مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال ششم، شماره ۱، بهار ۱۳۹۴؛ ص ۵۴-۴۵

طرح‌های تسهیم محرمانه با زیرمجموعه‌های مجاز پنج عضوی

زین‌العابدین نوروزی[1*]، حمیدرضا میمنی[2]

۱- استادیار، دانشگاه جامع امام حسین(ع) ۲- دانشیار، دانشگاه شهید رجایی، دانشکده علوم، گروه ریاضی

(دریافت: ۹۳/۱۱/۲۵، پذیرش: ۹۴/۰۲/۱۴)

چکیده

یکی از پارامترهای مهم در طرح تسهیم محرمانه، نرخ اطلاعات است، این نرخ مقدار اطلاعاتی است که بین سهام‌داران در مقایسه با اندازه کلید محرمانه می‌بایست توزیع گردد. در حالت کلی یافتن نرخ اطلاعات طرح‌های تسهیم محرمانه برای ساختار دسترسی داده شده وجود ندارد، ولی یافتن این نرخ برای برخی از طرح‌های خاص امکان‌پذیر می‌باشد. در این مقاله کران بالای نرخ اطلاعات با استفاده از روش دنباله مستقل ارائه شده، سپس ساختارهای دسترسی با پنج زیرمجموعه مجاز مینیمال را مورد بررسی قرار داده و برخی از مشخصه‌های نرخ اطلاعات بهینه را برای طرح‌های تسهیم محرمانه ایده‌آل به‌دست آورده و برای طرح‌های غیرایده‌آل، کران‌هایی را برای نرخ اطلاعات بهینه ثابت شد.

کلید واژه‌ها: روش دنباله مستقل، نرخ اطلاعات، طرح‌های تسهیم محرمانه و ساختار دسترسی مینیمال.

Secret Sharing Schemes with Five Minimal Qualified Subsets

Z. Norozi*, H. Maimani
Imam Hossein University

(Received: 14/02/2015, Accepted: 04/05/2015)

Abstract

One of the important parameters of the secret sharing scheme is information rate, which defines the size of distributed information among the shareholders in comparison of their secret key size. Generally, for any given access structure, it is not possible that one can find the information rate of secret sharing schemes, but finding these rate for some specific designs is possible. In this paper, an upper bound of information rate is presented using independent sequence method, then, the secret sharing schemes whose access structure having five minimal qualified subsets have been investigated and some of the characterizations of ideal secret sharing schemes have been obtained and for the non-ideal case, bounds on the optimal information rate have been provided.

Keywords: Independent Sequence Method, Information Rate, Secret Sharing Schemes and Minimal Access Structure.

*Corresponding Author E-mail: znorozi@ihu.ac.ir

۱. مقدمه

اطلاعات دارایی با ارزش و ذی‌قیمت هستند. برای بسیاری از افراد، شرکت‌ها و مؤسسات یک مسئله بحرانی به سرقت رفتن یا ناپدید شدن اطلاعات است و بازبینی اطلاعات ممکن است هزینه‌های سنگینی را به یک سازمان تحمیل نماید. شاید یکی از راه‌های منطقی نگهداری محرمانه اطلاعات در یک مکان امن با کلید اصلی محرمانه است. سؤال مهم این است که، کلید اصلی چگونه و در دسترس چه فرد یا افرادی باشد. از جمله راه‌حل‌های این مشکل، کپی‌برداری از این کلید و سپس در اختیار افراد مجاز و یا در مکان‌های متفاوت قرار دادن آن می‌باشد. مؤسسات فناوری اطلاعات (IT) سرویس‌هایی را برای این ذخیره‌سازی با قرنطینه مناسب ارائه می‌دهند. روش‌های گفته شده تا حدودی مشکل را حل می‌نمایند. یک راه‌حل مناسب استفاده از طرح‌های تسهیم محرمانه است. این طرح‌ها در سامانه‌هایی که به صورت شبکه‌ای عمل می‌کنند نقش مهمی ایفاء می‌نمایند. در علومی مانند پدافند نوین که نیاز به رعایت سلسله مراتب با وزن‌های متفاوت هست، این طرح‌ها بسیار مفید و کارا هستند. در طرح تسهیم محرمانه واگذارکننده[1] یک مقدار محرمانه را به‌عنوان راز بین شرکا طوری تسهیم می‌کند، که یک زیرمجموعه مجاز[2] از شرکا با روی هم قرار دادن سهام جزیی خویش قادر به بازسازی کلید محرمانه باشند، ولی هر زیرمجموعه غیرمجاز[3] با به اشتراک گذاشتن سهام جزیی خویش قادر به بازسازی کلید محرمانه نباشند [۱]. اگر شرکای غیرمجاز با به اشتراک گذاشتن سهام جزیی خویش، هیچ‌گونه اطلاعاتی در خصوص راز به دست نیاورند، در این صورت طرح را یک طرح تسهیم محرمانه کامل[4] گویند. به همه زیرمجموعه‌های مجاز یک طرح ساختار دسترسی[5] طرح گفته می‌شود. اولین طرح‌های تسهیم محرمانه ارائه شده، روش تسهیم محرمانه آستانه‌ای[6] بوده‌اند. این طرح‌ها هم‌زمان توسط شامیر [۲] بر مبنای چندجمله‌ای‌های لاگرانژ و بلکلی [۳] بر پایه هندسه تصویری در سال ۱۹۷۹ ارائه شدند. 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 [۶ و ۵]. در ادامه طرح‌های اثبات‌پذیر[8] توسط کوهر و همکارانش معرفی گردید [۷]. ساختار دسترسی یک طرح تسهیم محرمانه خانواده‌ای از زیرمجموعه‌های مجاز $\Gamma \subseteq 2^{|P|}$ است، که در آن P مجموعه شرکا می‌باشد. در حالت کلی اگر یک مجموعه مجاز باشد، آنگاه هر مجموعه مافوق نیز چنین است. بنابراین می‌توان نتیجه گرفت که ساختار دسترسی Γ توسط خانواده‌ای از زیرمجموعه‌های مجاز مینیمال Γ_0 تعیین می‌گردد.

یک موضوع مهم در طرح‌های تسهیم محرمانه، اندازه سهام است. چرا که امنیت یک سامانه، از مقدار اطلاعاتی که می‌بایست به صورت محرمانه نگهداری شود، تبعیت می‌کند. در نتیجه میزان سهمی که به هر شریک داده می‌شود از اهمیت خاصی برخوردار است. هرگاه طول کلید محرمانه هر یک از شرکا بزرگ باشد، آنگاه حفاظت از این کلید برای شخص سخت بوده، بنابراین به کارایی طرح خدشه وارد می‌شود. در یک طرح تسهیم محرمانه برای بالا بردن کارایی و امنیت آن، مهم این است که تا حد امکان اندازه[9] سهام را کوچک اختیار کرده و ارتباط بین طول بیت‌های محرمانه و طول بیشینه سهام از اهمیت خاصی برخوردار باشد. بنابراین از پارامتری بنام نرخ اطلاعات[10] در این طرح‌ها استفاده می‌شود.

اولین روش به کار برده شده جهت تعیین کران بالای نرخ اطلاعات به‌نام مجموعه دنباله مستقل است. این روش توسط بلاندو و همکارانش در سال ۱۹۹۷ بکار گرفته شده [۸] و سپس به صورت کلی‌تر در سال ۲۰۰۰ توسط پدرو و سیز[11] مورد استفاده قرار گرفته است [۹]. یک شرط لازم برای این‌که یک ساختار دسترسی ایده‌آل باشد توسط بریکل و داونپورت و یک شرط کافی از ساختار فضای برداری توسط بریکل حاصل و ارائه شده است. هر ساختار دسترسی فضای برداری، ایده‌آل است ولی عکس آن برای همیشه برقرار نیست [۱۱،۱۰].

ساختار مقاله به شرح زیر است. در بخش دوم تعریف دقیقی از یک طرح محرمانه را ارائه داده و به یکی از مؤلفه‌های بسیار مهم به‌نام نرخ اطلاعات اشاره می‌شود. روش دنباله مستقل برای یافتن کران بالای نرخ اطلاعات را در بخش سوم بیان کرده و در بخش چهارم به ساختارهای مینیمال با پنج زیرمجموعه مجاز اشاره و چهار قضیه بسیار مهم را بیان و اثبات می‌شود. در بخش پایانی نتیجه‌گیری را ارائه می‌گردد.

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 یک مجموعه $n-$تایی می‌باشد.

$$\Sigma : X \times R \to S_1 \times S_2 \times \cdots \times S_n \qquad (1)$$

به‌طوری‌که 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

[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] Size
[10] Information Rate
[11] Saez

می‌شود و در حالت کلی به صورت $\Sigma_i(x,r)=\Sigma(x_i,r_i)$ نشان می‌دهند که در آن S_i دامنه سهم شریک p_i می‌باشد.

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

تعریف: گردایه $\Gamma\subseteq 2^{|P|}$ یکنوا[1] است هرگاه اگر $B\in\Gamma$ و $B\subseteq C$ آنگاه $C\in\Gamma$. به‌علاوه گردایه یکنوا Γ از زیرمجموعه‌های غیرتهی $\{p_1,\ldots,p_n\}$ را یک ساختار دسترسی گویند. مجموعه‌های در Γ را مجموعه‌های مجاز و مجموعه‌هایی که در Γ نباشند را مجموعه‌های غیرمجاز می‌نامند.

تعریف: فرض کنید 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[2]: کلید محرمانه S توسط هر مجموعه مجاز از شرکا وقتی که سهام خویش را روی‌هم قرار دهند، قابل بازسازی باشد. بدین مفهوم که برای هر مجموعه مجاز در ساختار دسترسی مجاز مانند $A\in\Gamma;A=\{i_1,\ldots,i_{|A|}\}$ وجود دارد تابع بازسازی مانند f_A به صورت زیر است:

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

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

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

ب) لزوم امنیت[3]: در یک طرح تسهیم محرمانه امنیت بدین مفهوم است 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 می‌باشد، 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 آن این است 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 کنید P یک مجموعه از شرکا و Γ یک ساختار دسترسی روی P باشد. مجموعه $A\in\Gamma$ یک مجموعه مینیمال[4] است 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 کنید $P=\{a,b,c\}$ یک مجموعه از شرکا و $\Gamma=\{X\subseteq P\ ;\ |X|\ge 2\}$ یک ساختار دسترسی روی P باشد، آنگاه $\Gamma^-=\{ab,bc,ac\}$.

تعریف: فرض کنید P یک مجموعه از شرکا، Γ یک ساختار دسترسی روی P و S یک مجموعه از فضای محرمانه‌ها باشند، و $PS(\Gamma,S)$ یک طرح تسهیم محرمانه کامل با ساختار دسترسی Γ باشد، آنگاه نرخ اطلاعات این طرح به‌صورت زیر تعریف می‌شود:

$$\rho=\rho(PS(\Gamma,S))=\frac{\log q}{\log r}. \qquad (۵)$$

که در آن، $r=\max\{\#(p):p\in P\}$، نماد $\#(p)$ تعداد سهام ممکن و قابل قبول برای شریک p از مجموعه تمام شرکا و $q=|S|$.

پیچیدگی یک طرح تسهیم محرمانه به‌وسیله طول سهام طرح اندازه‌گیری می‌شود. در تمام طرح‌های تسهیم محرمانه کامل، طول هر سهم بزرگ‌تر یا مساوی با اندازه طول محرمانه است [۱۲]. بنابراین طرحی که اندازه هر سهم آن با اندازه محرمانه یکسان باشد، دارای پیچیدگی بهینه[5] است. طرح‌های تسهیم محرمانه آستانه‌ای دارای پیچیدگی بهینه هستند. در یک طرح تسهیم محرمانه کامل، اگر نرخ اطلاعات آن برابر با مقدار ۱ باشد، در این‌صورت طرح را ایده‌آل[6] گویند. و یک ساختار دسترسی ایده‌آل است، هرگاه دارای طرح تسهیم محرمانه ایده‌آل باشد. در مقاله [۱۳] ثابت شده است که برای هر ساختار دسترسی، یک طرح تسهیم محرمانه وجود دارد. ولی برخی ساختارهای دسترسی وجود دارند که برای آن‌ها هیچ طرح تسهیم محرمانه ایده‌آلی وجود ندارد [۱۴]. مشخصه‌های ساختارهای دسترسی ایده‌آل در زمره مسائل باز طرح‌های تسهیم محرمانه هستند. بریکل و داونپورت ارتباط بین ساختارهای دسترسی ایده‌آل و مترویدها را پایه‌ریزی نمودند [۱۱].

میانگین نرخ اطلاعات[7] طرح کامل $PS(\Gamma,S)$ عبارت است از:

$$\tilde{\rho}=\tilde{\rho}(PS(\Gamma,S))=\frac{|P|\log|S|}{\sum_{p\in P}\log\#(p)}. \qquad (۶)$$

در یک طرح تسهیم محرمانه کامل سهم هر شریک از شرکا همواره

[1] Monotone
[2] Reconstruction Requirement
[3] Security Requirement
[4] Minimal Set
[5] Optimal Complexity
[6] Ideal
[7] Average Information Rate

بزرگ‌تر یا مساوی اندازه محرمانه است، بنابراین $\tilde{\rho} \le 1$. به‌علاوه، $\tilde{\rho} = 1$ اگر و فقط اگر $\rho = 1$.

در تعاریف فوق نرخ اطلاعات و میانگین نرخ اطلاعات برای یک طرح تسهیم محرمانه به‌عنوان یک مشخصه اساسی طرح بیان شد.

امکان یافتن یک طرح تسهیم محرمانه ایده‌آل برای یک ساختار دسترسی داده شده مانند Γ همواره امکان‌پذیر نمی‌باشد. بنابراین سعی می‌شود یک طرح تسهیم محرمانه‌ای برای Γ بیابیم، که دارای نرخ اطلاعاتی به اندازه کافی بزرگ باشد. بنابراین نرخ اطلاعات بهینه[1] تعریف می‌شود. نرخ اطلاعات بهینه برای یک طرح کامل $PS(\Gamma, S)$ عبارت است از:

$$\rho^*(\Gamma) = \sup\{\rho : \exists PS(\Gamma, S)\} \qquad (۷)$$

در تعریف بالا، سوپریمم روی همه مجموعه‌های شدنی از محرمانه‌های $|S| \ge 2$ و همه طرح‌های تسهیم محرمانه Σ با ساختار دسترسی Γ گرفته می‌شود. البته نرخ اطلاعات بهینه برای یک ساختار دسترسی ایده‌آل برابر یک می‌باشد. روند فوق ما را به این سمت هدایت می‌کند که می‌بایست دو مسئله زیر را مورد بررسی قرار دهیم:

- مشخصه ساختارهای دسترسی ایده‌آل،
- یافتن کران‌هایی روی نرخ اطلاعات بهینه.

ما به این دو مسئله در بخش ۴ برای ساختارهای دسترسی با پنج در مجموعه مینیمال جواب داده‌ایم.

۳. روش دنباله مستقل

در این بخش با اولین روش به‌کار برده شده جهت تعیین کران بالای نرخ اطلاعات به‌نام مجموعه دنباله مستقل آشنا شده و به ارتباط بین ساختار دسترسی فضای برداری، ایده‌آل بودن طرح، میزان نرخ اطلاعات طرح و مجموعه دنباله مستقل برای ساختارهای دسترسی با کم‌تر از پنج زیرمجموعه مجاز مینیمال می‌پردازیم. در ادامه این بخش تعدادی تعریف، نتیجه، لم و قضیه مورد نیاز را بیان می‌شود [۱۷-۱۵].

تعریف: فرض کنید Γ یک ساختار دسترسی روی مجموعه شرکا P باشد. یک دنباله دلخواه از زیرمجموعه‌های $B_0 = \varnothing$, $\varnothing \ne B_1 \subset \ldots \subset B_m \notin \Gamma$ مستقل ساختاری[2] از $A \subseteq \mathrm{P}$ است، اگر برای هر $1 \le i \le m$ زیرمجموعه‌های $X_1, \ldots, X_m \subset A$ وجود داشته باشند به طوری که $B_i \cup X_i \in \Gamma$ و $B_{i-1} \cup X_i \notin \Gamma$.

مثال: فرض کنید G یک گراف روی مجموعه شرکا $\mathrm{P} = \{a,b,c,d,e\}$ با ساختار دسترسی مینیمال $\Gamma_0 = \{\{a,b\},\{b,c\},\{c,d\},\{c,e\},\{d,e\}\}$ باشد. در این‌صورت $B_1 = \{a\}$, $B_2 = \{a,c\}$ یک دنباله مستقل ساختاری از $A = \{a,b,c,d\}$ است.

مثال: فرض کنید $\mathrm{P} = \{a,b,c,d,e,f\}$ مجموعه شرکا و Γ یک ساختار دسترسی با $\{a,b,c,d\} \in \Gamma_0$ باشد. با فرض آنکه $A = \{a,b,c,d,e\}$، آنگاه دنباله زیر یک دنباله مستقل ساختاری از A است. $B_1 = \{a\}$, $B_2 = \{a,b\}$, $B_3 = \{a,b,c\}$ زیرا کافی است زیرمجموعه‌های $X_1, X_2, X_3 \subset A$ به‌صورت زیر انتخاب گشوند:

$$X_1 = \{b,c,d\} \ , \ X_2 = \{c,d\} \ , \ X_3 = \{d\}.$$

هرگاه بتوان در یک طرح تسهیم محرمانه یک دنباله مستقل ساختاری را به وسیله زیرمجموعه‌ای از شرکا به دست آورد، آنگاه امکان به دست آوردن کران بالای نرخ اطلاعات بهینه به وسیله قضیه زیر وجود دارد.

قضیه [۱-۳]: فرض کنید Γ یک ساختار دسترسی روی مجموعه متناهی از شرکا P باشد و $\varnothing \ne B_1 \subset \ldots \subset B_m \notin \Gamma$ یک دنباله از زیرمجموعه‌های P باشد که مستقل ساختاری به وسیله زیرمجموعه $A \subseteq \mathrm{P}$ است، آنگاه دو عبارت زیر برقرار هستند:

- اگر $A \in \Gamma$، آنگاه $\rho^*(\Gamma) \le \frac{|A|}{m+1}$،
- اگر $A \notin \Gamma$، آنگاه $\rho^*(\Gamma) \le \frac{|A|}{m}$.

فرض کنید Γ یک ساختار دسترسی یک طرح تسهیم محرمانه با ساختار دسترسی مینیمال Γ_0 باشد. هرگاه بتوان برای این ساختار دسترسی مینیمال یک تجزیه با شرایط زیر به دست آورد، آنگاه کران پایین نرخ اطلاعات این ساختار از قضیه بعدی نتیجه می‌شود (راه کلی برای یافتن یک تجزیه مناسب وجود نداشته و یک مسئله باز می‌باشد؟).

قضیه [۲-۳]: با مفروضات زیر [۱۱ و ۱۶]:

۱- Γ یک ساختار دسترسی روی مجموعه شرکا P با ساختار دسترسی مینیمال Γ_0 باشد،

۲- $\Gamma_{0,1}, \ldots, \Gamma_{0,r} \subset \Gamma_0$ یک تجزیه از Γ باشد،

۳- Γ_i ساختار دسترسی با ساختار دسترسی مینیمال $\Gamma_{0,i}$ روی $P_i \subseteq \mathrm{P}$ باشد، $P_i = \bigcup_{A \in \Gamma_{0,i}} A$;

۴- $\lambda_A = |\{i \in \{1,\ldots,r\} \ ; \ A \in \Gamma_{0,i}\}|$

۵- $r_p = |\{i \in \{1,\ldots,r\} \ ; \ p \in P_i\}|$،

۶- برای هر $1 \le i \le m$ وجود داشته باشد یک طرح تسهیم محرمانه ایده‌آل مانند Σ_i با ساختار دسترسی Γ_i،

آنگاه $\rho^*(\Gamma) \ge \frac{\min\{\lambda_A \ ; \ A \in \Gamma_0\}}{\max\{r_p \ ; \ p \in P_i\}}$.

ساختار فضای برداری[3] یکی از ساختارهای مفید برای طرح‌های ایده‌آل است. فرض کنیم P مجموعه‌ای از شرکا، Γ یک ساختار

[1] Optimal Information Rate
[2] Made Independent
[3] Vector Space Construction

دسترسی روی این مجموعه، $D \notin \mathrm{P}$ واگذارکننده و K یک میدان متناهی باشد. گوییم Γ یک ساختار دسترسی K- فضای برداری است اگر وجود داشته باشد یک فضای برداری E روی میدان متناهی مانند K با نگاشت $\varphi : \mathrm{P} \cup \{D\} \to E$ به طوری که $\varphi(x) \neq 0$ برای هر $x \in \mathrm{P} \cup \{D\}$. به‌علاوه $A \in \Gamma$ اگر و فقط اگر $\varphi(D)$ *ترکیب خطی*[1] (به مفهوم جبرخطی) از بردارهای مجموعه $\varphi(A) = \{\varphi(p) : p \in A\}$ باشد.

واگذاری سهام در این ساختار به صورت زیر انجام می‌پذیرد. واگذار کننده مقدار محرمانه $k \in K$ و مقدار تصادفی $v \in E$ را طوری انتخاب می‌نماید که $v \times \varphi(D) = k$ و مقدار $v \times \varphi(P) = s_P$ سهم شریک $p \in \mathrm{P}$ می‌باشد که در آن ضرب استفاده شده، ضرب برداری است.

تعریف: Γ را یک ساختار دسترسی فضای برداری گوییم هرگاه برای هر میدان متناهی K، آن یک ساختار دسترسی K- فضای برداری باشد.

توجه: اگر $q > |\mathrm{P}|$ قوایی از عدد اول باشد، آنگاه طرح آستانه‌ای شامیر روی میدان متناهی $K = GF(q)$، یک طرح تسهیم محرمانه ایده‌آل است. زیرا هر ساختار دسترسی فضای برداری، ایده‌آل است.

لم [۱-۳]: فرض کنید Γ یک ساختار دسترسی روی مجموعه شرکا P باشد و $\Gamma_{0,1}, \ldots, \Gamma_{0,r}$ یک تجزیه از Γ باشد و $P_1, \ldots, P_r$ یک افراز از مجموعه P بوده که در آن $P_i = \bigcup_{A \in \Gamma_{0,i}} A$. با فرض آنکه Γ_i نماد ساختار دسترسی روی مجموعه P_i با ساختار پایه $\Gamma_{0,i}$ باشد.

هرگاه $\Gamma_1, \ldots, \Gamma_r$ یک ساختار فضای برداری روی میدان متناهی K باشد، آنگاه ساختار دسترسی Γ نیز چنین است.

نتیجه [۱-۳]: فرض کنید Γ یک ساختار دسترسی روی مجموعه شرکا K با یک یا دو زیرمجموعه مجاز مینیمال باشد، آنگاه برای هر میدان متناهی K، ساختار دسترسی Γ یک ساختار دسترسی K - فضای برداری و در نتیجه یک ساختار دسترسی ایده‌آل است.

لم [۲-۳]: فرض کنید Γ یک ساختار دسترسی روی مجموعه شرکا P با مجموعه مینیمال Γ_0 باشد. اگر P' مجموعه‌ای از شرکا باشد که $\mathrm{P} \cap \mathrm{P}' = \varnothing$، و Γ' ساختار دسترسی روی مجموعه $\mathrm{P} \cup \mathrm{P}'$ با ساختار دسترسی مینیمال $\Gamma'_0 = \{A \cup \mathrm{P}' \; ; \; A \in \Gamma_0\}$ باشد، در صورتی که یک ساختار دسترسی فضای برداری روی میدان متناهی K باشد، آنگاه Γ' نیز یک ساختار دسترسی فضای برداری روی این میدان است.

لم [۳-۳]: فرض کنید Γ یک ساختار دسترسی روی مجموعه $\mathrm{P} = \{p_1, \ldots, p_m\}$ با پایه Γ_0 باشد. روی مجموعه $\mathrm{P}^e = \{B_{p_1}, \ldots, B_{p_m}\}$; $B_{p_i} = \{p_{i,1}, \ldots, p_{i,n_i}\}$ از $n = n_1 + \cdots + n_m$ شریک، ساختار دسترسی Γ^e با پایه $\Gamma_0^e = \{A^e : A \in \Gamma_0\}$، که در آن $A^e = \bigcup_{p \in A} B_p$، را در نظر بگیرید. حال اگر Γ ساختار دسترسی فضای برداری روی میدان متناهی F باشد، آنگاه ساختار دسترسی Γ^e نیز چنین است.

تعریف: فرض کنید Γ یک ساختار دسترسی روی مجموعه شرکا P با مجموعه مبنا $\Gamma_0 = \{A_1, \ldots, A_r\}$ باشد. برای هر $x \in P$ بردار وقوعی[2] از x عبارت است از $\chi(x) = (x_1, \ldots, x_r)$ که در آن اگر $x \in A_i$ آنگاه $x_i = 1$ و در جاهای دیگر $x_i = 0$.

۴. ساختارهای دسترسی با پنج زیرمجموعه مجاز مینیمال

در این بخش مشخصه‌ای از ساختارهای دسترسی ایده‌آل با پنج زیرمجموعه مجاز مینیمال را در چهار قضیه زیر بیان و اثبات می‌شود. اولین قضیه موقعیت‌های غیرمجاز را در یک ساختار دسترسی ایده‌آل با پنج زیرمجموعه مجاز مینیمال تعیین می‌کند.

قضیه [۱-۴]: فرض کنید Γ یک ساختار دسترسی روی مجموعه شرکا P با پنج زیرمجموعه مجاز مینیمال $\Gamma_0 = \{A_1, A_2, A_3, A_4, A_5\}$ باشد. اگر عناصر $a, b, c, d, x \in \mathrm{P}$ با یکی از بردارهای وقوعی جدول (۱) موجود باشند، به‌علاوه اگر بردار دیگری مانند y وجود داشته باشد که $\chi(y) = (0,0,0,0,1); y \in \mathrm{P}$ که فقط برای ردیف‌های ۴، ۸، ۱۲ و ۱۶ در نظر گرفته شود، آنگاه $\rho^*(\Gamma) \leq \frac{2}{3}$.

اثبات: فرض کنید یکی از ردیف‌های ۱، ۲، ۳، ۵، ۶، ۷، ۹، ۱۰ یا ۱۱ ارائه شده در جدول (۱) برقرار باشد. مجموعه‌های زیر را در نظر بگیرید:

$$B_1 = \mathrm{P} \setminus \{a,b,c,d\},$$
$$B_2 = \mathrm{P} \setminus \{a,b,d\},$$
$$B_3 = \mathrm{P} \setminus \{a,b\}.$$

از آنجایی که عبارت‌های $A_3 \subset B_1 \cup \{a,b\}$، $A_1 \subset B_2 \cup \{a\}$ و $A_2 \subset B_3 \cup \{b\}$ برقرار هستند، نتیجه آن مجاز بودن مجموعه‌های A_1، A_2 و A_3 است. از طرفی برای هر $i = 1, \ldots, 5$ داریم:

- چون $a \in A_1, b \in A_2, a \in A_3, b \in A_4$ و $a,b \in A_5$، آنگاه،
- با تو جه به $A_i \not\subset B_3$ این‌که $a \in A_1, d \in A_2, a \in A_3$ و $a,d \in A_4, A_5$، آنگاه $A_i \not\subset B_2 \cup \{b\}$.
- از این‌که $c \in A_1$، $b,c,d \in A_2$، $b \in A_3, A_5$ و $c,b,d \in A_4$ آنگاه $A_i \not\subset B_1 \cup \{a\}$.

بنابراین مجموعه‌های B_3، $B_2 \cup \{b\}$ و $B_1 \cup \{a\}$ غیرمجاز هستند، زیرا تمام مجموعه‌های A_iها مینیمال اختیار شده‌اند. حال اگر $\{a,b\} \in \Gamma$، آنگاه دنباله به صورت $\varnothing \neq B_2 \subset B_3$ یک دنباله مستقل ساختاری به وسیله مجموعه دو عضوی $\{a,b\}$ است. اگر $\{a,b\} \notin \Gamma$ آنگاه دنباله $\varnothing \neq B_1 \subset B_2 \subset B_3$، یک دنباله مستقل ساختاری به وسیله

[1] Linear Combination

[2] Incidence Vector

مجموعه $\{a,b\}$ است. از قضیه (۱-۳) نتیجه می‌گردد $\rho^*(\Gamma)\le\frac{2}{3}$.

حال فرض کنید یکی از ردیف‌های ۱۳، ۱۴ یا ۱۵ ارائه شده از جدول (۱) برقرار باشند. مجموعه‌های زیر را در نظر بگیرید:

$$B_1=\mathrm{P}\setminus\{a,b,c,d,x\},$$
$$B_2=\mathrm{P}\setminus\{a,b,d,x\},$$
$$B_3=\mathrm{P}\setminus\{a,b,x\}.$$

از آنجایی که $A_3\subset B_1\cup\{a,b,x\}$ همچنین $A_1\subset B_2\cup\{a,x\}$ و $A_2\subset B_3\cup\{b,x\}$ نتیجه آن مجاز بودن مجموعه‌های A_1، A_2 و A_3 است. از طرفی برای هر $i=1,\ldots,5$ داریم:

- با توجه به این‌که $a\in A_1,A_3$ ، $b\in A_2$ ، $x\in A_4$ و $d\in A_5$ ، آنگاه $A_i\not\subset B_3$،
- با توجه به‌این‌که $a\in A_1,A_3$ ، $c\in A_2,A_5$ ، $c\in A_5$، آنگاه $A_i\not\subset B_2\cup\{b,x\}$،
- از این‌که $c\in A_1$، $b\in A_2,A_3$ ، $d\in A_4$ و $d\in A_5$، آنگاه $A_i\not\subset B_1\cup\{a,x\}$.

بنابراین B_3، $B_2\cup\{b,x\}$ و $B_1\cup\{a,x\}$ غیرمجاز هستند. اگر $\{a,b\}\in\Gamma$، آنگاه $\varnothing\neq B_2\subset B_3$، یک دنباله مستقل ساختاری به وسیله مجموعه $\{a,b\}$ است. و اگر $\{a,b\}\notin\Gamma$، آنگاه $\varnothing\neq B_1\subset B_2\subset B_3$، یک دنباله مستقل ساختاری به وسیله مجموعه $\{a,b\}$ است. از قضیه (۱-۳) نتیجه می‌شود $\rho^*(\Gamma)\le\frac{2}{3}$.

در ادامه اثبات فرض کنید یکی از ردیف‌های ۴، ۸ یا ۱۲ ارائه شده از جدول (۱) برقرار باشد. مجموعه‌های زیر را در نظر بگیرید:

$$B_1=\mathrm{P}\setminus\{a,b,c,d,y\},$$
$$B_2=\mathrm{P}\setminus\{a,b,d,y\},$$
$$B_3=\mathrm{P}\setminus\{a,b,y\}.$$

مجموعه‌های A_1، A_2 و A_3 مجاز هستند، زیرا $A_3\subset B_1\cup\{a,b,y\}$، $A_1\subset B_2\cup\{a,y\}$ و $A_2\subset B_3\cup\{b,y\}$. به‌علاوه برای هر $i=1,\ldots,5$ داریم $A_i\not\subset B_3$، $A_i\not\subset B_2\cup\{b,y\}$ و $A_i\not\subset B_1\cup\{a,y\}$. نتیجه این‌که، مجموعه‌های B_3، $B_2\cup\{b,y\}$ و $B_1\cup\{a,y\}$ غیرمجاز هستند. حال اگر $\{a,b\}\in\Gamma$، آنگاه دنباله $\varnothing\neq B_2\subset B_3$، یک دنباله مستقل ساختاری به‌وسیله مجموعه $\{a,b\}$است. اگر $\{a,b\}\notin\Gamma$، آنگاه $\varnothing\neq B_1\subset B_2\subset B_3$ یک دنباله مستقل ساختاری به‌وسیله مجموعه $\{a,b\}$ است. از قضیه (۱-۳) نتیجه می‌شود $\rho^*(\Gamma)\le\frac{2}{3}$.

در پایان فرض کنید ردیف ۱۶ ارائه شده از جدول (۱) برقرار باشد. مجموعه‌های زیر را در نظر بگیرید:

$$B_1=\mathrm{P}\setminus\{a,b,c,d,x,y\},$$
$$B_2=\mathrm{P}\setminus\{a,b,d,x,y\},$$
$$B_3=\mathrm{P}\setminus\{a,b,x,y\}.$$

مجموعه‌های A_1، A_2 و A_3 مجاز هستند، زیرا $A_3\subset B_1\cup\{a,b,x,y\}$، $A_1\subset B_2\cup\{a,x,y\}$ و $A_2\subset B_3\cup\{b,x,y\}$. از طرفی به ازای هر $i=1,\ldots,5$ داریم $A_i\not\subset B_2\cup\{b,x,y\}$، $A_i\not\subset B_3$ و $A_i\not\subset B_1\cup\{a,x,y\}$. بنابراین B_3، $B_2\cup\{b,x,y\}$ و $B_1\cup\{a,x,y\}$ مجموعه‌های غیرمجاز هستند. حال اگر $\{a,b\}\in\Gamma$، آنگاه $\varnothing\neq B_2\subset B_3$ یک دنباله مستقل ساختاری به وسیله مجموعه $\{a,b\}$ست. در صورتی‌که $\{a,b\}\notin\Gamma$، آنگاه $\varnothing\neq B_1\subset B_2\subset B_3$ یک دنباله مستقل ساختاری به وسیله مجموعه $\{a,b\}$ است. از قضیه (۱-۳) نتیجه می‌شود $\rho^*(\Gamma)\le\frac{2}{3}$.

مشخصه‌ای از ساختارهای دسترسی ایده‌آل با پنج زیرمجموعه مجاز مینیمال در قضیه (۲-۳) آمده است. با توجه به این نکته که هر ساختار دسترسی فضای برداری ایده‌آل بوده، هدف ارائه شرط یا شرایطی است که بیان کند که اگر یک ساختار دسترسی ایده‌آل باشد، آنگاه در چه صورتی این ساختار دسترسی یک ساختار دسترسی فضای برداری نیز هست. ایده اصلی در معادل بودن گزاره‌های زیر، استفاده از بردارهای وقوعی قضیه (۱-۳) است.

قضیه [۲-۴]: فرض کنید Γ یک ساختار دسترسی روی مجموعه شرکا P با پنج زیرمجموعه مجاز مینیمال $\Gamma_0=\{A_1,A_2,A_3,A_4,A_5\}$ باشد، با فرض آنکه $A_i\cup A_j\cup A_k\neq\mathrm{P};1\le i\neq j\neq k\le 5$، $A_i\cup A_j\cup A_k\cup A_l=\mathrm{P};1\le i\neq j\neq k\neq l\le 5$ و همچنین $A_i\cap A_{i+1}\cap A_{i+2}\neq\varnothing\ ;\ i=1,2,3$، آنگاه گزاره‌های زیر معادل هستند:

- Γ یک ساختار دسترسی فضای برداری است،
- Γ یک ساختار دسترسی ایده‌آل است،
- $\rho^*(\Gamma)>\frac{2}{3}$،
- وجود دارد جایگشتی مانند σ روی مجموعه $\{i,j,k,l,t\}$ به طوری که،

$$A_{\sigma(i)}\cap A_{\sigma(j)}\cap A_{\sigma(k)}\cap A_{\sigma(l)}\subset A_{\sigma(t)}\ ;$$
$$1\le i\neq j\neq k\neq l\neq t\le 5.$$

اثبات: اگر Γ یک ساختار دسترسی فضای برداری باشد، آنگاه Γ یک ساختار دسترسی ایده‌آل است و به‌علاوه اگر Γیک ساختار دسترسی ایده‌آل باشد، آنگاه $\rho^*(\Gamma)>\frac{2}{3}$ [۱۰].

در ادامه فرض کنید $\rho^*(\Gamma)>\frac{2}{3}$. برای اثبات بند چهار به صورت زیر عمل کنید. بدون این‌که از کلیت مسئله کاسته شود کافی است زیرمجموعه ارائه شده $A_2\cap A_3\cap A_4\cap A_5\subset A_1$ را ثابت کنید. توجه شود که $A_l\not\subset A_i\cup A_j\cup A_k$ برای هر جایگشتی از عناصر $i,j,k,l\in\{1,\ldots,5\}$. زیرا بنا به فرض مسئله می‌دانیم اجتماع هر سه‌تایی مخالف P و در صورتی‌که اجتماع هر چهارتایی برابر با P است. بنابراین با توجه به جایگشت فوق می‌توان برای عناصر a,c و d

بردارهای وقوعی هر کدام را به صورت زیر در نظر گرفت:

$$a \in A_3 \setminus A_2 \cup A_4 \cup A_5 \therefore \chi(a) = (1,0,1,0,a_5)$$
$$c \in A_1 \setminus A_3 \cup A_4 \cup A_5 \therefore \chi(c) = (1,1,0,0,0)$$
$$d \in A_2 \setminus A_1 \cup A_3 \cup A_5 \therefore \chi(d) = (0,1,0,d_4,1)$$

به برهان خلف، فرض کنید $A_2 \cap A_3 \cap A_4 \cap A_5 \not\subset A_1$ در نتیجه عنصری مانند $b \in \mathrm{P}$ را می‌توان انتخاب کرد به طوری که $\chi(b) = (0,1,1,1,1)$. بنابراین طبق بند یازدهم قضیه (۱-۴) داریم، $\rho^*(\Gamma) \le \frac{2}{3}$. و این با فرض مسئله تناقض دارد. در اثبات فوق حالت فرض در جایگشت عبارت است از $A_1 \cup A_2 \cup A_3 \cup A_4 = \mathrm{P}$ و $A_1 \cup A_2 \cup A_3 \neq \mathrm{P}$. با این مفروض به بردارهای وقوعی بند یازده دست یافتیم. می‌توان با اعمال جایگشت‌های دیگر به یکی از حالات شانزده‌گانه فوق رسید.

در ادامه فرض کنید شرط ۴ برقرار باشد، هدف اثبات بند ۱ است. با توجه به لم (۲-۳)، می‌توان فرض کرد که اشتراک تمام مجموعه‌ها تهی باشد. یعنی $A_1 \cap A_2 \cap A_3 \cap A_4 \cap A_5 = \varnothing$. بنابراین برای هر $1 \le i \neq j \neq k \neq l \le 5$ دلخواه، همواره عبارت $A_i \cap A_j \cap A_k \cap A_l = \varnothing$ برقرار است. با توجه به این مطلب که از مجموعه پنج عضوی، اجتماع هر سه شریک تمام عناصر اصلی را می‌سازند، در نتیجه بردار وقوعی هر شریک به یکی از فرم‌های زیر است:

$$\chi_1 = (1,1,1,0,0) \quad , \quad \chi_2 = (1,1,0,1,0),$$
$$\chi_3 = (1,1,0,0,1) \quad , \quad \chi_4 = (1,0,1,1,0),$$
$$\chi_5 = (1,0,1,0,1) \quad , \quad \chi_6 = (1,0,0,1,1),$$
$$\chi_7 = (0,0,1,1,1) \quad , \quad \chi_8 = (0,1,0,1,1),$$
$$\chi_9 = (0,1,1,0,1) \quad , \quad \chi_{10} = (0,1,1,1,0).$$

با توجه به فرض مسئله، از این‌که $A_i \cap A_j \cap A_k \neq \varnothing$، در نتیجه عناصر با بردارهای وقوعی که در دو مکان یک و در سه مکان صفر ظاهر شوند وجود ندارند.

برای هر i از مجموعه $i \in \{1,2,\cdots,10\}$، فرض کنید $B_i = \{p \in \mathrm{P} : \chi(p) = \chi_i\}$. مشاهده می‌کنید همواره $B_i \neq \varnothing \; ; \; 1 \le i \le 10$. در غیر این صورت اجتماع حداقل یک سه‌تایی باید کل شرکا را بدهد که با فرض مسئله تناقض دارد. بنابراین مجموعه $\{B_1,\ldots,B_{10}\}$ یک افراز از P است. با توجه به بردارهای وقوعی فوق، مشاهده می‌کنید که $B_1 = \{a,b,c\}$ و $B_2 = \{a,b,d\}$، با همین فرایند در نهایت $B_{10} = \{b,c,b\}$ حاصل می‌شوند. به‌علاوه با توجه به بردارهای وقوعی بالا، امکان ساختن مجموعه‌های A_1, A_2, A_3, A_4 و A_5 به صورت زیر وجود خواهند داشت:

$$A_1 = B_4 \cup B_5 \cup B_6 \cup B_7,$$
$$A_2 = B_7 \cup B_8 \cup B_9 \cup B_{10},$$
$$A_3 = B_2 \cup B_3 \cup B_6 \cup B_8,$$
$$A_4 = B_1 \cup B_3 \cup B_5 \cup B_9,$$
$$A_5 = B_1 \cup B_2 \cup B_4 \cup B_{10}.$$

در نتیجه برای ساختار دسترسی Γ روی مجموعه شرکا $\mathrm{P} = \{p_1,\ldots,p_{10}\}$ یک ساختار دسترسی پایه به فرم زیر وجود دارد:

$$\Gamma_0 = \{\{p_4,p_5,p_6,p_7\},\{p_7,p_8,p_9,p_{10}\},$$
$$\{p_2,p_3,p_6,p_8\},\{p_1,p_3,p_5,p_9\},$$
$$\{p_1,p_2,p_4,p_{10}\}\}.$$

در ادامه کافی است ثابت کنید ساختار دسترسی Γ یک ساختار دسترسی F فضای برداری است. فرض کنید F یک میدان متناهی با مشخصه ۲ باشد. با فرض آنکه $E = F^5$، نگاشت با ضابطه زیر را در نظر بگیرید:

$$\Psi : \mathrm{P} \cup \{D\} \to E$$
$$\Psi(D) = (1,0,0,0,0)$$
$$\Psi(p_1) = (1,1,1,0,0) \;,\; \Psi(p_2) = (1,1,0,1,0),$$
$$\Psi(p_3) = (1,1,0,0,1) \;,\; \Psi(p_4) = (1,0,1,1,0),$$
$$\Psi(p_5) = (1,0,1,0,1) \;,\; \Psi(p_6) = (1,0,0,1,1),$$
$$\Psi(p_7) = (0,0,1,1,1) \;,\; \Psi(p_8) = (0,1,0,1,1),$$
$$\Psi(p_9) = (0,1,1,0,1) \;,\; \Psi(p_{10}) = (0,1,1,1,0).$$

با فرض آنکه $A \subset \mathrm{P}$ یک زیرمجموعه دلخواه باشد، آنگاه $A \in \Gamma$ اگر و فقط اگر $\Psi(D) \in \langle \Psi(p) : p \in A \}$. بنابراین Γ یک ساختار دسترسی F فضای برداری است.

قضیه [۳-۴]: فرض کنید Γ یک ساختار دسترسی روی مجموعه شرکا P با پنج زیرمجموعه مجاز مینیمال $\Gamma_0 = \{A_1,A_2,A_3,A_4,A_5\}$ باشد با فرض آنکه، $A_i \cup A_j \cup A_k \cup A_l \neq \mathrm{P}; 1 \le i \neq j \neq k \neq l \le 5$، آنگاه گزاره‌های زیر معادل هستند:

- Γ یک ساختار دسترسی فضای برداری است،
- Γ یک ساختار دسترسی ایده‌آل است،
- $\rho^*(\Gamma) > \frac{2}{3}$،
- برای هر $i,j,k \in \{1,\ldots,5\}$، یک جایگشت مانند σ روی $\{i,j,k\}$ وجود دارد به طوری که،

$$A_{\sigma(i)} \cap A_{\sigma(j)} = A_{\sigma(i)} \cap A_{\sigma(k)}.$$

اثبات: با برقرار بودن بند ۳ هدف اثبات بند ۴ است. فرض کنید $\rho^*(\Gamma) > \frac{2}{3}$. ابتدا نشان داده می‌شود که اگر $A_i \cap A_j \neq A_j \cap A_k$، آنگاه برای هر $i,j,k \in \{1,\ldots,5\}$ داریم $A_i \cap A_j \subset A_j$. بدون این‌که از کلیت مسئله کاسته شود، فرض کنید $\{i,j,k\} = \{1,2,3\}$ یک مجموعه دلخواه بوده و $A_1 \cap A_2 \neq A_2 \cap A_3$ (*). در ادامه ادعا می‌شود عبارت $A_1 \cap A_3 \subseteq A_2$ برقرار است. با توجه به (*) یکی از دو حالت زیر برقرار است:

- $A_1 \cap A_2 \not\subset A_2 \cap A_3$ و یا
- $A_2 \cap A_3 \not\subset A_1 \cap A_2$.

بدون کاستن از کلیت مسئله، فرض کنید $A_2\bigcap A_3\not\subset A_1\bigcap A_2$. در نتیجه $A_2\bigcap A_3\not\subset A_1$. برای اثبات رابطه $A_1\bigcap A_3\subseteq A_2$، به برهان خلف فرض کنید $A_1\bigcap A_3\not\subset A_2$. عناصر a,b,c,d,x و y را به همراه بردارهای وقوعی‌شان به صورت زیر انتخاب می‌شود:

$$a\in A_1\bigcap A_3\setminus A_2 \quad\therefore\quad \chi(a)=(1,0,1,a_4,a_5)$$
$$b\in A_2\bigcap A_3\setminus A_1 \quad\therefore\quad \chi(b)=(0,1,1,b_4,b_5)$$
$$c\in A_1\setminus A_2\bigcup A_3\bigcup A_4 \quad\therefore\quad \chi(c)=(1,0,0,0,c_5)$$
$$d\in A_2\setminus A_1\bigcup A_3\bigcup A_4 \quad\therefore\quad \chi(d)=(0,1,0,0,d_5)$$
$$x\in A_4\setminus A_1\bigcup A_2\bigcup A_3 \quad\therefore\quad \chi(x)=(0,0,0,1,x_5)$$
$$y\in A_5\setminus A_1\bigcup A_2\bigcup A_3\bigcup A_4 \quad\therefore\quad \chi(y)=(0,0,0,0,1)$$

با انتخاب فوق، آنگاه طبق بند شانزدهم از قضیه (۱-۳) داریم، $\rho^*(\Gamma)\geq\frac{2}{3}$. و این با فرض مسئله تناقض دارد. در ادامه نشان می‌دهد که برای هر یک از اعداد انتخابی مانند $i,j,k\in\{1,\ldots,5\}$، یک جایگشت دلخواه مانند σ روی مجموعه $\{i,j,k\}$ وجود دارد به طوری که، $A_{\sigma(i)}\bigcap A_{\sigma(j)}=A_{\sigma(i)}\bigcap A_{\sigma(k)}$. بدون اینکه از کلیت مسئله کاسته شود فرض کنید $\{i,j,k\}=\{1,2,3\}$ و

$$\begin{cases}A_1\bigcap A_2\neq A_2\bigcap A_3\\ A_1\bigcap A_3\neq A_2\bigcap A_3.\end{cases}$$

بنابراین $A_1\bigcap A_3\subset A_2$ و $A_1\bigcap A_2\subset A_3$. در نتیجه:

$$\begin{cases}A_1\bigcap A_2\bigcap A_1\subset A_3\bigcap A_1\\ A_1\bigcap A_1\bigcap A_3\subset A_1\bigcap A_2.\end{cases}$$

و از آنجا $A_1\bigcap A_3=A_1\bigcap A_2$. و اثبات ۳ به ۴ کامل می‌شود.

برای اثبات ۴ به ۱ دو حالت در نظر یگیرید:

حالت اول: جایگشتی مانند σ روی مجموعه اعداد صحیح $\{1,\ldots,5\}$ وجود دارد به طوری که برای این اعداد تساوی زیر برقرار باشد:

$A_{\sigma(1)}\bigcap(A_{\sigma(2)}\bigcup A_{\sigma(3)}\bigcup A_{\sigma(4)}\bigcup A_{\sigma(5)})=\varnothing$. بدون کاستن از کلیت مسئله، می‌توان فرض کرد که $A_1\bigcap(A_2\bigcup A_3\bigcup A_4\bigcup A_5)=\varnothing$. با توجه به بند ۴ از قضیه ۴،۱، برای هر یک از اعداد $i,j,k\in\{2,3,4,5\}$ یک جایگشت مانند σ روی $\{i,j,k\}$ وجود دارد به‌طوری که، $A_{\sigma(i)}\bigcap A_{\sigma(j)}=A_{\sigma(i)}\bigcap A_{\sigma(k)}$. طبق لم (۲-۳) می‌توان نتیجه گرفت که $\Gamma_1=\{A_2,A_3,A_4,A_5\}$ و $\Gamma_2=\{A_1\}$ دو ساختار دسترسی فضای برداری روی میدان متناهی F هستند. بنابر نتیجه (۱-۳) ساختار دسترسی Γ یک ساختار دسترسی F- فضای برداری است.

حالت دوم: برای هر جایگشت مانند σ روی $\{1,\ldots,5\}$ داریم $A_{\sigma(1)}\bigcap(A_{\sigma(2)}\bigcup A_{\sigma(3)}\bigcup A_{\sigma(4)}\bigcup A_{\sigma(5)})\neq\varnothing$. بدون کاستن از کلیت مسئله، فرض کنیم $A_1\bigcap A_2\bigcap A_3\bigcap A_4\bigcap A_5=\varnothing$. می‌توان فرض نمود $A_1\bigcap A_4\bigcap A_5\neq\varnothing$. بنابراین به دو مجموعه $\{i,j,k,l\}=\{1,2,4,5\}$ و $\{i,j,k,l\}=\{1,3,4,5\}$ خواهیم رسید. با توجه به این دو مجموعه و فرض مسئله به نتایج $A_1\bigcap A_3=A_3\bigcap A_4$ و $A_1\bigcap A_2=A_2\bigcap A_4=A_2\bigcap A_5=\varnothing$ می‌رسیم. طبق لم (۲-۳) می‌توان نتیجه گرفت که $\Gamma_1=\{A_1,A_4,A_5\}$ و $\Gamma_2=\{A_2,A_3\}$ دو ساختار دسترسی فضای برداری روی میدان متناهی F هستند. بنابر نتیجه (۱-۳) ساختار دسترسی Γ یک ساختار دسترسی F- فضای برداری است.

در قضیه بعدی هدف ما ارائه کران بالا و پایین نرخ اطلاعات بهینه برای طرح‌های تسهیم محرمانه با ساختارهای دسترسی غیرایده‌آل با پنج زیرمجموعه مجاز مینیمال می‌باشد.

قضیه[۴-۴]: فرض کنید Γ یک ساختار دسترسی روی مجموعه شرکا P با پنج زیرمجموعه مجاز مینیمال $\Gamma_0=\{A_1,A_2,A_3,A_4,A_5\}$ باشد. اگر Γ مرتبط با یک طرح تسهیم محرمانه ایده‌آل نباشد، آنگاه $\frac{1}{2}\leq\rho^*(\Gamma)\leq\frac{2}{3}$.

اثبات: اگر Γ مرتبط با یک طرح تسهیم محرمانه ایده‌آل نباشد، آنگاه قضیه قبل نامساوی $\rho^*(\Gamma)\leq\frac{2}{3}$ را نتیجه می‌دهد. در ادامه کافی است نامساوی $\frac{1}{2}\leq\rho^*(\Gamma)$ را ثابت کنیم. فرض کنید $\Gamma_0=\{A_1,A_2,A_3,A_4,A_5\}$ یک ساختار دسترسی مینیمال باشد. حال ساختارهای دسترس‌های زیر را انتخاب می‌شود:

$$\Gamma_{0,1}=\{A_2,A_3\}\ ,\ \Gamma_{0,2}=\{A_3,A_4\}$$
$$\Gamma_{0,3}=\{A_4,A_5\}\ ,\ \Gamma_{0,4}=\{A_5,A_1\}.$$

مشاهده می‌شود $\Gamma_{0,1},\Gamma_{0,2},\Gamma_{0,3},\Gamma_{0,4}\subset\Gamma_0$ یک تجزیه از Γ است. با فرض آن‌که Γ_i یک ساختار دسترسی با پایه $\Gamma_{0,i}$ روی مجموعه $P_i=A_{i+1}\bigcup A_{i+2}\ ;\ i=1,2,3$ و $\Gamma_{0,4}$ روی مجموعه $P_4=A_1\bigcup A_5$ باشد. نتیجه (۱-۳) بیان می‌کند، برای هر میدان متناهی F، یک طرح تسهیم محرمانه ایده‌آل با ساختار دسترسی Γ_i و مجموعه محرمانه‌های K وجود دارد. بنابراین برای هر شریک $p\in\mathrm{P}$ خواهیم داشت $r_p=|\{i\in\{1,2,3,4\}\ ;\ p\in\mathrm{P}_i\}|\leq 2$، این مطلب بیان کننده این است که $\max\{r_p\ ;\ p\in\mathrm{P}\}=2$. از طرف دیگر در صورتی‌که $A\in\Gamma_0$، آنگاه $\lambda_A=|\{i\in\{1,2,3,4\}\ ;\ A\in\Gamma_{0,i}\}|\geq 1$. این نامساوی بیان می‌کند که $\min\{\lambda_A\ ;\ A\in\Gamma_0\}=1$. با استفاده از قضیه (۲-۳) نامساوی $\rho^*(\Gamma)\geq\frac{1}{2}$ را نتیجه می‌گیرید. بنابراین اگر Γ مرتبط با یک طرح تسهیم محرمانه ایده‌آل نباشد، آن‌گاه $\frac{1}{2}\leq\rho^*(\Gamma)\leq\frac{2}{3}$.

جدول ۱. بردارهای وقوعی قضیه [۱-۴]

	$\chi(a)$	$\chi(b)$	$\chi(c)$	$\chi(d)$	$\chi(x)$
۱	$(1,0,1,1,1)$	$(0,1,1,1,1)$	$(1,c_2,0,c_4,c_5)$	$(0,1,0,d_4,d_5)$	
۲	$(1,0,1,1,1)$	$(0,1,1,1,b_5)$	$(1,c_2,0,c_4,c_5)$	$(0,1,0,d_4,1)$	
۳	$(1,0,1,1,a_5)$	$(0,1,1,1,1)$	$(1,c_2,0,c_4,c_5)$	$(0,1,0,d_4,1)$	
۴	$(1,0,1,1,a_5)$	$(0,1,1,1,b_5)$	$(1,c_2,0,c_4,c_5)$	$(0,1,0,d_4,d_5)$	
۵	$(1,0,1,1,1)$	$(0,1,1,b_4,1)$	$(1,c_2,0,c_4,c_5)$	$(0,1,0,1,d_5)$	
۶	$(1,0,1,1,1)$	$(0,1,1,b_4,b_5)$	$(1,c_2,0,c_4,c_5)$	$(0,1,0,1,1)$	
۷	$(1,0,1,1,a_5)$	$(0,1,1,b_4,1)$	$(1,c_2,0,c_4,c_5)$	$(0,1,0,1,1)$	
۸	$(1,0,1,1,a_5)$	$(0,1,1,b_4,b_5)$	$(1,c_2,0,c_4,c_5)$	$(0,1,0,1,d_5)$	
۹	$(1,0,1,a_4,1)$	$(0,1,1,1,1)$	$(1,c_2,0,c_4,c_5)$	$(0,1,0,1,d_5)$	
۱۰	$(1,0,1,a_4,1)$	$(0,1,1,1,b_5)$	$(1,c_2,0,c_4,c_5)$	$(0,1,0,1,1)$	
۱۱	$(1,0,1,a_4,a_5)$	$(0,1,1,1,1)$	$(1,c_2,0,c_4,c_5)$	$(0,1,0,1,1)$	
۱۲	$(1,0,1,a_4,a_5)$	$(0,1,1,1,b_5)$	$(1,c_2,0,c_4,c_5)$	$(0,1,0,1,d_5)$	
۱۳	$(1,0,1,a_4,1)$	$(0,1,1,b_4,1)$	$(1,c_2,0,c_4,c_5)$	$(0,1,0,d_4,d_5)$	$(0,0,0,1,x_5)$
۱۴	$(1,0,1,a_4,1)$	$(0,1,1,b_4,b_5)$	$(1,c_2,0,c_4,c_5)$	$(0,1,0,d_4,1)$	$(0,0,0,1,x_5)$
۱۵	$(1,0,1,a_4,a_5)$	$(0,1,1,b_4,1)$	$(1,c_2,0,c_4,c_5)$	$(0,1,0,d_4,1)$	$(0,0,0,1,x_5)$
۱۶	$(1,0,1,a_4,a_5)$	$(0,1,1,b_4,b_5)$	$(1,c_2,0,c_4,c_5)$	$(0,1,0,d_4,d_5)$	$(0,0,0,1,x_5)$

مثال: فرض کنیم Γ یک ساختار دسترسی روی مجموعه شرکا $P=\{p_1,\ldots,p_6\}$ باشد. ساختار دسترسی مینیمال را به فرم زیر تعریف می‌شود:

$$\Gamma_0=\{\{p_1p_2p_3\},\{p_2p_3p_4\},\{p_3p_4p_5\},\{p_4p_5p_6\},\{p_1p_5p_6\}\}$$
$$A_1=\{p_1p_2p_3\},\quad A_2=\{p_2p_3p_4\},$$
$$A_3=\{p_3p_4p_5\},\quad A_4=\{p_4p_5p_6\},$$
$$A_5=\{p_1p_5p_6\}.$$

مشاهده می‌شود برای تمام مقادیر $1\le i\neq j\neq k\le 5$ عبارت $A_i\cup A_j\cup A_k\neq P$ صادق بوده و همچنین برای همه مقادیر $1\le i\neq j\neq k\neq l\le 5$ همواره تساوی $A_i\cup A_j\cup A_k\cup A_l=P$ برقرار است. به‌علاوه شرط چهارم قضیه (۲-۳) یعنی برای تمام مقادیر $1\le i\neq j\neq k\neq l\neq t\le 5$ زیرمجموعه‌های $A_i\cap A_j\cap A_k\cap A_l\subset A_t$ نیز برقرار هستند. بنابراین ساختار دسترسی فوق یک ساختار دسترسی فضای برداری بوده و $\rho^*(\Gamma)=1$. در نتیجه یک ساختار دسترسی ایده‌آل است.

۵. نتیجه‌گیری

در این مقاله دنباله مستقل را تعریف نموده و چگونگی استفاده از این روش را برای یافتن کران بالای نرخ اطلاعات یک طرح بیان شد. در ادامه برای ساختارهای دسترسی با پنج زیرمجموعه مجاز مینیمال، ارتباط بین ساختار دسترسی فضای برداری، ایده‌آل بودن طرح، میزان نرخ اطلاعات طرح و مجموعه دنباله مستقل را با ارائه چهار قضیه مهم و اساسی بیان و اثبات نموده و در صورتی که ساختار دسترسی مرتبط با یک طرح تسهیم محرمانه ایده‌آل نباشد، آنگاه کران بالا و پایین نرخ اطلاعات بهینه را به‌دست آورده شد.

۶. مراجع

[1] Anderson, R. J.; Ding, H. C. T.; Klove, T. "How to Build Robust Control Systems"; Designs, Codes and Cryptography 1998, 15, 111-124.

[2] Shamir, A. "How to Share a Secret"; Commun. ACM 1979, 2, 612-613.

[3] Blakley, G. R. "Safeguarding Cryptographic Keys"; AFIPS Conf. Proc. 1979, 48, 313-317.

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

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

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

[7] Chor, B.; Goldwasser, S.; Micali, S.; Awerbuch, B. "Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults"; Proc. FOCS 1985, 383-395.

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

[9] Padro, C.; Saez, G. "Secret Sharing Schemes with Bipartite Access Structure"; IEEE Trans. Inform Theory 2000, 46, 2596-2604.

[10] Brickell, E. F.; Davenport, D. M. "On the Classification of Ideal Secret Sharing Schemes"; J. Cryptology 1991, 4, 123-134.

[11] Dijk, M. V. "A Linear Construction of Incomplete Secret Sharing Schemes"; Designs, Code and Cryptography 1997, 12, 161-201.

[12] Jacson, W. A.; Martin, K. M. "Perfect Secret Sharing Schemes on Five Participants"; Designs, Code and Cryptography 1996, 9, 267-286.

[13] Goldreich, O.; Micali, S.; Wigderson, A. "How to Play Any Mental Game or a Completeness Theorem for Protocols with Honest Majority"; In Proc. 19th ACM Conf. on Theory of Computing, New York, NY, 1987, 218-229.

[14] Benaloh, J.; Leichter, J. "Generalized Secret Sharing and Monotone Functions"; Lecture Notes in Computer Science 1990, 403, 27-35.

[15] Farras, O.; Farre, J. M.; Padro, C. "Ideal Multipartite Secret Sharing Schemes"; Advances in Cryptology, Eurocrypt, Lecture Notes in Computer Science 2007, 4515, 448-465.

[16] Farre, J. M.; Padro, C. "Ideal Secret Sharing Schemes Whose Minimal Qualified Subset Have at Most Three participants"; Designs, Codes and Cryptography 2009, 52, 1-14.

[17] Farre, J. M.; Padro, C. "Secret Sharing Schemes with Three or Four Minimal Qualified Subsets"; Designs, Codes and Cryptography 2005, 34, 17-34.