Лекция 13

Схеми за разпределяне на секретни данни

13.1 Предварителни бележки

В практическата дейност на хората е обичайно да се изисква съгалсието на двама или повече души за одобряване на действия, които са критични в някакъв смисъл. Пример за това е регуларенето на достъпа до ядрени оръжия, където се изисква контрол от поне двама души. Естествено тази идея се обобщава до понятието (k, n)-прагова схема,въведено независимо от Blakley [7] и Shamir [53]. Целта в такива схеми е да се разпредлят някакви секретни данни, напр. ключ K, между n потребители. Всеки потребител получава част от данните. Тази част наричаме дял на съответния потребител. При това поставяме изскването дяловете на кои да е k потребителя да позволяват възстановяването на ключа K,но дяловете на никои $k-1$ от тях да не позволяват еднозначното му реконструиране. Това не изглежда особено слжно. Така например, нека имаме трима потребители P_1, P_2, P_3 и да преставим клыча K като конкатенация на три подниза с приблизително равна дължина $K = \alpha\beta\gamma$. Сега нека P_1 получи α и β, P_2 – β и γ и накрая P_3 — β и γ. Ясно е, че кои да е двама от потребителите могат да възстановят целия ключ. Ясно е също така, че никой потребител не разполага с целия ключ. Така че описаната схема е $(2, 3)$-прагова схема. Не е трудно да се забележи, че макар да не разполага с целия ключ, всеки потребител знае доста голяма част от него. Така например, за U_1 $K = \alpha\beta*$ и ако трябва да приложи груба сила P_1 би търсилключа върху много по-малко множество. Затова еприето към праговите схеми да се да поставя идопълнителното условие всяка коалиция от $k-1$ и по-малко потребители да не може да извлече *никаква* допълнителна информация за ключа. Ако например всички ключове са равновероятни, то след обединяване на дяловете на $k-1$ или по-малко потребители всички ключове трябва да продължават да изглеждат равновероятни. Схеми,притежаващи това допълнително свойство наричаме *съвършени* [61]. Сигурността, която се предоставя от такива схеми е *безусловна*,т.е. независима от изчислителните възможностина потенциалния опонент. Дори с неограничени изчислителни възможност опо-

нентът няма по-добра стратегия от това да отгатне ключа, защото е изправен пред равномерно разпределение върху всички възможни избори за K.

Често реалните приложения изискват повече възможности от тези, които предлагат (k, n)-праговите схеми. Например можем да поискаме да имаме по-сложно структуриран списък от авторизирани коалицци (т.е. по-сложна *структура на достъп*) от този,включващ просто всички k-елементни подмножества. В такъв случай говорим за *схеми за разпределяне на данни*.За конструиране на такива по-общи схеми се използват различни комбинаторни структури: Schellenberg и Stinson [52] използват комбинаторни дизайни, Stinson и Vanstone [61] – ортогонални масиви, Bloom [9], McEliece и Sarwate [43] и Yamamoto [65] – линейни блокови кодове, някои автори разглеждат схемите за разпределяне на данни в термините на матроиди [12][34]. Известно е, че всяка монотонна структура на достъп може да се реализира със съвършена схема за разпределяне на данни [5, 33].

Важен проблем, възникващ при изследването на схеми за разпределяне на данни е минимизирането на информацията, която всеки потребител получава. Съвършени схеми,при които тази информация е равна информацията, съдържаща се в ключа, наричаме минимални. Не всички монотонни структури на достъп могат да се реализират чрез идеална схема за разпределяне на данни. Brickell и Davenport [12] доказаха, че минималните авторизирани множества в идеална схема за разпределяне на данни могат да се разглевдат като множеството от циклите на матроид. От друга страна, не всеки матроид има свойството, че циклите му са минимални авторизирани множества на някаква идеална схема за разпределяне на данни.Калсификацията на всички матроиди, които могат да се реализират като иделни схеми за разпределяне на данни, е все още нерешена задача. Обширна библиография за схеми за разпределяне на данни се съдържа в обзорите [59][60].

13.2 Прагови схеми

13.2.1 Прагова схема на Shamir

Понятието (k, n)-прагова схема е въведено независимо от Blakeley [7] и Shamir [53] през 1979. Нека $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ е множеството от потребители в някаква информационна система. Съществува и още един, специален потребител D, който наричаме *дилър* и който се ползва от доверието на всички потребители. D избира по случаен начин някакъв елемент K от крайно множество от ключове $\mathcal{K}$ (най-често се приема,че всички ключове от $\mathcal{K}$ са ревновероятни. Задачата не D е да разпределипонякакъв начин K между потребителите от $\mathcal{P}$, давайки на всекиот тях някаква частична информация за $\mathcal{K}$,която наричаме *дял* на съответния потребител. Дяловете се разпределят тайни, така че никой потребител не знае нищо за дяловете на другите потребители. В по-късен момент някаво подмножество от потребители $B \subset \mathcal{P}$ обединяват дяловете си в опит да пресметнат тайния ключ K. Ако $|B| \geq k$, където k е някакво естествено число, те трябва да могат да възстановят K; ако $|B| < k$ те нетрябва да са в състояние да пресметнат K. Това оправдава следната дефиниция.

Дефиниция 13.1. Нека $\mathcal{K}$ е крайно множество от ключове и нека K е фиксиран елемент от $\mathcal{K}$. (k, n)-прагова схема наричаме всеки метод за създаване на множество

от дялове $C = \{c_1, c_2, \ldots, c_n\}$ от n елемента от множество $\mathcal{S}$ (множество на дяловете), така че да са изпълнени условията:

(T1) Тайният ключ K се определя еднозначно от кои да е k елемента на C.

(T2) Тайният ключ K не мохзе да се възстанови от никои $k-1$ (или по-малко) елемента от C.

Понякога (T2) се заменя с по-силното условие:

(T2′) Знанието на $k-1$ или по-малко елемнта от C не разкрива никаква информация за K.

Една (k,n)-прагова схема,изпълняваща (T2′) наричаме *съвършена.*

По-нататък ще направим тази дефиниция по-строга.

Конструкцията по-долу е предложена от Shamir [53]. Нека k и n, $k \leq n$, са естествени числа, а $q = p^s$ е степен на просто число. Нека $\mathcal{K} = \mathcal{S} = \mathbb{F}_q$. Нека K е тайната информация, която се разпределя между участниците в системата $P_1, \ldots, P_n$. Дилърът D избира по случаен начин и независимо $k-1$ елемента $a_0, a_1, \ldots, a_{k-1}$ от $\mathbb{F}_q$, $a_{k-1} \neq 0$, и образува полинома

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1},$$

където $a_0 = K$. D пресмята $y_i = f(x_i)$ за n различни стойности $x_i \in \mathbb{F}_q$ и разпределя дяловете $c_i = (x_i, y_i)$, $i = 1, 2, \ldots, n$, т.е. $C = \{c_i | i = 1, 2, \ldots, n\}$ и P_i получава c_i. да отбележим, еч няма нужда да пазимв тайна стойностите x_i и те може да са публични. Така единствената информация,коыто се изпраща тайно са елементите y_i.

Теорема 13.2. *Схемата на Шамир е съвършена (k,n)-прагова схема.*

Proof. Нека са известни k двойки $(x_{i_j}, y_{i_j}), j = 1, 2, \ldots, k$. Тогава $f(x)$ може да се възстанови от интерполационната полином на Лагранж

$$f(x) = \sum_{j=1}^{k} y_{i_j} \prod_{l \neq j} \frac{x - x_{i_l}}{x_{i_j} - x_{i_l}}.$$

Очевидно $K = a_0 = f(0)$, т.е. в сила е (T1). Бихме могли и направо да пресметнем K от формулата

$$K = f(0) = \sum_{j=1}^{k} y_{i_j} \prod_{l \neq j} \frac{-x_{i_l}}{x_{i_j} - x_{i_l}}.$$

Да допуснем, че са известни двойките $(x_{i_j}, y_{i_j}), j = 1, \ldots, l, l < k$. Очевидно е изпълнено

$$\left|\begin{array}{ccccccccc} y_{i_1} & = & K & + & a_1 x_{i_1} & + & \ldots & + & a_{k-1} x_{i_1}^{k-1} \\ y_{i_2} & = & K & + & a_1 x_{i_2} & + & \ldots & + & a_{k-1} x_{i_2}^{k-1} \\ \vdots & & \vdots & & & & \ddots & & \vdots \\ y_{i_l} & = & K & + & a_1 x_{i_l} & + & \ldots & + & a_{k-1} x_{i_l}^{k-1} \end{array}\right. \tag{13.1}$$

За всеки избор $K = \alpha \in \mathbb{F}_q$ (13.1) е система от l уравнения с $k-1$ неизвестни: $a_1, \ldots, a_{k-1}$. Ясно е че матрицата от коефициентите пред $a_1, \ldots, a_l$ е матрица на Вандермонд. Така броят на решенията на системата е q^{k-l-1}, т.е. за всяко $\alpha \in \mathbb{F}_q$ съществуват точно q^{k-l-1} полинома $f(x)$, които удовлетворяват $y_{i_j} = f(x_{i_j}), j = 1, \ldots, l$, $f(0) = \alpha$. Следователно всички възможности за α са равновероятни и произволна коалиция от $l < k$ потребителя не може да получи допълнителна информация от споделянето на дяловете си. Това доказва (T2′). □ □

Пример 13.3.

13.2.2 Модификацията на McEliece и Sarwate

McEliece и Sarwate [43] предефинират схемата на Shamir в термините на разширените кодове на Рид-Соломон. Нека $\alpha_1, \alpha_2, \ldots, \alpha_{q-1}$ са ненулевите елементи на $\mathbb{F}_q$. Кодовът на Рид-Соломон с параметри $[q-1, k]_q$ съдържа всички думи $\boldsymbol{c} = (c_1, c_2, \ldots, c_{q-1})$, за които $c_i = \sum_{j=0}^{k-1} a_j \alpha_i^j$. Тук $\boldsymbol{a} = (a_0, a_1, \ldots, a_{k-1}), a_i \in \mathbb{F}_q$, пробягва всички k-орки от $\mathbb{F}_q^k$. Разширеният код на Рид-Соломон е $[q, k]_q$-код с кодови думи от вида $(c_0, c_1, \ldots, c_{q-1})$, където последните $q-1$ компоненти образуват дума от кода на Рид-Соломон, а $c_0 = -\sum_{i=1}^{q-1} c_i$ е проверка по четност.

В модификацията на McEliece иSarwate се приема, че $\mathcal{K} = \mathcal{S} = \mathbb{F}_q$, $q > n$. Дилърът фиксира резширен код на Рид-Соломон $\mathcal{C}$, определя координатна позиция за всеки потребител (да речем i-тата позиция се асоциира с потребителя P_i), оставяйки една позиция (нулевата) за себе си. По-нататък той избира по случаен начин кодова дума $(c_0, c_1, c_2, \ldots, c_{q-1}) \in \mathcal{C}$ с $K = c_0$ и разпределя компонентите на избраната кодова дума на потребителите от $\mathcal{P}$. Поспециално, P_i получава c_i.

Едно добре известно свойство на разширените кодове на Рид-Соломон (както и на всички MDS-кодове) е, че кои да еk координатни позиции са информационни. С други думи кои да е k стълба в коя да е пораждаща матрица на MDS-код са линейно независими. При зададени k дяла c_{i_j} е възможно да се възстанови по единствен начин кодова дума от разширения код на Рид-Соломон,която има c_{i_j} в i_j-тата си позиция. Това възстановява тайния ключ. Ако са известни $l < k$ дяла c_{i_j}, то за всяко $\alpha \in \mathbb{F}_q$ съществуват точно q^{k-l-1} кодови думи от $\mathcal{C}$, за които α е в нулевата позиция, а елементите c_{i_j} са в i_j-та позиция, $j = 1, \ldots, l$. Следователно всички елементи от $\mathcal{K}$ са равновероятни кандидати за таен ключ. Така доказахме следната теорема.

Теорема 13.4. *Модифицираната* схема на McEliece *и* Sarwate *е съвършена* (k, n)-*прагова схема.*

Не е трудно да се покаже, че схемите на Shamir иMcEliece-Sarwate са еквивалентни. Въпреки това използването на кодове ни дава някои предимства. Да допуснем, че някои от участниците са лъжци, т.е. по някаква причина те споделят грешен дял. Дори при това условие схемата на McEliece-Sarwate може да работи коректно.

Теорема 13.5. *Нека в схемата на* McEliece-Sarwate *s участници споделят дяловете си и нека t от дяловете са некоректни. Ако* $s \geq k + 2t$,*то тайният ключ може да бъде реконструиран ефективно.*

Доказателство. Известен е алгоритъм за декодиране на кодовете на Рид-Соломон, който позволява поправяне на t грешки и r изтривания, ако $2t+r \leq d-1 = n-k$ [6][62]. Неизвестните $n-s$ координатимогат да бъдат разгледани като $n-s$ изтривания,а грешните t дяла–като t грешки. Декодиращият алгоритъм възстановява $(c_1, c_2, \ldots, c_n)$,ако $2t+(n-s) \leq n-k$, т.е. $s \geq k+2t$. Щом определим $c_1, \ldots, c_n$,лесно възстановяваме и K. □

13.2.3 Прагова схема основана на Китайската теорема за остатъците

Ще опишем прагова схема,предложена от Asmuth и Bloom [4]. Нека $m_1, m_2, \ldots, m_n$ са цели ползохителни числа, за които $\gcd(m_i, m_j) = 1$ за $i \neq j$, и нека $c_1, c_n \ldots, c_n$ са цели числа, удовлетворяващи $0 \leq c_i < m_i, i = 1, 2, \ldots, n$. Да положим $M = m_1 m_2 \ldots m_n$ и $M_i = M/m_i$. Нека по-нататък N_i е единственото решение на сравнението $M_i x \equiv 1 \pmod{m_i}$. Системата

$$x \equiv c_i \pmod{m_i}, i = 1, 2, \ldots, n,$$

има единствено решение помодул M, което е $x = \sum_{i=1}^{n} c_i M_i N_i$.

Нека k е цяло число, за което $1 < k \leq n$. Да означим

$$\min(k) = \min\{m_{i_1} m_{i_2} \ldots m_{i_k} | i_1 < i_2 \ldots < i_k\},$$

$$\max(k) = \max\{m_{i_1} m_{i_2} \ldots m_{i_k} | i_1 < i_2 \ldots < i_k\}.$$

Нека числата $m_1, \ldots, m_n$ са избрани по такъв начин, че разликата $\min(k) - \max(k-1)$ е "достатъчно голяма". Интуитивно ясно е, че това се случва, когато числата $m_1, \ldots, m_n$ са близки едно до друго.Да положим $\mathcal{K} = \{s \in \mathbb{Z} | \max(k-1) < s < \min(k)\}$, $\mathcal{S} = \{s \in \mathbb{Z} | 0 < s < \max_{1 \leq i \leq n} m_i\}$ и нека i-тият потребител получава като свой дял $c_i \equiv K \pmod{m_i}, i = 1, 2, \ldots, n$, т.е. $C = \{(c_1, c_2, \ldots, c_n) | c_i \equiv K \pmod{m_i}, K \in \mathcal{K}\}$.

Теорема 13.6. *При горните условия, описаната схема е несъвършена (k, n)-прагова схема.*

Доказателство. да допуснем, че числата $c_{i_j}, j = 1, \ldots, k$, са известни. Възможно е да се пресметне $M' = \Pi_{j=1}^{k} m_{i_j}$, $M'_j = M'/m_{i_j}$,катои решението N'_j на $M'_j x \equiv 1 \pmod{m_{i_j}}$. Тогава $y_0 = \sum_{j=1}^{k} c_{i_j} M'_j N'_j$ ис а е решение на системата

$$x \equiv c_{i_j} \pmod{m_{i_j}}, j = 1, 2, \ldots, k.$$

Очевидно, ако K е друго решение на тази система имаме $y_0 \equiv K \pmod{M'}$. Тъй като $K < \min(k) < M'$, можем да определим K от $K = y_0 \pmod{M'}$.

Да допуснем, че $c_{i_1}, \ldots, c_{i_{k-1}}$ са известни. Както и по-горе, да намерим решение y_1 на $x \equiv c_{i_j} \pmod{m_{i_j}}, j = 1, \ldots, k-1$. Отново имаме $y_1 \equiv K \pmod{m_{i_1} \ldots m_{i_{k-1}}}$, т.е. $K = y_1 + A m_{i_1} \ldots m_{i_{k-1}}$. Това води до поне

$$\frac{\min(k) - \max(k-1) - 1}{m_{i_1} m_{i_2} \ldots m_{i_{k-1}}}$$

възможности за K. Ние имаме поне $\min(k) - \max(k-1)$ кандидати за K, откъдето следва, че схемата е несъвършена. □

M. Mignotte [45] доказа, че горните схеми могат да се получат като специални случаи на по-обща конструкция, използващаКитайската теорема за остатъците за произволен комутативен пръстен с единица.

13.3 Линейни кодове и схеми за разпределяне на данни

13.3.1 Структури на достъп

Ще започнемс обобщение на понятието прагова схема. Както по-горе нека $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ е множеството от потребителите на някаква информационна система. Всяко множество Γ от подмножества на $\mathcal{P}$, $\Gamma \in 2^{\mathcal{P}}$, наричаме структура на достъп. Нека Γ е произволна структура на достъп и нека ис $\mathcal{K}$ и $\mathcal{S}$ са произволни множества, които ще наричаме съответно *множество от ключове* и *множество от дялове*.

Дефиниция 13.7. *Схема за рапредляне на данни, реализираща структурата на достъп* Γ наричаме всеки метод за създаване на множество $C(K) = \{c_1, c_2, \ldots, c_n\}$, $c_i \in \mathcal{S}$, $K \in \mathcal{K}$,за което са в сила условията:

(S1) Ключът K може да бъде ефективно възстановен от всяко множество от дялове $\{c_i | i \in B\}$, $B \in \Gamma$.

(S2) Ключът K не може да бъде възстановен от никое множество от дялове $\{c_i | i \in B\}, B \notin \Gamma$.

Една схема за разпределяне на данни наричамее *съвършена*, ако вместо (S2) се изпълнява по-силното условие

(S2′) Дяловете $\{c_i | i \in B\}, B \notin \Gamma$ не разкриват никаква информация за ключа K.

Множествата $B \in \Gamma$ (съотв. $B \notin \Gamma$) наричаме *авторизирани* (съотв. *неавторизирани*) множества. Елементите на Γ описват онезикоалиции от потребители, които могат да възстановят ключа като обединят дяловете си. Множеството от всички неавторизирани коалиции означаваме с $\overline{\Gamma}$, и.е. $\overline{\Gamma} = 2^{\mathcal{P}} \setminus \Gamma$. естествено е да предположим, че ако някаво множество от потребители B е авторизирано, то и всяко множество,съдържащо B, също е такова. Формално ще изкаме Γ да има следното свойство:

$$\text{ако} \quad B \in \Gamma \quad \text{и} \quad B \subset B' \subset \mathcal{P} \quad \text{то} \quad B' \in \Gamma. \tag{13.2}$$

Структура на достъп, удовлетворяваща (13.2) наричаме *монотонна*. По-нататък ще разглеждаме само монотонни структури на достъп. Две структури на достъп наричаме *еквивалентни*, ако те са изоморфни като структури на инцидентност.

Нека Γ е монотонна структура на достъп. Едно множество $B \in \Gamma$, имащо свойството

$$\forall B' \in \mathcal{P}: \quad \mathcal{P} \supset B' \supset B \quad \Rightarrow \quad B' \in \Gamma$$

наричаме *минимално множество* в Γ. Аналогично едно множество $B \in \overline{\Gamma}$ със свойството

$$\forall B' \in \mathcal{P}: \quad \mathcal{P} \supset B' \supset B \quad \Rightarrow \quad B' \in \Gamma$$

наричаме *максимално множество* в $\overline{\Gamma}$. Множеството от всички минимални множества в Γ (съотв. всички максималнимножества в $\overline{\Gamma}$) означаваме с $\Gamma_{\min}$ (съотв. $\overline{\Gamma}_{\max}$).

Да свържем с всеки потребител P_i променлива x_i. Нека е дадена монотонна структура на достъп Γ. Дефинираме формална дизюнкция $\gamma = \bigvee_{B \in \Gamma_{\min}} \gamma_B$, където $B = \{P_{i_1}, \ldots, P_{i_s}\}$ и $\gamma_B = x_{i_1} \wedge \ldots \wedge x_{i_s}$. Обратно, всяка дизюнкция, несъдържаща

двойка елементарни конюнкции от вида $x_{i_1} \dots x_{i_s}$ и $x_{i_1} \dots x_{i_s} x_{i_s+1} \dots x_{i_t}$, описва множеството от минималните множества на някава структура на достъп Γ. Да дефинираме

$$\gamma^* = \bigwedge_B (x_{i_1} \vee \dots \vee x_{i_s}).$$

Тук $B = \{P_{i_1}, \dots, P_{i_s}\}$ пробягва $\Gamma_{\min}$. Структурата на достъп, свързана с израза (**??**) наричаме дуална структура на Γ и означаваме с Γ. (Изразът (**??**) се упростява използвайкиобичайните правила $x \wedge x = x$, $x \vee x = x$ $x \vee (x \wedge y) = x$.)

Теорема 13.8. Нека Γ е монотонна структура на достъп и нека Γ^* е дуалната структура на Γ. Тогава за всяко $\{P_{i_1}, P_{i_2}, \dots, P_{i_s}\} \in \Gamma^*_{\min}$ множеството $\mathcal{P} \setminus \{P_{i_1}, P_{i_2}, \dots, P_{i_s}\}$ принадлежи на $\overline{\Gamma}_{\max}$ и всички максимални множества се получават по този начин.

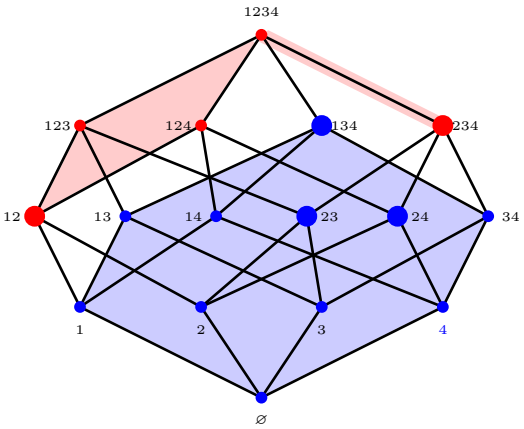
Пример 13.9. Нека $\Gamma_{\min} = \{\{P_1, P_2\}, \{P_2, P_3, P_4\}\}$. Сега имаме

$$\gamma = (x_1 \wedge x_2) \vee (x_2 \wedge x_3 \wedge x_4).$$

За γ^* получаваме

$$\begin{aligned} \gamma^* &= (x_1 \vee x_2) \wedge (x_2 \vee x_3 \vee x_4) \\ &= (x_1 \wedge x_2) \vee x_2 \vee (x_1 \wedge x_3) \vee (x_2 \wedge x_3) \vee (x_1 \wedge x_4) \vee (x_2 \wedge x_4) \\ &= x_2 \vee (x_1 \wedge x_3) \vee (x_1 \wedge x_4). \end{aligned}$$

Така получаваме $\overline{\Gamma}_{\max} = \{\{P_2\}, \{P_1, P_3\}, \{P-1, P_4\}\}$.



13.3.2 Схеми за разпределяни на данни и линейни кодове

Конструкцията от раздел 13.2.2 може да се обобщи за кодове над произволни крайни полета. Нека $\mathbb{F}_q$ е крайно поле и да положим $\mathcal{K} = \mathcal{S} = \mathbb{F}_q$. Дилърът фиксира линеен $[n+1, k]_q$-код $\mathcal{C}$ с пораждаща матрица $\boldsymbol{G}_{\mathcal{C}} = [\boldsymbol{g}_0^t, \boldsymbol{g}_1^t, \dots, \boldsymbol{g}_n^t]$, $\boldsymbol{g}_i \in \mathbb{F}_q^k$. Матрицата $vek G_{\mathcal{C}}$ е публична.Всеки участник $P_i \in \mathcal{P}$ получава стълб в матрицата $\boldsymbol{G}_{\mathcal{C}}$.

Един стълб, да кажем нулевия, е определен за дилъра. Малкопо-обща конструкция можем да получим, ако потрбителите и дилърът получават множества от стълбове. По-нататък ще използваме такова обобщение. Засега оставаме с ограничението, че всички дялове са с един и същи размер. Дилърът избира случаен вектор $\boldsymbol{a} = (a_0, a_1, \ldots, a_{k-1}) \in \mathbb{F}_q^k$, който се пази в тайна.тайният ключ е $K = \boldsymbol{a}\boldsymbol{g}_0^t$, а дялът на P_i е $c_i = \boldsymbol{a}\boldsymbol{g}_i^t$.

Нека $\mathcal{C}$ е линеен код с пораждаща матрица $\boldsymbol{G}_{\mathcal{C}} = \left[\boldsymbol{g}_0^t, \boldsymbol{g}_1^t, \ldots, \boldsymbol{g}_{n-1}^t\right]$.Дефинираме структурата на достъп $\Gamma(\mathcal{C})$ чрез

$$B = \{P_{i_1}, P_{i_2}, \ldots, P_{i_s}\} \in \Gamma(\mathcal{C}) \;\; \Leftrightarrow \;\; \boldsymbol{g}_0 \in \langle \boldsymbol{g}_{i_1}, \boldsymbol{g}_{i_2}, \ldots, \boldsymbol{g}_{i_s} \rangle.$$

Структурата на достъп $\Gamma(\mathcal{C})$ не зависи от избора на $\boldsymbol{G}_{\mathcal{C}}$.

Теорема 13.10. *Описаната схема е съвършена схема за разпределяне на данни, реализираща структурата на достъп* $\Gamma(\mathcal{C})$.

Доказателство. Да допуснем, че $B = \{P_{i_1}, \ldots, P_{i_s}\}$ е авторизирано множество. Това означава, че ако две кодови думи съв пада т в координатните позиции с номера i_1, i_2, $\ldots$, i_s,то те съвпадат и в нулевата си позиция. С други думи, от

$$\boldsymbol{a}\left[\boldsymbol{g}_{i_1}^t \ldots \boldsymbol{g}_{i_s}^t\right] = \boldsymbol{b}\left[\boldsymbol{g}_{i_1}^t \ldots \boldsymbol{g}_{i_s}^t\right]$$

следва, че $\boldsymbol{a}\boldsymbol{g}_0^t = \boldsymbol{b}\boldsymbol{g}_0^t$. Следователно всяко решение на системата $\boldsymbol{x}\left[\boldsymbol{g}_{i_1}^t \ldots \boldsymbol{g}_{i_s}^t\right] = \boldsymbol{0}$ е rexenie i na $\boldsymbol{x}\left[\boldsymbol{g}_0^t, \boldsymbol{g}_{i_1}^t \ldots \boldsymbol{g}_{i_s}^t\right] = \boldsymbol{0}$. Taka $\mathrm{rk}\left[\boldsymbol{g}_0^t, \boldsymbol{g}_{i_1}^t \ldots \boldsymbol{g}_{i_s}^t\right] = \mathrm{rk}\left[\boldsymbol{g}_{i_1}^t \ldots \boldsymbol{g}_{i_s}^t\right]$ i $\boldsymbol{g}_0 \in \langle \boldsymbol{g}_{i_1}, \ldots, \boldsymbol{g}_{i_s} \rangle$.

Нека $\boldsymbol{g}_0 \in \langle \boldsymbol{g}_{i_1}, \ldots, \boldsymbol{g}_{i_s} \rangle$. Тогава $\boldsymbol{g}_0 = \mu_1 \boldsymbol{g}_{i_1} + \mu_2 \boldsymbol{g}_{i_2} + \ldots + \mu_s \boldsymbol{g}_{i_s}$, където $\mu_i \in \mathbb{F}_q$. Оттук

$$\begin{aligned} K = \boldsymbol{a}\boldsymbol{g}_0^t &= \mu_1 \boldsymbol{a}\boldsymbol{g}_{i_1}^t + \mu_2 \boldsymbol{a}\boldsymbol{g}_{i_2}^t + \ldots + \mu_t \boldsymbol{a}\boldsymbol{g}_{i_t}^t \\ &= \mu_1 c_{i_1} + \mu_2 c_{i_2} + \ldots + \mu_t c_{i_t}. \end{aligned}$$

Тъй като $\boldsymbol{G}_{\mathcal{C}}$ е публична, потребителите могат да пресметнат коефициентите μ_i, а следователно и K. Сега да допуснем, че $B = \{P_{i_1}, \ldots, P_{i_t}\} \notin \Gamma(\mathcal{C})$, т.е. $\boldsymbol{g}_0 \notin \langle \boldsymbol{g}_{i_1}, \ldots, \boldsymbol{g}_{i_t} \rangle$. Нека по-нататък $k' = \dim\langle \boldsymbol{g}_0, \boldsymbol{g}_{i_1}, \ldots, \boldsymbol{g}_{i_t} \rangle$. За всяко $\alpha \in \mathbb{F}_q$ съществуват точно $q^{k-k'} \geq 1$ решения $\boldsymbol{a}$ на системата

$$\left| \begin{array}{rcl} \boldsymbol{a}\boldsymbol{g}_0^t & = & \alpha \\ \boldsymbol{a}\boldsymbol{g}_{i_j} & = & c_{i_j}, j = 1, 2, \ldots, t. \end{array} \right.$$

Така всички елементи от $\mathbb{F}_q$ се равновероятни кандидати за тайния ключ K и схемата е съвършена. □

Ще казваме, че векторът $\boldsymbol{c}' = (c_0', c_1', \ldots, c_n') \in \mathbb{F}_q^{n+1}$ покрива вектора $\boldsymbol{c} = (c_0, c_1, \ldots, c_n)$, ако за всяко i от $c_i \neq 0$ следва $c_i' \neq 0$. Една кодова дума от линйния код $\mathcal{C}$ наричаме *минимална*, ако тя покрива само нумевата дума в $\mathcal{C}$. Множеството от всички минимални думи наричаме *проекционно множество* за кода и означаваме с $\mathcal{C}_{\min}$.

Теорема 13.11. *Множеството* $\Gamma_{\min}(\mathcal{C})$ *съвпада с носителите на минималните думи* $\boldsymbol{C} = (c_0, c_1, \ldots, c_n)$ *от* $\mathcal{C}^{\perp}$, *за които* $c_0 \neq 0$. *coordinate.*

Proof. Да допуснем, че $B = \{P_1, \ldots, P_s\} \in \Gamma_{\min}(\mathcal{C})$, т.е. $\boldsymbol{g}_0 \in \langle \boldsymbol{g}_1, \ldots, \boldsymbol{g}_s \rangle$. Съществуват елементи $\mu_i \in \mathbb{F}_q$, за които

$$\boldsymbol{g}_0 = \mu_1 \boldsymbol{g}_1 + \mu_2 \boldsymbol{g}_2 + \ldots + \mu_s \boldsymbol{g}_s.$$

Тук потребителите в авторизирано множество B са взети за улеснение с последователни индекси. От горното равенство следва, че $\boldsymbol{c} = (1, -\overline{\mu_1}, -\overline{\mu_2}, \ldots, -\overline{\mu_s}, 0, \ldots, 0)$ е кодова дума от $\mathcal{C}^\perp$ с ненулева най-лява координата. Думата $\boldsymbol{c}$ е минимална,тъй като множеството B е минимално. По подобен начин, ако $\boldsymbol{c} = (1, -\overline{\mu}_1, -\overline{\mu}_2, \ldots, -\overline{\mu}_s, 0, \ldots, 0) \in \mathcal{C}^\perp_{\min}$, то $B = \{P_1, P_2, \ldots, P_s\} \in \Gamma_{\min}(\mathcal{C})$. □

Теорема 13.12. $\Gamma^*(\mathcal{C}) = \Gamma(\mathcal{C}^\perp)$.

Доказателство. Нека $B \in \Gamma^*_{\min}(\mathcal{C})$. Съгласно Теорема **??** съществува множество $B' \in \overline{\Gamma}_{\max}(\mathcal{C})$, за което $B' = \mathcal{P} \setminus B$. Следователно

$$\operatorname{rk} \boldsymbol{G}_{\mathcal{C}}[B' \cup \{0\}] = \operatorname{rk} \boldsymbol{G}_{\mathcal{C}}[B'] + 1.$$

Ясно е, че $\operatorname{rk} \boldsymbol{H}_{\mathcal{C}}[J \setminus \{B' \cup \{0\}\}] = \operatorname{rk} \boldsymbol{H}_{\mathcal{C}}[J \setminus B']$ и $\operatorname{rk} \boldsymbol{H}_{\mathcal{C}}[B \cup \{0\}] = \operatorname{rk} \boldsymbol{H}_{\mathcal{C}}[B]$. Това означава, че нулевия стълб на пораждащата матрица на $\mathcal{C}^\perp$ елинейна комбинация на стълбове, индексирани с елементите на B, т.е. $B \in \Gamma(\mathcal{C}^\perp)$. Всъщност от $B' \in \overline{\Gamma}_{\max}(\mathcal{C})$ следва $B \in \Gamma_{\min}(\mathcal{C}^\perp)$, което завършва доказателството. □

По-горе доказахме, че проекционното множество на линеен код описва структурата на достъп на някаква схема за разпределяне на данни. В този смисъле важно да се определи $\mathcal{C}_{\min}$ за различни класове от линейникодове. Любопитно е, че понятието проекционно множество възниква и във връзка със задачата за декодиране на различни класове линейни кодове. фор дифферент цлассес оф линеар [17][31][46]. Тази задача се разглежда най-вече за двоични кодове [3][11]. Следната теорема е формулирана в [3], но частиот нея могат да бъдат намерени и в [31] и [41].

Теорема 13.13. *Let $\mathcal{C}$ be an $[n, k, d]_q$ code and let $\mathbf{H}_{\mathcal{C}}$ be a parity check matrix of $\mathcal{C}$.*

(a) Кодовата дума $\boldsymbol{c} \in \mathcal{C}$ е минимална тогава и само тогава, когато рангът на $\boldsymbol{H}_{\mathcal{C}}$, ограничена върху ненулевите позиции на $\boldsymbol{c}$ е $w_{\mathrm{Ham}}(\boldsymbol{c}) - 1$.

(b) Ако $\boldsymbol{c}_1 \in \mathcal{C}_{\min}$ и носителите на кодовите думи $\boldsymbol{c}_1$ и $\boldsymbol{c}_2$ съвпадат, то $\boldsymbol{c}_1$ и $\boldsymbol{c}_2$ са скаларни кратни.

(c) От $\boldsymbol{c} \in \mathcal{C}_{\min}$ следва $w_{\mathrm{Ham}}(\boldsymbol{c}) \leq n - k + 1$.

(d) В случая на двоични кодове всяка кодова дума $\boldsymbol{c} \in \mathcal{C}$ с $w_{\mathrm{Ham}}(\boldsymbol{c}) \leq 2d - 1$ е минимална.

(e) $\mathcal{C}_{\min}$ поражда $\mathcal{C}$.

Линейни кодове, за които $\mathcal{C}_{\min} = \mathcal{C} \setminus \{\mathbf{0}\}$ се наричат кодове с пресичане. Кодове с пресичане съществуват. Така например, ортогоналния код на двоичния БЧХ-код с дължина $2^m - 1$ и конструктивно разстояние $d = 2t - 1$, където $t < \frac{1}{3} 2^{\frac{m}{2}-1}$, е код с пресичане [3][17].

За някои класове от кодове е относително лесно да се определи множеството от минималните думи. Съгласно Теорема 13.13, множеството от минималните кодови думи на $[n, k]_q$ MDS-код се състои от всички $\binom{n}{k-1}$ думи с минимално тегло. По подобен начин проекционното множество на $[n, k]_q$ почти-MDS код се състои от всички думи с тегло $n - k$ и $n - k + 1$.

13.3.3 Схеми за достъп за монотонни структури

От криптографска гледна точка по-естествен е случаят, когато структурата на достъп е предварително зададена и целта е да се построи схема, реализираща Γ. за решениетона тази задача използваме модификация на конструкцията от раздел ?? като позволяваме на всеки участник да притежава като дялповече от една координатна позиция.

Теорема 13.14. *Всяка монотонна структура на достъп γ може да бъде реализирана чрез съвършена чрез съвършена* схема за разпределяне на данни.

Доказателство. Let us start by noting that the secret sharing scheme from a linear code with generator matrix $\mathbf{G} = [\mathbf{e}_m^t | \mathbf{I}_m]$, where $\mathbf{e}_m$ is the m-dimensional all-one vector and $\mathbf{I}_m$ is the identity matrix of order m, is a (m, m)-threshold scheme.

Set $m = |\overline{\Gamma}_{\max}|$ and consider an (m, m)-threshold scheme defined by the $[m+1, m]_q$ code $\mathcal{C}$ with generator matrix $\mathbf{G} = [\mathbf{e}_m^t | \mathbf{I}_m]$. Index the coordinate positions by $0, 1, \ldots, m$ and assign a position to each set $B_i \in \overline{\Gamma}_{\max}$, $i = 1, 2, \ldots, m$. For each participant P_i define the set of indices $I_i = \{l | P_i \notin B_l\}$. Each participant P_i receives as his share the elements $\{c_l | l \in I_i\}$. The secret key K and the c_i's are the same as in section 2.2. We are going to prove that the scheme defined in this way is a perfect secret sharing scheme realizing Γ.

Let $B_j \in \overline{\Gamma}_{\max}$. This means that the index j is not contained in $\mathcal{J}_j = \cup_{\{s: P_s \in B_j\}} I_s$, i.e. $|\mathcal{J}_j| < m$ and the shares of the participants in B_j, $\{c_\alpha | \alpha \in \mathcal{J}_j\}$ are not enough to determine the secret.

Let $B = \{P_{i_1}, P_{i_2} \ldots, P_{i_s}\} \in \Gamma$. Then B is not a subset of any set in $\overline{\Gamma}_{\max}$. This means that $B \setminus B_i \neq \emptyset$ for all $i \in \{1, 2, \ldots, m\}$. For any i there is at least one $j \in \{i_1, i_2, \ldots, i_s\}$ with $i \in I_j$. Hence $|\cup_{j: P_j \in B} I_j| = m$ and all users from B are able to determine the secret.

Схемата,която конструирахме е съвършена, тъй като (m, m)-праговата схема, с която започнахме е съвършена.

Пример 13.15. Нека $\Gamma_{\min} = \{P_1P_2, P_1P_3P_4, P_2P_3P_4\}$. Тогава

$$\overline{\Gamma}_{\max} = \{P_1P_3, P_1P_4, P_2P_3, P_2P_4, P_3P_4\}.$$

Да допуснем, че дилърът е избрал $[6, 5, 2]_4$-код и е фиксирал кодовата дума $(\alpha, 1, \alpha, \alpha^2, 1, \alpha^2)$, т.е. $c_0 = K = \alpha, c_1 = 1, c_2 = \alpha, c_3 = \alpha^2, c_4 = 1, c_5 = \alpha^2$. Сега $I_1 = \{3, 4, 5\}, I_2 = \{1, 2, 5\}, I_3 = \{2, 4\}, I_4 = \{1, 3\}$. P_1 получава дяловете c_3, c_4, c_5, P_2 – дяловете c_1, c_2, c_5, P_3 – дяловете c_2, c_4, а P_4 – дяловете. c_1, c_3. Съгласно теорема 13.14 конструираната схема е съвършена и редлизира Γ. implements Γ.

13.3.4 Геометричният подход на Simmons

В своя обзор [59] Г. Симмонс разглежда два общи геометрични модала за разпределяне на данни. Първият може да се разглежда като обобщение на оригиналната схема на Blakley. Да разгледаме проективното пространство $\mathrm{PG}(k-1, q)$ и нека $\mathcal{K}$ съвпада с точките на $\mathrm{PG}(k-1, q)$. Тайният ключ K е случайно избрана точка от $\mathcal{K}$. Дяловете са подпространства от $\mathrm{PG}(k-1, q)$, например нека P_i получава подпространството π_i. Подпространствата π_i се избират по такъв начин, че $B = \{P_{i_1}, P_{i_2}, \ldots, P_{i_s}\} \in \Gamma$ тогава и само тогава, когато $\cap_{j: P_{i_j} \in B} \pi_{i_j} = K$. Тхази конструкция очевидно дава несършени схеми.

Във тория модел $\mathcal{K} = V_D$ е някакво множество от точки (многообразие) в PG$(k-1, q)$. Всеки потребител получава като дял точка или точки от друго случайно избрано множество от точки (многообразие) V_I, което пресича V_D в единствена точка – тайния ключ K. Дяловете се разпределят по такъв начин, че V_I може да се реконструира самоот авторизирано множество от потребители. Многообразието V_D може да се публикува, докато V_I е тайно. Схемата на Shamir може да се разглежда като специален случай на този модел. Подробно описание на двата модела се съдържа в [59].

13.4 Матроиди и схеми за резпределяне на данни

13.4.1 Обща дефиниция

Нека $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ е крайно множество, идентифицирано с участниците в някаква информационна система и нека $\Gamma \subset 2^{\mathcal{P}}$ е структура на достъп. Да означим $\mathcal{P}' = \mathcal{P} \cup \{D\}$, където D е произволен елемент,който не принадлежи на $\mathcal{P}$ (D се идентифицира с дилъра). Нека по-нататък $\mathcal{F} = \{f : \mathcal{P}' \to \mathcal{S}\}$ е множествато от функции, които наричаме *правила за разпределяне на дяловете* и които приемат стойности в някакво множество $\mathcal{S}$. Да означимс с $\mathcal{K} = \{f(D) | f \in \mathcal{F}\}$ (множеството от тайните ключове) и $\mathcal{S}_i = \{f(P_i) | f \in \mathcal{F}\}$ (множеството от дяловете, които получава P_i).

Дефиниция 13.16. Двойката $\langle \Gamma, \mathcal{F} \rangle$ наричаме *схема за разпределяне на данни, реализираща структурата на достъп* Γ, ако са изпълнени следните условия:

(SS1) За всяко $B \in \Gamma$ и всяка двойка от функции $f_1, f_2 \in \mathcal{F}$, от $f_1(P_i) = f_2(P_i)$ за всички $P_i \in B$ следва, че $f_1(D) = f_2(D)$.

(SS2) За всяко $B \notin \Gamma$ и всяка функция $f \in \mathcal{F}$

$$|\{g \in \mathcal{F} \mid g(P_i) = f(P_i) \ \ \forall P_i \in B, g(D) \neq f(D)\}| > 0.$$

Ако условието (SS2) се замени с

(SS2′) за всяко $B \notin \Gamma$, за всяка функция $f \in \mathcal{F}$ и всеки ключ $K \in \mathcal{K}$, съществува константа $\lambda(f, B) \geq 1$, за която

$$|\{g \in \mathcal{F} \mid g(P_i) = f(P_i) \ \ \forall P_i \in B, g(D) = K\}| = \lambda(f, B),$$

то $\langle \Gamma, \mathcal{F} \rangle$ се нарича *съвършена*.

Ефективността на една съвършена схема за разпределяне на данни с измерва от нейната *скорост*. Количеството информация,което i-тия потребител получава чрез своя дял $\log_2 |\mathcal{S}_i|$ бита, докато информацията, съдържаща се в ключа е $\log_2 |\mathcal{K}|$ биц. *Информационната скорост на i-тия потребител* дефинираме като частното

$$\rho_i = \frac{\log_2 |\mathcal{K}|}{\log_2 |\mathcal{S}_i|}.$$

Скорост ρ на една схема за разпределяне на данни наричаме минимума на скоростите на всички участници, т.е. $\rho = \min_{1 \leq i \leq n} \rho_i$.

Теорема 13.17. *Скоростта на всяка съвършена схема за разпределяне на данни не надхвърля 1.*

Доказателство. Нека $\langle \Gamma, \mathcal{F} \rangle$ е съвършена схема за разпределяне на данни. Фиксираме $B \in \Gamma_{\min}$ и нека $P_j \in B$. Означаваме $B' = B \setminus \{P_j\}$ и избираме правило $f \in \mathcal{F}$. От $B' \notin \Gamma$ и (SS2′) получаваме

$$|\{g \in \mathcal{F} \mid g(P_i) = f(P_i) \ \ \forall P_i \in B', g(D) = K\}| = \lambda(f, B') \geq 1,$$

за всчкиключ $K \in \mathcal{K}$. Следователно за всяка $K \in \mathcal{K}$, съществува правило $g_K \in \mathcal{F}$, за което $g_K(D) = K$ и $g_K(P_i) = f(P_i)$ за всички $P_i \in B'$. От (SS1) получаваме $g_K(P_j) \neq g_{K'}(P_j)$ за $K \neq K'$, откъдето $|\mathcal{S}_j| \geq |\mathcal{K}|$. Оттук следва $\rho \leq 1$. □

В Теорема 13.17 се твърди, че количеството информация, което всеки участник в една съвършена схема получава като дял не може да е по-малко от информацията, която се съдържа в ключа. Една съвършена схема за разпределяне на данни със скорост $\rho = 1$ *идеална*. Конструквията от раздел 13.3 дава идеални с|textcyrhemi.

13.4.2 Вероятностен подход към схемите за разпределяне на данни

В този раздел че опишемедин по-общ вероятностен подход към схемите за разпределяне на данни,предложен от Blakley и Kabatianski [8].

Нека $S_0, S_1, \ldots, S_n$ са случайни величини, дефинирани съответно върху множествата $\mathcal{S}_0, \mathcal{S}_1, \ldots, \mathcal{S}_n$, и нека $P(\mathcal{S})$ есъвместното имразпределение върху $\mathcal{S} = \mathcal{S}_0 \times \mathcal{S}_1 \times \ldots \times \mathcal{S}_n$. Нека $\Gamma \subset 2^{\{1,2,\ldots,n\}}$ е структура на достъп. Двойката $\langle P, \mathcal{S} \rangle$ наричаме *съвършена схема за разпределяне на данни, реализираща* Γ, ако са изпълнени условията

(PS1) $P(S_0 = s_0 \mid S_i = s_i, \forall i \in B) \in \{0, 1\}$ ако $B \in \Gamma$,

(PS2) $P(S_0 = s_0 \mid S_i = s_i, \forall i \in B) = P(S_0 = s_0)$ ако $B \notin \Gamma$.

Тайният ключ $K = s_0$ се избира от $\mathcal{S}_0$ с вероятност

$$P(S_0 = s_0) = \sum_{s_1 \in \mathcal{S}_1} \ldots \sum_{s_n \in \mathcal{S}_n} P(S_0 = s_0, S_1 = s_1, \ldots, S_n = s_n).$$

Ключът s_0 се разпределя между участницитекато се генерират n дяла $s_1, s_2, \ldots, s_n$, $s_i \in \mathcal{S}_i$, с вероятност $P(S_1 = s_1, \ldots, S_n = s_n | S_0 = s_0)$. Никой от участниците няма информация за дяловете на кой да е отостаналите потребители, но разполага с множествата $\mathcal{S}_i$ и разпределенията $P(S_0 = s_0)$ и $P(S_1 = s_1, \ldots, S_n = s_n | S_0 = s_0)$. Условие (PS1) означава, че всяко авторизиранео множество B от потребители е в състояние да възстанови ключа. Второто условие гарантира, че никое неавторизираномножество не може да получи допълнителна информация,различна от тази,която е вече налична. Лесно се доказва, че двете условия (PS1) и (PS2) са еквивалентни на единственотоусловие

(PS3) $H(S_i, i \in B \cup \{0\}) = H(S_i, i \in B) + \delta_\Gamma(B) H(S_0)$, където $B \subset \{1, 2, \ldots, n\}$ и

$$\delta_\Gamma(B) = \begin{cases} 0 & \text{ако } B \in \Gamma, \\ 1 & \text{ако } B \notin \Gamma, \end{cases} \tag{13.3}$$

където $H(S_i, i \in B)$ е съвместната ентропия на случайните величини S_i.

Една съвършена схема за разпределяне на данни, дефинирана чрез (SS1) и (SS2′) удовлетворява също (PS1) и (PS2), ако всички правила са равновероятни. Оказва се, че е изпълнено $H(S_i) \geq H(S_0)$ (вж.Лема 13.18 по-долу). Една съвъшена схема за разпределяне на данни наричаме *идеална*, ако $H(S_i) = H(S_0)$ за всички i. Тази дефиниция се съгласаува с Дефиниция 13.16.

Следващият резултат е доказан първоначално от Brickell и Davenport [12], и характеризира всички идеални схеми за разпределяне на данни. По-долу ще скицираме доказателство на Blakley и Kabatianski [8]на малко по-общ резултат.

Нека $f(0)$ е функция,приемаща реални стойности, дефинирана върху подмножествата на $\{0, 1, \ldots, n\}$, коыто изпълнява условията:

(F1) $f(\emptyset) = 0$;

(F2) $f(A) \leq f(B)$ за $A \subset B$;

(F3) $f(A \cup B) \leq f(A) + f(B)$.

Казваме, че f е съвършена функция, реализираща структурата на достъп Γ, ако if

$$f(A \cup \{0\}) = f(A) + \delta_\Gamma(A) f(\{0\}),$$

където $\delta_\Gamma(A)$ е дефинирана в (13.3). Ако f е съвършена функция, ще казваме, че елементът $a \in \{0, 1, \ldots, n\}$ "принадлежи" на $A \subset \{0, 1, \ldots, n\}$, или формално "$a \in A$", ако $f(\{a\} \cup A) = f(A)$. Елементът a "не принадлежи" на A, или "$a \notin A$", ако $f(\{a\} \cup A) = f(A) + f(\{a\})$. Възможно да не е изпълнено нито "$a \in A$", нито "$a \notin A$". Но за всяко A е изпълнено "$0 \in A$" или "$0 \notin A$".

Лема 13.18. *Ако "$0 \notin A$", но 0" $\in$ "$A \cup \{i\}$, то $f(A \cup \{i\}) \geq f(A) + f(\{0\})$ и $f(\{a\}) \geq f(\{0\})$.*

Ентропията $H(S_i, i \in B)$ удовлетворява (F1)–(F3) и следователно $H(S_i) \geq H(S_0)$. Една съвършна функция f, реализираща Γ, наричаме *идеална*, ако $f(\{a\} = f(\{0\})$ за всички a.

Лема 13.19. *Ако "$a \notin A$", но "$a \in A \cup \{b\}$",то "$b \notin A$" и "$b \in$ "$A \cup \{a\}$".*

Нека f удовлетворява и условията

(F4) от "$a \in A$" и $A \subset B$ следва "$a \in B$";

(F5) от "$a \notin A$" и $B \subset A$ следва "$a \notin B$".

Да отбележим, че $H(S_i, i \in B)$ удовлетворява и условията (F4) и (F5). Без ограничение на общността можем да допуснем, че за идеалната функция f, $f(\{a\}) = 1$ за всички $a \in \{0, 1, \ldots, n\}$. Следните леми се получават лесно от свойствата (F1)–(F5).

Лема 13.20. *Ако "$b \in A \cup B \cup \{b\}$" за всяко $b \in B$, то $f(A' \cup B) = f(A') + |B|$ за всяко $A' \subset A$.*

Лема 13.21. *Ако "$a \in A \cup \{b\}$" и "$b \in B$", то "$b \in A \cup B$".*

Лема 13.22. *Ако "$0 \notin B$",но "$0 \in A \cup B$ ",тосъществува $a \in A$, за което "$a \in \{0\} \cup B \cup A \setminus \{a\}$". По специално, ако "$0 \in A$" то съществува $a \in A$, за което a" $\in$ "$\{0\} \cup A \setminus \{a\}$.*

Теорема 13.23. *За всяка идеална функция f стойностите $f(A)$ са цели числа за всяко $A \subset \{0, 1, \ldots, n\}$.*

Доказателство. Нека A е множество с минимална мощност, за което $f(A)$ не е цяло число.

1) Нека "$0 \in A$", т.е. $A \in \Gamma$. Съгласно Лема 13.22, съществува $a \in A$, за което "$a \in \{0\} \cup A \setminus \{a\}$", откъдето

$$f(A) = f(\{0\}) \cup A) = f(\{0\}) \cup A \setminus \{a\}) = f(A \setminus \{a\}) + \delta.$$

Дясната страна е цяло число,тъй като $f(A \setminus \{a\})$ е цяло число от допускането и от $\delta \in \{0, 1\}$.

2) Нека "$0 \notin A$". Да разгледаме множество B с минимална мощност, за което "$0 \notin B$" и "$0 \in A \cup B$. Съгласно Лема 13.22 съществува $a \in A$,за което "$a \in \{0\} \cup B \cup A \setminus \{a\}$". От друга страна "$0 \in B \cup A \setminus \{a\}$", тъй като в противен случай "$a \notin B \cup A \setminus \{a\}$", "$a \notin A \setminus \{a\}$" и $f(A) = f(A \setminus \{a\}) + 1$ в протоворечие на първоначалното ни допускане. От Лема 13.21 имаме $f(A \cup B) = f(B \cup A \setminus \{a\})$. Освен това "$b \notin A \cup B \setminus \{b\}$" за всички b (в противен случай "$0 \in A \cup B \setminus \{b\}$", противоречие с минималността на B). Сега от Лема 13.20 $f(A \cup B) = f(A) + |B|$ и $f(B \cup A \setminus \{a\}) = f(A \setminus \{a\}) + |B|$. Следователно $f(A) = f(A \setminus \{a\})$ и $f(A \setminus \{a\})$ е цяло число, противоречие.

Теорема 13.24. *Нека f е свързена функция, реализираща структурата на достъп Γ. Тогава всичкимножества A, дефинирани чрез $f(A) = |A|$ образуват свързан матроид над $\{0, 1, \ldots, n\}$. Всички цикли на този матроид, съдържащи 0, са от вида $\{0\} \cup A$, където $A \in \Gamma_{\min}$.*

Доказателство. От Теорема 13.23 имаме, че f е целочислена функция. Остава да се провери, че тя удовлетворява (R1)–(R3), което е очевидно.

Известно е, че съществуват матроиди със свойството, че множеството от техните цикли не съвпада с множеството от независимите множества на идеална схема за разпределяне на данни. От друга страна всеки матроид, представим над крайно поле може да бъде реализиран като множеството от всички неавторизирани коалиции на някава идеална схема за разпределяне на данни.

Съществуват матроиди, които не са представими над крайно поле,но въпреки това могат да бъдат реализирани като неавторизираните множества на идеална схема за разпределяне на данни.