصحیح خطا به‌صورت زیر انجام می‌گیرد:

- اگر دو بیتی 11 در خروجی ظاهر شود، آنگاه مقدار ۲ در ورودی به مقدار ۱باید تصحیح گردد،
- اگر دو بیتی 10 در خروجی ظاهر شود، آنگاه مقدار ۲ در ورودی به مقدار ۰ باید تصحیح گردد،
- اگر دو بیتی 01 در خروجی ظاهر شود، آنگاه مقدار ۰ در ورودی به مقدار ۱باید تصحیح گردد.

لازم به توضیح می‌باشد که تصحیح بدین شکل انجام می‌گیرد که دو بیتی 11 یعنی عدد ۳ که در مد ۲ برابر ۱ می‌باشد، یعنی اگر در خروجی 11 داشتیم سهم سهام‌دار مربوطه به ۱ تصحیح می‌شود. و دو بیتی 10 در خروجی یعنی عدد ۲ که در مد ۲ برابر ۰ می‌باشد، یعنی 10 در خروجی به معنای تصحیح عدد ۲ ورودی به ۰ می‌باشد. در مورد 01 در خروجی نیز به همین طریق تحلیل می‌شود.

توجه: دوبیتی 11 که در واقع عدد ۳ می‌باشد هرگز در مجموعه ورودی و یا کدکلمه‌ها ظاهر نمی‌شود و راز صحت و قطعیت این فرضیه برای تصحیح نیز همین می‌باشد.

در واقع حالات ممکن برای کدهای سه‌سه‌یی با در نظر گرفتن دو بیتی‌های مربوطه به‌صورت زیر می‌باشند:

$$\begin{matrix}0&1\\1&0\end{matrix},\ \begin{matrix}1&0\\1&1\end{matrix},\ \begin{matrix}0&0\\0&1\end{matrix},\ \begin{matrix}0&0\\1&0\end{matrix},\ \begin{matrix}1&0\\1&0\end{matrix},\ \begin{matrix}0&1\\0&1\end{matrix}$$

و سه مورد زیر که در صورت به‌وجود آمدنشان موجب عدم تصحیح قطعی می‌گردید هرگز اتفاق نمی‌افتند:

$$\begin{matrix}0&1\\1&1\\1&0\end{matrix},\ \begin{matrix}0&0\\1&1\\1&1\end{matrix},\ \begin{matrix}1&0\\1&1\\0&1\end{matrix}$$

لازم به توضیح است که از این فرضیه یعنی فرضیه‌ی مربوط به تصحیح خطا برای تشخیص متقلب هم می‌شود استفاده کرد که در واقع کم‌ترین تعداد دو بیتی‌های غیرصفر بعد از اعمال عمل‌گر مربوطه به تمام بردارها (تمام کدکلمه‌ها با مجموعه‌ی دلخواه ورودی) تعداد متقلبین را می‌دهد . ضمن این‌که اگر بخواهیم فقط تعداد متقلبین را بدانیم به‌راحتی از فرضیه‌ی اول استفاده می‌کنیم.

پس در حالت کلی فاصله‌ی بین کدکلمه‌ها را طبق فرضیه‌ها

بدست آورده و حداقل آن را در نظر می‌گیریم تا تعداد خطاهای قابل آشکارسازی و قابل تصحیح به دست آید.

هر مجموعه‌ای که بخواهند کلید را پیدا کنند با توجه به سهم آورده شده از طرف آن‌ها، کدکلمه متناظر با آن را مد نظر قرار می‌دهیم و بعد از اضافه کردن عدد ۱ به ابتدای سمت چپ آن، فاصله‌ی آن را با تک‌تک کدکلمه‌ها طبق فرایند بالا پیدا نموده و در ادامه با استفاده از فرضیه‌های فوق آن را با کدکلمه‌یی که کم‌ترین فاصله را داشته باشد تصحیح می‌کنیم.

شرح عملیات تشخیص و تصحیح خطا و یا به عبارتی تشخیص و تصحیح متقلب به‌طور کامل در مثال زیر آمده است.

مثال: بررسی یک طرح تسهیم محرمانه مبتنی بر کدهای سه‌سه‌یی برای حالت $n=3$؛

با فرض $r=1$ و با توجه به تعریف کدهای سه‌سه‌یی مقدار $k=4$ به دست می‌آید، پس G دارای چهار سطر و همچنین H نیز دارای چهار سطر می‌باشد. در نتیجه مجموعه‌ی دلخواه انتخابی X باید دارای چهار عضو باشد.

این طرح تسهیم محرمانه شامل هفت شریک ($N=2^n-1$) می‌باشد. حال اگر مجموعه‌ی دلخواه را به‌صورت زیر انتخاب کنیم:

$$X=\{x_0,x_1,x_2,x_3\}=\{0,1,2,4\} \qquad (11)$$

با توجه به تعریف $f_i(y)$ ، مقادیر زیر بدست می‌آید.

$$x_0=0 \rightarrow f_0(0)=f_1(0)=f_2(0)=\ldots=f_7(0)=1$$

,

$$x_1=1 \rightarrow \begin{cases} f_0(1)=f_2(1)=f_4(1)=f_6(1)=1 \\ f_1(1)=f_3(1)=f_5(1)=f_7(1)=2 \end{cases}$$

,

$$x_1=2 \rightarrow \begin{cases} f_0(2)=f_1(2)=f_4(2)=f_5(2)=1 \\ f_2(2)=f_3(2)=f_6(2)=f_7(2)=2 \end{cases}$$

,

$$x_1=4 \rightarrow \begin{cases} f_0(4)=f_1(4)=f_2(4)=f_3(4)=1 \\ f_4(4)=f_5(4)=f_6(4)=f_7(4)=2 \end{cases}$$

اگر v_i برای $0\le i\le N-1$ برداری به‌صورت زیر نمایش داده شود:

$$\left(f_0(x_i),f_1(x_i),\ldots,f_{N-1}(x_i)\right)$$

پس مجموعه‌ی $\{v_0,v_1,\ldots,v_{N-1}\}$، مستقل خطی است، در نتیجه برای مجموعه‌ی فوق بردارهای v_0,v_1,v_2,v_4 مستقل خطی‌اند.

با توجه به مستقل خطی بودن بردارهای فوق می‌توان گفت $H=\left[f_{j-1}(x_{i-1})\right]_{1\le i\le t\ ,\ 1\le j\le N}$ دارای مرتبه t و یک ماتریس کنترل مشابهت برای کد می‌باشد. و داریم:

$$H=\begin{bmatrix} 1&1&1&1&1&1&1&1 \\ 1&2&1&2&1&2&1&2 \\ 1&1&2&2&1&1&2&2 \\ 1&1&1&1&2&2&2&2 \end{bmatrix}$$

از این‌که $G=\left[f_{j-1}(x_{t-1+i})\right]_{1\le i\le N-t\ ,\ 1\le j\le N}$ دارای مرتبه $N-t$ و یک ماتریس مولد برای C_X است، بنابراین C_X یک کدخطی $[N,N-t]$ بر روی $GF(3)$ می‌باشد. به‌علاوه H یک ماتریس مولد برای C_{X^c} و $C_X\oplus C_{X^c}=GF(3)^N$ است. بنابراین برای پیدا کردن ماتریس مولد، $X^c=\{x_4,x_5,x_6,x_7\}=\{3,5,6,7\}$ را به‌عنوان مکمل مجموعه منتخب در نظر گرفته و لذا ماتریس مولد آن به‌صورت زیر به دست می‌آید،

$$G=\begin{bmatrix} 1&2&2&1&1&2&2&1 \\ 1&2&1&2&2&1&2&1 \\ 1&1&2&2&2&2&1&1 \\ 1&2&2&1&2&1&1&2 \end{bmatrix}.$$

لذا با در نظر گرفتن $r=1$ و با توجه به فرمول‌های قبلی، $C_3(1,3)$ یک کد سه‌سه‌یی[۴و۴و۸] و دوگان آن نیز یک کد سه‌سه‌یی [۴و۴و۸] است. با توجه به این‌که H یک ماتریس 8×4 به‌عنوان ماتریس کنترل مشابهت برای $C_3(1,3)$ و نیز یک ماتریس مولد برای $C_3^{\perp}(1,3)$ می‌باشد و داریم $C^{\perp}=[A]_{1\times 4}[H]_{4\times 8}$ که در آن $A=(a_1,a_2,a_3,a_4)$ به ازاء $a_i\in\{0,1,2\}$ است. نتیجه آن ۸۱ کدکلمه است که از طریق کد دوگان به دست می‌آید. توجه داریم، کدکلمه‌هایی با مختصات اولیه‌ی ۱ (نرمال شده) که هیچ کدکلمه دیگر را پوشش ندهند کدکلمه‌های مینیمال می‌باشند، که در این مثال عبارتند از:

(11121222), (11212122), (12112212), (11111111), (11000022), (10100202), (10221102), (12011201), (11202011), (11020211), (12220001), (12011201), (10120121), (10211021), (10002221), (11101000), (11222200), (11010100), (12122020), (12210220), (12001120), (10110010), (10201210), (12200112), (12021012), (12102101), (10022110)

از روی کدکلمه‌های مینیمال مجموعه‌های دسترسی مجاز (سهام‌داران مجاز) به‌صورت زیر به دست می‌آیند:

$(p_1,p_2,p_3,p_4,p_5,p_6,p_7)$, (p_1,p_6,p_7), (p_2,p_5,p_7),
(p_3,p_4,p_7), (p_1,p_2,p_4), (p_1,p_3,p_4,p_5,p_7),
(p_2,p_3,p_5,p_6,p_7), (p_2,p_3,p_4,p_6,p_7), (p_1,p_2,p_3,p_4,p_5),
(p_1,p_2,p_3,p_4,p_6), (p_1,p_2,p_3,p_5,p_6), (p_1,p_2,p_5,p_6,p_7),
(p_1,p_3,p_4,p_6,p_7), (p_3,p_4,p_5,p_6), (p_2,p_3,p_4,p_5,p_7),
(p_1,p_2,p_4,p_6,p_7), (p_1,p_3,p_5,p_6,p_7), (p_1,p_3,p_5),
(p_2,p_3,p_6), (p_1,p_2,p_3,p_7), (p_4,p_5,p_6,p_7), (p_2,p_4,p_5,p_6).
(p_1,p_2,p_4,p_5,p_7), (p_1,p_4,p_5,p_6)

با توجه به مجموعه‌ی فوق، مجموعه‌های دسترسی مینیمال در این مثال برابر است با:

(p_3,p_4,p_5,p_6), (p_1,p_3,p_5), (p_2,p_3,p_6)
(p_1,p_2,p_3,p_7), (p_1,p_6,p_7), (p_2,p_5,p_7)
(p_3,p_4,p_7), (p_1,p_2,p_4), (p_4,p_5,p_6,p_7)
(p_2,p_4,p_5,p_6), (p_1,p_4,p_5,p_6)

۵. تحلیل تشخیص و تصحیح خطا

فرض کنیم بردار 1202221 هدفشان بازسازی کلید باشد؛ بر طبق فرضیه‌ی۱، عمل‌گر تعریف شده را برای آن (بعد از اضافه کردن عدد یک به ابتدای سمت چپ آن) به تمام کدکلمه‌ها اعمال می‌کنیم. در ادامه کم‌ترین فاصله را بدست می‌آوریم. برای این مثال نتیجه $d=2$ بدست می‌آید. به بیان دیگر نزدیک‌ترین کدکلمه به بردار هدف عبارتند از: 0002221 و 1202011.

بدین مفهوم که دو خطا (متقلب) در بین بردار ورودی وجود دارند. همان‌طورکه انتظار می‌رفت هر دو کدکلمه مربوط به کدکلمه‌های در مجموعه‌های دسترسی مینیمال هستند.

با توجه به فرضیه‌ی۲ که برای تصحیح خطا استفاده می‌شود، اگر مجموعه‌ی دلخواه ورودی و نیز کدکلمه‌ها را به‌صورت دودویی نوشته و عمل‌گر تعریف شده را اعمال کنیم باز به نتیجه‌ی فوق یعنی دو خطا یا دو متقلب خواهیم رسید. به این صورت که بعد از اعمال عمل‌گر، تمام بیت‌ها را دو بیت دو بیت از سمت چپ در نظر گرفته و تعداد هر دو بیت دارای مختصات غیرصفر را به‌عنوان خطا یا متقلب در نظر می‌گیریم، یعنی در مثال فوق اگر مجموعه 0002221 را در نظر بگیریم نفر اول و دوم متقلب محسوب می‌شوند که برای تصحیح خطا دو بیت مربوط به نفر دوم یعنی 10 را بعد از اعمال فرضیه‌ی۲ در نظر گرفته که همان عدد ۲ می‌باشد چون این عدد در مد ۲ صفر می‌شود پس سهم 2 مربوط به نفر دوم به 0 تصحیح می‌شود یعنی یک نفر را با قطعیت تصحیح می‌کنیم.

00	00	00	10	10	10	01
01	10	00	10	10	10	01
01	10	00	00	00	00	00

و اگر مجموعه 1202011 را در نظر بگیریم نفر پنجم و ششم متقلب محسوب می‌شوند که برای تصحیح خطا دو بیت مربوط به نفر پنجم و ششم یعنی 10 و 11 را بعد از اعمال فرضیه‌ی ۲ مد نظر قرار می‌دهیم، که همان اعداد ۲ و ۳ می‌باشند. چون این اعداد در مد ۲ صفر می‌شود پس سهم ۲ مربوط به نفر پنجم به 0 و سهم مربوط به نفر ششم به 1 تصحیح می‌شوند یعنی دو نفر را با قطعیت تصحیح می‌کنیم.

01	10	00	10	00	01	01
01	10	00	10	10	10	01
00	00	00	00	10	11	00

به‌عنوان نمونه‌ی بعدی اگر مجموعه‌ی دلخواه ورودی را به‌صورت 0011222 در نظر بگیریم و عملیات فوق را طبق فرضیه‌ی ۲ برای همه‌ی کدکلمه‌ها انجام دهیم به دو بردار با $d=3$ می‌رسیم یعنی: 0012002 و 0002221. با توجه به خروجی به دست آمده از اعمال عمل‌گر به کدکلمه‌های فوق و در نظر داشتن حداقل تعداد دو بیتی غیرصفر، دو بردار خروجی به‌صورت 11 00 00 11 01 00 00 و 00 10 10 11 00 00 00 به ترتیب برای دو کدکلمه مینیمال 1 2 2 2 0 0 0 و 2 0 0 1 2 0 0 به دست می‌آیند که در مورد کدکلمه اولی با توجه به وجود 11 دودویی در آن که معرف عدد ۳ و در نتیجه عدد 1 در مد 2 می‌باشد عدد 2 مربوط به سهم نفر هفتم در مجموعه‌ی دلخواه ورودی به 1 تصحیح می‌شود و در مورد دومی با توجه به وجود 10 دو دویی در خروجی که معرف عدد ۲ و در نتیجه عدد 0 در مد ۲ می‌باشد سهم 2 و 2 مربوط به نفرات پنجم و ششم به عدد 0 تصحیح می‌شوند.

۶. نتیجه‌گیری

با توجه به این‌که یکی از اهداف اصلی در طرح‌های تسهیم محرمانه، پیدا کردن مجموعه‌های دسترسی مجاز و مینیمال بوده و استفاده از کدها برای این منظور بسیار مناسب می‌باشد که دلیل اصلی استفاده از آن‌ها، پیدا کردن سریع مجموعه‌های دسترسی مجاز و مینیمال با استفاده از کدکلمه‌های مینیمال می‌باشد. در این مقاله برای پیدا کردن خطا یا متقلب و نیز

تصحیح خطا در طرح‌های تسهیم راز مبتنی بر کدهای سه‌سه‌یی دو فرضیه جدید ارائه دادیم. سپس با استفاده از این فرضیه‌ها، برای طرح‌های با تعداد محدودی شریک (کم‌تر از ۱۰ شریک) شبیه‌سازی انجام پذیرفت که نتایج قابل قبولی بدست آمده است (با توجه به حجم زیاد خروجی از آوردن آنها صرف‌نظر شده است). نکته قابل تامل این‌که در این روش برای تشخیص و تصحیح متقلب، نیاز به استفاده از کدکلمه‌های مینیمال نیست. این امر زمان محاسبات را به دلیل عدم استفاده از کدکلمه‌های مینیمال و تنها با استفاده از بردارهای حاصل از ماتریس مولد یا ماتریس کنترل مشابهت به نسبت قابل توجهی کاهش می‌دهد.

۷. مراجع

[1] Shamir, A. "How to Share a Secret."; Commun. of the ACM 1979, 22, 612-613.

[2] Blakley, G. R. "Safeguarding Cryptographic Keys."; AFIPS Conference Proceedings 1979, 48, 313-317.

[3] Tassa, T. "Hierarchical Threshold Secret Sharing, The Proceeding of the First Theory of Cryptography Conference."; MIT, Cambridge, TCC 2004, 473-490.

[4] Bertilsson, M. "Linear Code and Secret Sharing."; PHD Thesis, Linkoping University, 1993.

[5] Stinson, D. R. "An Explication of Secret Sharing Schemes; Designs Codes and Cryptography."; 1992, 2, 357-390.

[6] Chor, B.; Goldwasser, S. S.; Micali, B. "Verifiable Secret Sharing and Achieving Simultaneity in the Presence Offaults."; Proceeding of FOCS 1985, 383-395.

[7] Ding, C.; Kohel, R.; Ling, S. "Elementary 2-group Character Codes."; IEEE Trans Inform. Theory 2000, 46, 280-284.

[8] Ding, C.; Kohel, R.; Ling, S. "Note Secret Sharing with a Class of Ternary Codes."; Theoretical Computer Science 2000, 246, 285-298.

[9] Mac Williams, F. J.; Sloane, N. J. A. "The Theory of Error-Correcting Codes."; North-Holland, Amsterdam; 1978.

[10] Beimel, A.; Tassa, T.; Weinreb. E. "Characterizing Ideal Weighted Threshold Secret Sharing, the Proceeding of the Second Theory of Cryptography Conference."; MIT, TCC 2005, , 600-619.

[11] Brickell, E. F.; Stinson, D. R. "The Detection of Cheaters in Threshold Schemes. In S. Goldwasser, editor."; Advances in Cryptology- CRYPTO LNCS 1988, 403, 564-577. Springer- Verlag.

[12] Iwamoto, M.; Koga, H.; Hirosuke, H. "Coding Theorems for Cheating-Detectable Secret Sharing Schemes with Tow Shares."; IEEE, Information Theory Workshop, Japan, 2009.

[13] Tompa, M.; Woll, H. "How to Share a Secret with Cheaters."; Journal of Cryptology 1988, 1, 133-139.

[14] Preneel, B. "Design of Cryptography Hash Functions."; PHD Thesis, COSIC, 2003.

[15] Safavi-Naini, R. "Feistel Type Authentication Codes."; Advances in Cryptology, Proc. Asiacrypt 91, LNCS, Springer – Verlag, to appear.

[16] Carpentieri, M.; Santis, A. D.; Vaccaro, U. "Size of Shares and Probability of Cheating in Threshold Scheme."; Advances in Cryptology- Eurocrypt 93, LNCS 765, 1994, Springer-Verlag, 118-125.

[17] Ogata, W.; Kurosawa, K.; Stinson, D. R. "Optimum Secret Sharing Scheme Secure Against Cheating."; SIAM Journal of Discrete Mathematics 2006, 20(1), 79-95.

[18] Anderson, R. J. C.; Helleseth, Ding T.; Klove, T. "How to Build Robust Control Systems."; Designs Codes Cryptogr 1998, 15, 111-124.