KAZALO

1. UVOD

S skrivanjem skrivnosti se srečujemo v vsakdanjem življenju. Skrivati moramo na primer osebno številko bančne kartice ali pa ključe stanovanja, sicer bi nam lahko ukradli denar oziroma vdrli v hišo. Posledice odkritja takih skrivnosti posameznika naj ne bi bile tako velike, kot posledice odkritje ključa trezorja v banki ali pa odkritje ključa za izstrelitev rakete v vojski. Zato moramo take pomembne kode bolj zavarovati. To lahko naredimo tako, da kodo oziroma **ključe** razdelimo med več ljudi (**članov**), ki morajo sodelovati po predpisani **shemi za delitev skrivnosti**. Dobre sheme za delitev skrivnosti preprečujejo nedovoljen dostop do ključev in zagotavljajo, da lahko določena množica članov še vedno sestavi celotno skrivnost, pa čeprav se je nekaj ključev izgubilo. Poznamo več vrst shem za delitev skrivnosti, ki niso vse enako uporabne, tako da se večinoma uporabljajo kombinacije med njimi. Poglejmo kakšne vrste shem za delitev skrivnosti poznamo:

- $k_i - l_i$ **delitvena shema** kjer skrivnost razdelimo tako, da za rekonstrukcijo skrivnosti potrebujemo določeno sodelovanje članov (iz i-tega razreda, v katerem je vseh članov l_i, potrebujemo k_i članov).
- **Večnivojska shema** je k_i - l_i delitvena shema, kjer zasebne dele informacije razdelimo v dva ali več nivojev, tako da za rekonstrukcijo skrivnosti potrebujemo določeno sodelovanje članov na kateremkoli nivoju (k_i jih potrebujemo iz i-tega nivoja, k_j jih potrebujemo iz j-tega nivoja…). Možno je tudi sodelovanje po nivojih.
- **Zunanja shema** je v nasprotju z **notranjo shemo**, kjer je rekonstrukcija skrivnosti odvisna od funkcije zasebnega dela informacije do drugih delov informacije, ki jih imajo člani in ne od vsebine, ki jo vsebuje posamezen del.
- **Časovna shema za delitev skrivnosti** v katerih člani lahko sestavijo skrivnost le v določenem času.
- **Večskupinska shema za delitev skrivnosti**, kjer nastopa več skupin s člani in vsaka skupina mora oddati svoj glas, da lahko skupaj sprožita akcijo (ena sama skupina brez druge, akcije ne more sprožiti).

Podrobneje bomo spoznali večnivojske in večskupinske sheme za delitev skrivnosti, saj jih lahko sestavljamo in so zato najprimernejši za implementacijo. Ogledali si njihove konstrukcije in realizacije. Poglejmo si vsebino diplomskega dela.

V 2. poglavju si bomo ogledali matematiko, ki jo potrebujemo za razumevanje diplomskega dela. Spoznali bomo osnovno kriptografijo in popolno verjetnost, ki jo potrebujemo pri konstrukciji shem za delitev skrivnosti. Pogledali bomo definicijo končnih obsegih nad katerimi bomo predstavljali projektivno in afino geometrijo.
V 3. poglavju si bomo ogledali dve osnovni konstrukciji shem za delitev skrivnosti, Shamirjevo in Blakleyevo. Pokazali bomo, kako prevedemo sheme v matematiko in spoznali novo terminologijo, ki nastopa v njih. Ogledali si bomo lastnosti različnih pristopov h konstrukcijam in rezultate takega pristopa.
V 4. poglavju bomo predstavili dve pomembnejši shemi za delitev skrivnosti. To je sodelovanje po nivojih in sodelovanje članov iz različnih skupin. Prikazali bomo prednosti vsake vrste in primere uporabe. Analizirala bom varnost pri posploševanju teh shem. Na koncu pa bomo govorili še o uporabljeni geometriji, ki nastopa v shemah.
V 5. poglavju bomo pogledali povezavo med geometrično in grafično predstavitvijo shem. Razlog za to je lažja implementacija preko grafov. Ogledali si bomo primerov iz katerih bomo izpeljali izreke, po katerih lahko pretvorimo geometrične konstrukcije v grafične.
V 6. poglavju, ki je zaključek diplomskega dela, bomo opisali kaj od shem v realni uporabi pričakujemo. Ogledali si bomo težave in možne rešitve, ki se pojavljajo pri uporabi shem v vojski, kjer so ključi deljeni po nivojih in so posledice nepooblaščene uporabe ključev lahko zelo velike.

2. MATEMATIČNE OSNOVE

V tem poglavju bomo spoznali vse matematične pojme, ki jih bomo v tem delu potrebovali za razumevanje snovi.
Pri ugotavljanju varnosti v shemah za delitev skrivnosti pa je zelo pomembna verjetnosti, ki jo imajo napadalci, da odkrijejo skrivnost in zato bomo v razdelku 2.1. omenili še totalno verjetnost in Baysove formule. Opisali bomo definicijo in lastnosti kriptosistema, saj je kriptografija tista, ki uporablja sheme za delitev skrivnosti. Vpeljali bomo tudi pojem entropije, ki nam podaja negotovost napadalca.
Ker bodo vse geometrične predstavitve potekale nad končnimi obsegi v afinih oziroma projektivnih prostorih, bomo v razdelku 2.2. vse te strukture definirali in povedali njihove osnovne lastnosti. Pri afinih in projektivnih ravninah pa bomo še napisali formulo za število elementov določene dimenzije v teh prostorih.
V razdelku 2.3. se bomo srečali tudi z grafi in mrežami in zato bomo tudi za njih povedali nekaj osnovnih lastnosti za lažje razumevanje snovi.
V razdelku 2.4. bomo povedali nekaj o interpolaciji s katero se srečamo pri Shamirjevih shemah. Opisali bomo le osnovno nalogo interpolacije.
V razdelku 2.5. pa bom opisala še stožernice in njihove lastnosti, ki nam zagotavljajo linearno neodvisnost.

2.1. VERJETNOST IN KRIPTOGRAFSKI SISTEMI

Sedaj bomo opisali vse potrebne definicije, ki jih potrebujemo za analiziranje varnosti v naših shemah za delitev skrivnosti. Predstavili bomo verjetnostne formule s katerimi izračunamo verjetnost ugibanja skrivnosti in pa entropijo. Definirali bomo kriptosistem s katerim potem podamo definicijo popolne varnosti.

Poglejmo si najprej osnove verjetnosti, saj jih bomo potrebovali pri definiciji popolne verjetnosti, ki pa je osnova za popolno varnost v shemah.
Če se nek dogodek vedno zgodi, ga imenujemo **gotov dogodek** in ga označimo z G. Če pa za nek dogodek velja, da se nikoli ne bo zgodil, ga imenujemo **nemogoč dogodek** in ga označimo z N.

Vzemimo dva dogodka A in B. Verjetnosti dogodka B ob pogoju, da se je dogodek A zgodil, imenujemo pogojna verjetnost dogodka B ob pogoju A in jo označimo z $P(B / A)$. Če dogodek A oziroma dogodek B nista nemogoča dogodka, potem veljata formule:

$$P(B / A) = \frac{P(A \cap B)}{P(A)} \text{ oziroma } P(A / B) = \frac{P(A \cap B)}{P(B)} \qquad (*)$$

$$\Rightarrow Za\ A, B \neq N \text{ velja } P(A)P(B / A) = P(B)P(A / B). \qquad (\ )$$

Opomba: Presek dogodkov $A \cap$B krajše zapišemo kot AB.

Definicija: *Dogodka A in B sta **neodvisna** (dogodek A ne pove nič o dogodku B), potem velja P(AB) = P(A)P(B).*

Propozicija 2.1: *Dogodka A in B sta neodvisna natanko takrat, ko velja P(A/B) = P(A).*

■

Vzemimo **popoln sistem dogodkov** $B = \{B_i, i = 1,.., n\}$ (t.j. $\bigcup_i B_i = G$ in $B_i \cap B_j = N$).

Poglejmo si situacijo, ko imamo popoln sistem dogodkov $B = \{B_i, i = 1,.., n\}$ potem velja formula za popolno verjetnost:

$$P(A) = \sum_{i=1}^{n} P(A / B_i)P(B_i). \qquad (**)$$

Iz formul (*) in (**) dobimo naslednji izrek:

Bayesev izrek: $$P(B_k / A) = \frac{P(A / B_k)P(B_k)}{\sum_{i=1}^{n} P(A / B_i)P(B_i)}.$$

Sedaj si poglejmo definicije nekaterih osnovnih pojmov kriptografije, ki jih bomo srečali.

Definicija: ***Kriptosistem*** *je peterica $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, kjer veljajo naslednji pogoji:*

- *$\mathcal{P}$ je končna množica vseh možnih besedil,*
- *$\mathcal{C}$ je končna množica vseh možnih kodiranih besedil,*
- *$\mathcal{K}$ je končna množica vseh možnih ključev,*
- *Za vsak $K \in \mathcal{K}$ obstaja pravilo kodiranja $e_K \in \mathcal{E}$ in korespondentno pravilo odkodiranja $d_K \in \mathcal{D}$. Vsak $e_K : \mathcal{P} \to \mathcal{C}$ in $d_K : \mathcal{C} \to \mathcal{P}$ sta taki funkciji, da velja $d_K(e_K(x)) = x$ za vsako besedilo $x \in \mathcal{P}$.*

Definicija: *Kriptosistem je **popolnoma varen**, če je verjetnost p(X/Y) = p(X) za vsako besedilo $X \in \mathcal{P}$ in vsako kodirano besedilo $Y \in \mathcal{C}$. To pomeni, da je verjetnost, da je besedilo, ki ga odkrivamo besedilo X pri danem kodiranem besedilu Y enaka kot prvotna verjetnost, da je besedilo, ki ga odkrivamo besedilo X.*

Definirajmo sedaj še **entropijo**, ki jo bomo uporabljali pri računanju negotovosti napadalca o skrivni točki p (tj. točka oziroma skrivnost katero s shemami za delitev skrivnosti iščemo). Entropijo lahko gledamo kot na matematično mero informacij oziroma negotovost in jo izračunamo kot funkcijo danih verjetnosti. Recimo, da imamo naključno spremenljivko X, ki lahko zavzame vrednosti v končni množici glede na podane verjetnosti PX). Koliko informacij dobimo pri dogodku, ki se zgodi glede na njegovo verjetnost $P(X)$. Ekvivalentno temu je, če se dogodek še ni zgodil, da se lahko vprašamo, kakšna je negotovost o rezultatu dogodka. To količino merimo z entropijo dogodka X in jo označimo z $H(X)$.

Definicija: *Naj bo X naključna spremenljivka, ki deluje na končnih množicah vrednosti glede na podano verjetnost P(X). Potem je entropija te verjetnosti definirana z:*

$$H(X) = -\sum_{i=1}^{n} P_i \log_2 P_i .$$

Če so možne vrednosti za X x_i, $1 \le i \le n$, *potem imamo formulo:*

$$H(X) = -\sum_{i=1}^{n} P(X = x_i) \log_2 P(X = x_i) .$$

2.2. AFINI IN PROJEKTIVNI PROSTORI NAD KONČNIMI OBSEGI

Definirajmo obseg in si poglejmo nekaj njegovih lastnosti. Bolj nas bodo zanimali končni obsegi s katerimi se srečamo v naslednjih poglavjih.

Definicija: ***Obseg*** *je množica K, ki je zaprta za operaciji + in *, tako da velja:*
(a) *(K,+) je Abelova grupa z enoto* 0*;*
(b) *Za* $K_0 = K \setminus \{0\}$je *(K_0,*) je Abelova grupa z enoto* 1*;*
(c) x(y + z) = xy + xz, (x + y)z =xz + yz, za vse x,y in z iz K (distributivnost).

Definicija:

- ***Končen obseg*** *je obseg s končno elementi. Če je število njegovih elementov q, potem končni obseg označimo z* **GF*(q)***.
- ***Karakteristika*** *končnega obsega K je najmanjše pozitivno celo število p za katerega velja* $px = 0$ *, za vsak* $x \in K$*. Očitno mora biti p praštevilo.*
- *Za p praštevilo imenujemo* GF*(p)* ***praštevilski obseg*** *in ga označimo z* $\mathbb{Z}_p$*. Predstavimo ga lahko z ostanki celih števil pri seštevanju in množenju po modulu p.*

Poglejmo si še naslednji izrek, ki nam pove zakaj je $\mathbb{Z}_p$ končen obseg.

Izrek 2.1: *Končen netrivialen kolobar brez deliteljev niča je obseg.*

Dokaz: Naj bo kolobar K brez deliteljev niča in naj vsebuje le končno število elementov. V kolobarju K si izberemo poljuben element $a \neq 0$ in si ogledamo množico $\{ax, x \in K\}$. Ker velja v kolobarju K pravilo krajšanja (ker morajo biti v kolobarju vsi elementi obrnljivi), sledi iz $ax = ay$, da je $x = y$. Torej je produktov ax ravno toliko, kolikor je elementov končnega kolobarja K. Zato so v množici $\{ax, x \in K\}$ vsi

elementi kolobarja K. To pomeni, da je enačba $ax = b$ rešljiva za vsak $b \in K$. Prav tako ugotovimo, da je enačba $xa = b$ vselej rešljiva.
Posebaj za $b = a$ se prva enačba glasi $ax = a$. Njeno rešitev zaznamujemo z e, tako da je $ae = a$. naj bo zdaj x poljuben element iz kolobarja K. Ker je produkt $a(x - ex) = ax - aex = ax - ax = 0$ in kolobar K brez deliteljev niča, sledi od tod $x - ex = 0$ ali $ex = x$. za $a = x$ dobimo npr. $ea = a$. Ker je tudi produkt $(ex - x)a = xea - xa = xa - xa = 0$, sledi od tod $xe = x$. Torej je e identiteta kolobarja K. Enačbi $ax = e$ in $ya = e$ sta za vsak $a \neq 0$ rešljivi. Zato je vsak od nič različen element obrnljiv in kolobar K je obseg. ■

Definicija: *Red elementa x je najmanjše tako število r, za katerega velja* $x^r = e$.

Izrek 2.2: *Red elementa grupe deli moč grupe.* ■

Naštejmo nekaj lastnosti končnih obsegov:

1. Končen obseg K s karakteristiko p vsebuje podobseg izomorfen $\mathbb{Z}_p$. Na K lahko gledamo kot vektorski prostor nad obsegom $\mathbb{Z}_p$. Zato ima p^h elementov za nek $h \in \mathbb{N}$. Velja naslednje: $x \in \mathbb{Z}_p$ natanko tedaj, ko $x^p - x = 0$.
2. Elementi iz GF(q), $q = p^h$ ustrezajo enačbi: $x^q - x = 0$
   in v GF(q) obstaja tako število s, da velja GF(q) = $\{0, s^0, s^1, ..., s^{q-2} | s^{q-1} = 1\}$.
3. Vsak obseg s q elementi je izomorfen obsegu GF(q).

Definirajmo pojem incidenčni sistem, s katerim bomo vpeljali projektivne in afine geometrije.

Definicija: *Urejena trojica (X,Y,p), kjer sta X in Y neprazni množici in p binarna relacija v X x Y se imenuje* ***incidenčni sistem***.

Incidenčni sistem lahko definiramo tudi s funkcijo. Urejena trojica (X,Y,f), kjer sta X in Y neprazni množici in $f : Y \to P(X)$ se imenuje incidenčni sistem. Relacija p je s funkcijo f v naslednji zvezi: $f(y) = \{x \mid x \in X, xpy\}$.

V delu bomo preko geometrije spoznavali konstrukcije shem, zato si poglejmo definicije projektivne geometrije, prostora in ravnine ter definicijo afine geometrije, prostora in ravnine.

PROJEKTIVNA GEOMETRIJA

Oglejmo si najprej definicijo projektivnega prostora. Premico skozi dve točki A in B bomo označevali z p_{AB}.

Definicija: ***Projektivni prostor*** *je par* $(\mathcal{P}, \mathcal{L})$*, kjer je* $\mathcal{P}$ *neprazna množica točk in* $\mathcal{L}$ *neprazna družina podmnožic množice* $\mathcal{P}$*, ki jim rečemo premice in ustrezajo naslednjim pogojem:*
PG1*: Če imamo dve različni točki P in Q, potem obstaja natanko eno premico, ki ju vsebuje.*

PG2: *Če imamo štiri različne točke A, B, C in D take, da obstaja točka E, ki je presečišče premic p_{AB} in p_{CD}, potem obstaja točka F, ki je presečišče premic p_{AC} in p_{BD}.*
PG3: *Vsaka premica vsebuje vsaj tri točke; vse točke niso kolinearne.*

Definicija: ***Projektivna ravnina*** *je urejen par $(\mathcal{P}, \mathcal{L})$, kjer je $\mathcal{P}$ neprazna množica točk in $\mathcal{L}$ neprazna družina podmnožic množice $\mathcal{P}$ (rečemo jim premice), za katerega veljajo naslednji aksiomi:*
P1: *če sta P in Q različni točki, potem obstaja natanko določena premica l, za katero velja $P \in l$ in $Q \in l$,*
P2: *če sta l in m različni premici v $\mathcal{L}$, potem velja $m \cap l \neq \emptyset$,*
P3: *na vsaki premici obstajajo vsaj tri točke; obstajata vsaj dve premici,*
P4: *obstaja premica, ki vsebuje $q+1$ točk ($q>1$).*

Izrek 2.2: *Za vsako projektivno ravnino obstaja naravno število $q > 1$ tako, da velja:*
- *Vsaka premica vsebuje natanko $q+1$ točk.*
- *Skozi vsako točko gre natanko $q+1$ premic.*
- *Število točk je natanko q^2+q+1.*
- *Število premic je natanko q^2+q+1.*

Dokaz: Po aksiomu $P4$ obstaja premica $p = \{A_1, A_2, ..., A_{q+1}\}$, ki vsebuje $q + 1$ točk. Vzemimo zdaj neko drugo premico $p_i \neq p$. Po $P2$ se premici sekata v eni točki in naj bo to točka A_i. Na p_i zagotovo obstaja točka B, ki ne leži na premici p. Po aksiomu $P3$ premica s točkama B in A_i vsebuje neko točko $C \neq B, A_i$. Sedaj premice s točkama C in A_i $(i = 1, ..., q+1)$ izčrpajo vse možne premice skozi C, kar vidimo iz aksioma $P1$ in $P2$. Še več, vsaka izmed njih ima po eno skupno točko s premico p_i. Pri tem p_i ne more vsebovati več kot $q+1$ točk, ker bi sicer čez točko C šlo več kot $q+1$ premic. S tem sta dokazani prvi dve trditvi.
Poglejmo sedaj točke projektivne ravnine. Čez vsako točko gre po drugi trditvi $q+1$ premic in vsaka od njih vsebuje $q+1$ točk, po prvi trditvi. Zato je skupno število točk $q(q+1)+1 = q^2+q+1$ in dokazano imamo tretjo trditev in zaradi dualnosti tudi četrto. ■

Poglejmo si splošne formule. $N_0(n,q)$ je število točk neke projektivne geometrije dimenzije n in reda q. Iz trditve sledi $N_0(0,q) = 1$, $N_0(1,q) = q+1$ in $N_0(2,q) = q^2+q+1$. Velja formula $N_0(n,q) = q^n + ... + q + 1$ to je

$$N_0(n,q) = \frac{q^{n+1} - 1}{q - 1}.$$

Sedaj poglejmo število k-dimenzionalnih podprostorov v n-dimenzionalnem prostoru reda q:

$$N_k(n,q) = \frac{(q^n + ... + 1)(q^n + ... + q)...(q^n + ... + q^k)}{(q^k + ... + 1)(q^k + ... + q)...(q^k)} \qquad (+)$$

oziroma:

$$N_k(n,q) = N_{n-k-1}(n,q), \qquad (++)$$

kar pomeni, da je v n-dimenzionalnem projektivnem prostoru število k-dimenzionalnih podprostorov enako številu (n-k-1)-dimenzionalnih podprostorov. Posebej, število točk je enako številu hiperravnin.

Opomba: Zaradi formul (+) in (++) označujemo $N_k(n,q)$ tudi z $\begin{bmatrix} n \\ k \end{bmatrix}_q$.

Označimo z $N_{m,k}(n,q)$ število k-dimenzionalnih podprostorov n-dimenzionalnega projektivnega prostora reda q, ki vsebujejo en fiksen m-dimenzonalen prostor:

$$N_{m,k}(n,q) = \frac{(q^n + \ldots + q^{m+1})(q^n + \ldots + q^{m+2})\ldots(q^n + \ldots + q^k)}{(q^k + \ldots + q^{m+1})(q^k + \ldots + q^{m+2})\ldots(q^k)}.$$

AFINA GEOMETRIJA

Oglejmo si osnovne pojme v afini geometriji.

Definicija: *Podprostor katerega dimenzija je za ena manjša od celega prostora imenujemo* ***hiperravnina****.*

Definicija: ***Afin prostor*** $\mathcal{A}$ *je trojica* $(\mathcal{P}, \mathcal{L}, \mathcal{E})$*, kjer je* $\mathcal{P}$ *neprazna množica točk in* $\mathcal{L}$ *in* $\mathcal{E}$ *neprazni družini podmnožic množice* $\mathcal{P}$*, imenovane premice (iz* $\mathcal{L}$*) in ravnine (iz* $\mathcal{E}$*), ki zadoščajo naslednjim pogojem:*
AG1*: Če sta P in Q različni točki, potem obstaja enolična premica* l*, za katero velja* $P \in l$ *in* $Q \in l$.
AG2*: Če so P, Q in R različne nekolinearne točke, potem obstaja enolično določena ravnina (določena s temi točkami).*
AG3*: Če P ne leži na premici* l*, potem obstaja enolična premica* m *, tako da* $P \in m$ *in* $m \parallel l$.
AG4*: Če so* l *,* m *in* k *različne premice z lastnostmi* $l \parallel m$ *in* $m \parallel k$*, potem velja* $l \parallel k$.

Poglejmo si še definicijo afine ravnine.

Definicija: ***Afina ravnina*** *je urejen par* $(\mathcal{P}, \mathcal{L})$*, kjer je* $\mathcal{P}$ *neprazna množica elementov, ki jim rečemo točke, in* $\mathcal{L}$ *neprazna družina podmnožic množice* $\mathcal{P}$*, imenovane premice, ki imajo naslednje lastnosti:*
A1*: Če Sta P in Q različni točki, potem obstaja enolična premica* l*, za katero velja* $P \in l$ *in* $Q \in l$.
A2*: Če P ne leži na premici* l*, potem obstaja enolična premica* m*, tako da* $P \in m$ *in* $m \cap l = \emptyset$.
A3*: Na vsaki premici obstajata vsaj dve točki; obstajata vsaj dve premici.*

Tudi tukaj bomo opisali koliko je afinih podprostorov v nekem afinem porstoru. Število k-dimenzionalnih podprostorov (oznaka $M_k(n,q)$).

- $M_0(n,q) = N_0(n,q) - N_0(n-1,q)$
- $M_0(n,q) = q^{n-1}$
- $M_k(n,q) = q^{n-k} \prod_{s=1}^{k} \frac{q^{n+1-s} - 1}{q^{k+1-s} - 1}$
- $M_{m,k}(n,q) = N_{m,k}(n,q)$

2.3. GRAFI IN MREŽE

V delu se srečamo s pojmoma mreže in grafa le v zaključku kakšnega poglavja, zato ju bomo le na kratko opisali in definirali.

GRAF

Definicija: *Vzemimo neprazno množico X in binarno operacijo na X. Urejen par (X, ρ) se imenuje **graf**. Elementi množice X se imenujejo vozlišča in elemente množice ρ imenujemo povezave grafa.*

Opomba: Če gledamo na incidenčne sisteme (*X*, *Y*, *f*) neformalno, se elementi množice *Y* lahko identificirajo s svojimi slikami pri preslikavi s funkcijo *f*. Zato lahko zapišemo incidenčni sistem tudi kot par (*X*, *E*). Par (*X*, *E*) se v literaturi imenuje **hipergraf**. Množica *X* so točke hipergrafa in množica *E* so **hiperpovezave**. Hiperpovezave v splošnem povezujejo več kot le dve točki iz množice *X*. To je posplošitev multigrafa: Če je *E* sestavljena le iz podmnožic z dvema elementoma potem se hipergraf posploši na neorientiran multigraf.
Včasih damo pod pogoje v definicijo hipergrafa tudi to, da mora vsaka točka ležati vsaj na eni hiperpovezavi in da ima vsaka hiperpovezava vsaj eno točko.
Hipergrafe lahko predstavimo z neorijentiranimi grafi in vso teorijo hipergrafov lahko prevedemo na običajno teorijo grafov.

MREŽE

Sedaj bomo definirali pojem **mreže**, ki ga bomo srečali v tem delu. Ne bomo povedali veliko o mrežah, saj v delu niso tako pomembne. Omenimo jih zaradi lažjega razumevanja zaključkov. Najprej definirajmo delno urejenost:

Definicija: ***Delno urejena množica*** *je par (S, ≤), kjer je S množica in ≤ binarna operacija, ki zadošča naslednjim pogojem:*
- *$x \le x$ za vsak $x \in S$ (≤ je reflexsivna)*
- *$x \le y$ in $y \le x$ sledi $x = y$ (≤ je atisimetrična)*
- *$x \le y$ in $y \le z$ sledi $x \le z$ (≤ je tranzitivna)*

Definicija: *Mreža je množica L z dvema binarnima operacijama ∧ in ∨ in dvema konstantama* 0 *in* 1 *in zadošča naslednjim pogojem:*
L1: ∧ in ∨ sta idempotentna, komutativna in asociativna
L2: $x \vee (x \wedge y) = x$ in $x \wedge (x \vee y) = x$
L3: $x \wedge 0 = x$ in $x \vee 1 = x$

Iz teh aksiomov sledi, da velja $x \wedge y = x$ če in samo če $x \vee y = y$. Pišemo $x \leq y$, če veljajo ekvivalentni pogoji. Potem je $(L, \leq)$ je delno urejena množica z največjim elementom 1 in najmanjšim elementom 0. $x \vee y$ in $x \wedge y$ sta najmanjša zgornja meja in največja spodnja meja. Vsaka delno urejena množica, kjer obstajata najmanjša zgornja meja in največja spodnja meja za vsak par elementov v množici in največji in najmanjši element te množice obstajata, je mreža.

Za najmanjšo zgornjo mejo velja, če je $x \leq z$ in $y \leq z$ in če $x, y \leq t$ potem je $z \leq t$. Za x in y je w največja spodnja meja, če velja $w \leq x$ in $w \leq y$ in ko $u \leq x, y$ potem $u \leq w$.

V mreži je **atom** naničelen element a takšen, da velja a ∧ x = 0 ali a za vsak x.
Povejmo še kaj je to **princip dualnosti**:

Definicija 2.17: *Če v nekem aksiomu nadomestimo* $\wedge$ *z* $\vee$ *ali* $\vee$ *z* $\wedge$ *in* 1 *z* 0 *in* 0 *z* 1 *dobimo dualni aksiom. Zamenjavi pravimo dualiziranje.*

2.4. INTERPOLACIJA

Pri numeričnem računanju imamo velikokrat opravka s funkcijami, ki so podane v obliki tabele:

$$x : x_0, x_1, ..., x_n$$
$$f(x) : y_0, y_1, ..., y_n$$

Vzemimo, da so vrednosti $y_i = f(x_i)$ natančno znane. Naloga je določiti vrednost y = $f(x)$ pri poljubnem argumentu x. V tem primeru lahko konstruiramo neko **interpolacijsko funkcijo** $g(x)$, to je funkcija, ki zavzame pri $x = x_i$ vrednost $g(x_i) = y_i$ in vzamemo $g(x)$ za približžek funkcije $f(x)$.
Osnovna naloga interpolacije je poiskati funkcijo, katere graf poteka skozi dano zaporedje točk (x_i, y_i), $i = 0, 1, ..., n$.

$$g(x_i) = y_i,\ i = 0, 1, ..., n.$$

Točke skozi katere položimo interpolacijsko krivuljo imenujemo interpolacijske točke. Interpolacijske funkcije so običajno polinomi oziroma trigonometrični polinomi za periodične funkcije. Skozi $n + 1$ interpolacijskih točk lahko vedno položimo polinom stopnje n. Število n pomeni stopnjo interpolacije.
Če so argumenti x_i v tabeli med seboj različni, potem obstaja natanko en interpolacijski polinom n-te stopnje, ki zavzame predpisane vrednosti $I_n(x_i) = y_i$ za $i = 1, .., n$.
Eksistenco interpolacijskega polinoma najlažje dokažemo tako, da polinom konstruiramo. Brez težav se prepričamo, da je $I_n = \sum_{k=0}^{n} y_k L_k^{(n)}(x)$, kjer je

$$L_k^{(n)}(x) = \frac{(x - x_0)...(x - x_{k-1})(x - x_{k+1})...(x - x_n)}{(x_k - x_0)...(x_k - x_{k-1})(x_k - x_{k+1})...(x_k - x_n)}.$$

Očitno je namreč $L_k^{(n)}(x_i) = \delta_{ik}$, $I_n(x_i) = y_i$.

Koeficienti $L_k^{(n)}$ se imenujejo Lagrangevi koeficienti. Formula $I_n = \sum_{k=0}^{n} y_k L_k^{(n)}(x)$ pa Lagrangeva formula za interpolacijski polinom.
Enoličnost interpolacijskega polinoma sledi iz dejstva, da se dva različna polinoma stopnje *n* ne morata ujemati v več kot *n* različnih točkah.

2.5. STOŽERNICE

S **stožernicami** si bomo pomagali pri linearni neodvisnosti, ki je zelo pomembna pri dodeljevanju zasebnih delov informacije. Nas bodo zanimale stožernice v projektivni ravnini.
V projektivni ravnini nad obsegom $\mathbb{F}$ je stožernica množica točk, ki zadoščajo homogeni kvadratni enačbi

$$Q(x) = f_1x_1^2 + f_2x_2^2 + f_3x_1x_3 + f_4x_2x_3 + f_5x_1x_2 + f_6x_3^2 = 0$$

$Q(x)$ imenujemo homogena kvadratna forma. Imamo elipso, hiperbolo in parabolo. V primeru, ko je obseg $\mathbb{F} = \mathbb{R}$ lahko povemo več. Projektivna stožernica $Q(x) = 0$ seka premico v neskončnosti ($x_3 = 0$) v točkah, ki zadoščajo enakosti $f_1x_1^2 + f_2x_2^2 + f_5x_1x_2 = 0$, ki so korespondentne afinim točkam, ki zadoščajo enačbi $f_1X_1^2 + f_2X_2^2 + f_5X_1X_2 = 0$.
To lahko zapišemo kot:

$$\frac{1}{2f_1}\left[2f_1X_1 + (f_5 + \sqrt{f_5^2 - af_1f_2})X_2\right] * \left[2f_1X_1 + (f_5 - \sqrt{f_5^2 - af_1f_2})X_2\right].$$

Realno število $D = f_5^2 - 4f_1f_2$ imenujemo diskriminanta realne afine stožernice podane s formo $Q(x)$. Če je $D < 0$ je stožernica elipsa, če je $D = 0$ je stožernica parabola. Če pa je $D > 0$ je stožernica hiperbola.

V projektivni ravnini obstaja le ena vrsta stožernice, v smislu, da lahko elipso preslikamo na hiperbolo ali parabolo in obratno, z linearno transformacijo. Poglejmo si sedaj zakaj je stožernica uporabna.

Segrejeva teorija:
Za lih q je množica q + 1 elementov v PG*(2, q), kjer ni nobena trojica kolinearna, stožernica.*

Dokaz: Vzemimo množico $q + 1$ točk , S, v projektivni ravnini reda q, kjer ni nobena trojica teh točk kolinearna. Vsaka od teh točk leži na $q + 1$ premicah in premice, ki jo povezujejo z ostalimi q premicami so različne. Torej leži na enolični tangentni premici, ki seka množico S le v eni točki.
(V splošnem se imenuje množica točk v projektivni ravnini ovalna, če je vsaka trojica točk nekolinearna in ima enolično tangento čez vsako točko. Segre-jeva teorija pravi, da je vsaka ovalna množica v PG(2, q), za q lih, stožernica. V realnem evklidskem prostoru obstajajo ovalne množice, ki niso stožernice. Vzemimo dve semi elipsi in ju zlepimo skupaj z dvema semi osema.)

Pokažimo, da se nobena trojica tangent ne seka v isti točki. To je odvisno od lihosti q-ja. Naj bo x_j število točk zunaj ravnine S, ki ležijo na j tangentah. Če štejemo srečanja točk zunaj množice S in i tangent za $i = 0, 1, 2$, vidimo:

$\sum x_i = q^2$, $\sum ix_i = (q+1)q$, $\sum i(i-1)x_i = (q+1)q$.

Zato je $\sum i(i-2)x_i = 0$.

Ker je število $q + 1$ točk množice S sodo, je število tangent skozi vsako točko zunaj množice S sodo. Torej zgornja vsota lahko izgine le, če je $x_i = 0$ za $i \neq 0, 2$; z drugimi besedami, vsaka točka zunaj množice S leži na nič ali dveh tangentah.

Zdaj vemo, da tri tangente tvorijo trikotnik Vzemimo točke (1, 0, 0), (0, 1, 0), (0, 0, 1) iz množice S in predvidevajmo, da imajo tangente enačbe $x_3 = \alpha x_2$, $x_1 = \beta x_3$, $x_2 = \gamma x_1$. Izračun s pomočjo dejstva, da so tangenta v točki p v množici S in premice, ki povezujejo točko p z drugimi točkami iz množice S, vse premice skozi točko p in da je produkt neničelnih elementov iz GF(q) enak –1, pokaže, da $\alpha\beta\gamma = -1$.

Lema 2.1: *Naj bodo $L_1, L_2, ..., L_n$ premice v* PG*(2, q) in se ne sekajo. Naj bodo* $p_{i1}, ..., p_{im}$ *točke na L_i ne nujno različne, vendar ne ležijo na nobeni drugi premici $L_{i'}$. Recimo, da za vsako trojico premic obstaja algebraična krivulja stopnje m, katere presek s temi premicami so točke $p'_{i1, ..., } p'_{im}$ (štete z večkratnostjo). Potem obstaja krivulja stopnje m, ki seka vsako premico le v teh točkah.*

■

S to lemo dokažemo teorijo. Če vzamemo $n = q + 1$, $m = 2$, in so $L_1, L_2, ..., L_n$ tangente množice S. Na vsaki tangenti vzemimo njen presek z množico S z večkratnostjo 2. Računanje zgoraj potrjuje lemo:

tri točke ležijo na stožernici $x_1x_2 - \beta x_2x_3 + \beta\gamma x_3x_1 = 0$, ki je tudi tangentna izbranim premicam.

Ugotovimo, da obstaja krivulja C reda 2, ki vsebuje vse točke iz množice S in nobene druge točke na tangenti. Potem ima krivulja C največ dve točki na vsaki premici in iz tega sledi, da je krivulja C natanko množica S.

■

Opomba: Za q je sod trditev ne velja [4]!

3. OSNOVNA DELITVE SKRIVNOSTI

V tem poglavju si bomo ogledali osnovne sheme za delitev skrivnosti. Predvsem pa se bomo seznanili z osnovno terminologijo in definicijami. Pogledali bomo na kakšnih osnovah lahko gradimo konstrukcije.
V razdelku 3.1. bomo predstavili osnovne definicije in pojme, ki jih bomo uporabljali tudi v naslednjih poglavjih in so zelo pomembni pri analizi varnosti shem za delitev skrivnosti.
V razdelkih 3.2. in 3.3. bomo pogledali dva osnovna modela konstrukcij shem za delitev skrivnosti, to sta Shamirjeva in Blakleyeva konstrukcija in si ogledali, kakšne so razlike med njima pri samih predstavitvah konstrukcij.
Vse pojme in lastnosti shem bomo v razdelku 3.4. predstavili bolj matematično s pomočjo formalnih definicij s funkcijami.
V razdelku 3.5. si bomo ogledali koliko informacij mora imeti vsak član pri skrivanju skrivnosti in kdaj so te informacije varne.

Poglejmo si motivacijo za uporabo shem za delitev skrivnosti. V banki imamo trezor, ki ga odpiramo vsak dan. Banka zaposli tri višje uradnike, vendar jim ne zaupa celotne šifre za odpiranje trezorja. Zato želimo narediti sistem, da bi lahko katerakoli dva uradnika skupaj odprla trezor in noben posamezen višji uradnik ne bo mogel odpreti trezorja. Ta problem lahko rešimo s shemami za delitev skrivnosti.

3.1. OSNOVE SHEM ZA DELITEV SKRIVNOSTI

Predstaviti moramo definicije in terminologijo shem za delitev skrivnosti s katerimi opisujemo lastnosti uporabnih in varnih shem. Poglejmo si poseben tip shem za delitev skrivnosti, to je delitvena shema. Za pozitivni celi števili t in w, $t \leq w$ je ***t*-*w* delitvena shema** način delitve ključa K med w članov, ki sodelujejo v shemi, tako da vsako sodelovanje t članov lahko izračuna ključ K, vendar pa nobeno sodelovanje $t - 1$ ali manj članov ne more določiti niti en sam bit ključa.
Zgornji primer z banko lahko rešimo z 2-3 delitveno shemo. Število K izbere poseben član, ki ga imenujemo delivec. Delivec, ki ga označimo z D, ne pripada množici

članov, ki v shemi sodeluje. Ko želi delivec deliti ključ K med člane, da vsakemu članu le po en del tega ključa. Te dele varno razdeli, tako da noben član ne ve kakšen del je bil dan drugemu članu. Kasneje lahko podmnožica B teh članov združi svoje zasebne dele informacije in ti skupaj izračunajo ključ K (dele lahko dajo tudi nadzorni enoti, ki jim ključ izračuna). Če velja $|B| \geq t$, potem lahko člani iz množice B izračunajo ključ s svojimi zasebnimi deli informacije, če pa je $|B| < t$ potem tega ne morejo storiti.
Izberimo še naslednje oznake za pojme, ki jih bomo uporabljali:
$\mathcal{P} = \{ P_i : 1 \leq i \leq w\}$ je množica w članov, $\mathcal{K}$ množica ključev in $\mathcal{S}$ množica delov ključa.
Rekli smo, da lahko vsaka množica s t od w članov odkrije ključ. Bolj splošno bi bilo povedati katere podmnožice lahko odkrijejo ključ in katere ne smejo. Naj bo Γ množica podmnožic iz množice $\mathcal{P}$. Elementi v množici Γ so take podmnožice članov, ki lahko izračunajo ključ K. Množico Γ imenujemo **dostopna množica** in podmnožice v Γ imenujemo **pooblaščene podmnožice**.
Naj bo $\mathcal{K}$ množica ključev in $\mathcal{S}$ množica delov ključa. Ko želi delivec D razdeliti ključ $K \in \mathcal{K}$, bo dodelil vsakemu članu nek del iz množice $\mathcal{S}$. Kasneje bodo člani želeli sestaviti ključ iz svojih podanih delov. Sedaj pa potrebujemo definicijo, ki opisuje eno izmed lastnosti varnih shem za delitev skrivnosti.

Definicija: ***Popolna shema za delitev skrivnosti****, ki realizira dostopno množico Γ je način deljenja ključa K med množico z w člani, tako da veljajo naslednji pogoji:*

- *Če združijo svoje dele ključa člani pooblaščene podmnožice $B \in \mathcal{P}$, potem lahko določijo vrednost ključa K.*
- *Če združijo svoje dele ključa člani nepooblaščene množice $B \in \mathcal{P}$, potem ne morejo odkriti nič o ključu K (nepooblaščene množice nimajo več informacij kot zunanji napadalec).*

Poglejmo si še eno lastnost v shemah za delitev skrivnosti. Recimo, da je množica $B \in \Gamma$ in $B \subseteq C \in \mathcal{P}$ in da želi podmnožica C določiti ključ K. Ker je množica B pooblaščena, lahko določi ključ K. Zato lahko podmnožica C določi ključ K s tem, da ne upošteva delov članov iz množice $C \setminus B$. Drugače povedano je množica, ki vsebuje pooblaščeno množico tudi pooblaščena. Rečemo, da so pooblaščene množice **monotone**. To pomeni, da iz $B \in \Gamma$ in $B \subseteq C \in \mathcal{P}$ sledi $C \in \Gamma$. V nadaljevanju tega poglavja bomo predpostavili, da so vse dostopne množice monotone.
Poglejmo si najmanjše dostopne množice, ki lahko odkrijejo ključ K. Naj bo Γ dostopna množica. Množica $B \in \Gamma$ je **minimalna pooblaščena podmnožica**, če iz $A \subseteq B$ in $A \neq B$ sledi $A \notin \Gamma$. Množica minimalnih pooblaščenih podmnožic množice Γ je označena z Γ_0 in jo imenujemo **baza dostopne množice** Γ. Ker množica Γ vsebuje vse pooblaščene podmnožice iz množice $\mathcal{P}$, vsebuje tudi vse podmnožice v bazi Γ_0. Torej velja $\Gamma_0 \subseteq \Gamma$ in vsaka množica iz množice Γ vsebuje vsaj eno množico iz baze Γ_0 kot svojo podmnožico. Če imamo dostopno množico Γ lahko vidimo, da Γ_0 vsebuje le minimalne pooblaščene podmnožice Γ. Tako je množica Γ določena enolično kot funkcija baze Γ_0 (t.j. $\Gamma = \{C \in \mathcal{P} : \exists\, B \subseteq C, B \in \Gamma_0\}$). Rečemo, da je množica Γ zaprtje Γ_0 in zapišemo $\Gamma = \mathrm{cl}(\Gamma_0)$. Za lažjo predstavo si oglejmo primer.

Primer 3.1:
Vzamemo množico članov $\mathcal{P} = \{P_1, P_2, P_3, P_4\}$ in bazo $\Gamma_0 = \{\{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3\}\}$.
Potem velja $\Gamma = \Gamma_0 \cup \{\{P_1, P_2, P_3\}, \{P_2, P_3, P_4\}, \{P_1, P_2, P_3, P_4\}\}$.

▲

Opomba: V primeru *t*-*w* delitvene sheme je baza sestavljena iz vseh podmnožic z natanko *t* člani.

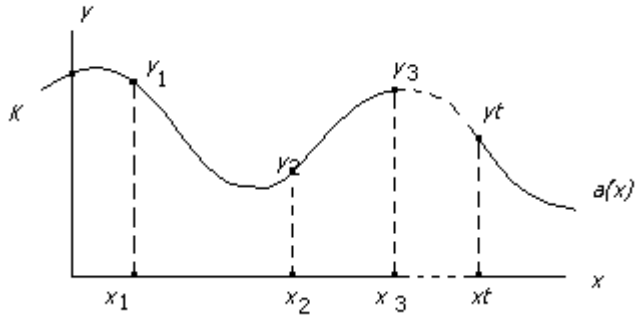
3. 2. SHAMIRJEVA DELITVENA SHEMA

En izmed načinov kako konstruirati shemo za delitev skrivnosti je leta 1979 predstavil Shamir. Poglejmo si kako lahko konstruiramo Shamirjevo *t*-*w* delitveno shemo. Ogledali si bomo postopek konstrukcije in kako varna je taka shema za delitev skrivnosti. Ogledali si bomo dva različna pristopa pri določanju ključa. En je s pomočjo sistema linearnih enačb s katerim določimo koeficiente polinoma, drug pa z Lagrangevo interpolacijo.

Naj bo množica ključev $\mathcal{K} = \mathbb{Z}_p$ kjer je $p \geq w + 1$ praštevilo. Naj bo množica delov ključa $\mathcal{S} = \mathbb{Z}_p$. Poglejmo si kako delivec pri Shamirjevi delitveni shemi deli dele ključa *K*.

KONSTRUKCIJA 3.1: (Shamirjeva konstrukcija *t*-*w* delitvene sheme)

➢ **Faza inicijalizacije:**
Delivec *D* izbere *w* različnih neničelnih elementov iz $\mathbb{Z}_p$, označimo jih z x_i, $1 \leq i \leq w$ (tu potrebujemo zahtevo $w + 1 \leq p$). Za $1 \leq i \leq w$ dodeli delivec *D* vrednosti x_i članu P_i.
➢ **Delitev delov:**
▪ Recimo, da želi delivec *D* deliti ključ $K \in \mathbb{Z}_p$. Delivec *D* skrivno določi (naključno in neodvisno) $t - 1$ delov $a_1, ..., a_{t-1}$ iz $\mathbb{Z}_p$. ▪ Za $1 \leq i \leq w$, delivec *D* izračuna $y_i = a(x_i)$, kjer je $a(x) = K + \sum_{j=1}^{t-1} a_j x^j \bmod p$. Za $1 \leq i \leq w$ da delivec *D* del y_i članu P_i.



Slika 3.1: Shamirjeva delitvena shema s polinomom.

V tej shemi delivec sestavi naključni polinom $a(x)$ (polinomi so definirani nad končnim obsegom GF(q) v tem primeru nad obsegom $\mathbb{Z}_p$), ki je največ stopnje $t - 1$ in v katerem je konstantni člen polinoma iskani ključ K. Vsak član P_i dobi točko (x_i, y_i) na tem polinomu. Poglejmo kako lahko t članov, ki sestavljajo podmnožico B, sestavi ključ s polinomsko interpolacijo.

Recimo, da člani $P_1, ..., P_t$ želijo določiti ključ K.

- Vedo, da je $y_j = a(x_j)$, $1 \le j \le t$, kjer je $a(x) \in \mathbb{Z}_p[x]$ skrivni polinom, ki ga je delivec D izbral.
- Stopnja polinoma $a(x)$ je največ $t - 1$, zato lahko polinom $a(x)$ zapišemo kot $a(x) = a_0 + a_1x + \ldots + a_{t-1}x^{t-1}$, kjer so $a_0, a_1, \ldots, a_{t-1}$ neznani elementi v obsegu $\mathbb{Z}_p$ in $a_0 = K$ je ključ.
- Ker je $y_j = a(x_j)$, $1 \le j \le t$, lahko člani podmnožice B sestavijo t linearnih enačb s t neznankami $a_0, a_1, \ldots, a_{t-1}$ in vsa aritmetika poteka v obsegu $\mathbb{Z}_p$.
- Če so enačbe linearno neodvisne, bomo imeli enolično rešitev in bo a_0 ključ, ki ga iščemo.

Očitno mora to veljati za vsake indekse $i_1, i_2, \ldots, i_t$ namesto $1,2,\ldots, t$.

Primer 3.2:
Recimo, da je $p = 17$, $t = 3$ in $w = 5$ in so $x_i = i$, $1 \le i \le 5$, javne x koordinate. Recimo, da člani iz $B = \{P_1, P_3, P_5\}$ združijo svoje dele, ki so v tem primeru 8, 10 in 11. Zapišimo polinom $a(x) = a_0 + a_1x + a_2x^2$, in izračunajmo $a(1)$, $a(3)$ in $a(5)$. Tako dobimo tri linearne enačbe:

$$a_0 + a_1 + a_2 = 8$$
$$a_0 + 3a_1 + 9a_2 = 10$$
$$a_0 + 5a_1 + 8a_2 = 11.$$

Sistem ima enolično rešitev v $\mathbb{Z}_{17}$: $a_0 = 13$, $a_1 = 10$ in $a_2 = 2$. Ključ je zatorej $K = a_0 = 13$.

▲

Trditev 3.1: *Shamirjeva t-w delitvena shema po konstrukciji* 3.1 *je popolna.*

Dokaz:
Pokažimo najprej, da lahko poljubnih t oseb iz konstrukcije 3.1 določi ključ K, t.j. reši ustrezen sistem t linearnih enačb. V splošnem imamo $y_j = a(x_j)$, $1 \le j \le t$, kjer je $a(x) = a_0 + a_1x + \ldots + a_{t-1}x^{t-1}$ in $a_0 = K$. Iz deležov t oseb dobimo naslednji sistem linearnih enačb v $\mathbb{Z}_p$

$$\begin{aligned}
a_0 + a_1 x_1 + \cdots + a_{t-1} x_1^{\,t-1} &= y_1 \\
a_0 + a_1 x_2 + \cdots + a_{t-1} x_2^{\,t-1} &= y_2 \\
\cdots \quad \cdots \quad \cdots \quad \cdots & \\
\cdots \quad \cdots \quad \cdots \quad \cdots & \\
\cdots \quad \cdots \quad \cdots \quad \cdots & \\
a_0 + a_1 x_t + \cdots + a_{t-1} x_t^{\,t-1} &= y_t,
\end{aligned}$$

ki ga zapišemo v matrični obliki :

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{t-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & x_t & x_t^2 & \ldots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \ldots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \ldots \\ y_t \end{pmatrix}.$$

Matrika A je **Vandermondova matrika**. Poglejmo si, kako lahko z matematično indukcijo dokažemo formulo za determinanto matrike A.

Formula je $\det(A) = \prod_{1 \le j < k \le t} (x_k - x_j) \bmod p$.

Za $t = 2$ trditev očitno drži. Naprej v dokazu bomo označevali x_1 le s spremenljivko x. Če matriko A razvijemo po prvi vrstici, dobimo

$$\det(A) = \sum_{i=0}^{t-1} p_i x^i . \qquad (*)$$

Torej je $\det(A)$ polinom stopnje $t - 1$ in p_i so poddeterminante determinante matrike A. Označimo polinom $\det(A)$ s $p(x)$. Če v matriki A spremenljivko x nadomestimo z x_2, $x_{3,\ldots,}$ x_t, bo $\det(A) = 0$, saj bosta po dve vrstici v matriki A enaki. Torej so x_2, $x_{3,\ldots,}$ x_t ničle polinoma $p(x)$ in velja enačba

$$p(x) = a\prod_{j=2}^{t} (x_j - x) \bmod p \qquad (**)$$

Ker je s tem polinom $p(x)$ že stopnje $t - 1$, moramo določiti le še vodilni člen a. Po enačbi (*) je vodilni člen a ravno poddterminanta p_{t-1}, ki je enaka:

$$\begin{bmatrix} 1 & x_2 & \ldots & x_2^{t-2} \\ 1 & x_3 & \ldots & x_3^{t-2} \\ 1 & \ldots & \ldots & \ldots \\ 1 & x_t & \ldots & x_t^{t-2} \end{bmatrix}.$$

Po indukcijski predpostavki pa je $\det(p_{t-1}) = \prod_{2 \le j < k \le t} (x_k - x_j) \bmod p$. V enačbi (**) namesto spremenljivke x spet pišemo x_1 in dobimo željeno formulo za determinanto matrike A.

Nadaljujmo z dokazom, da lahko t članov s svojimi deli določi ključ. Spomnimo se, da so abscise x_i vse različne, zato noben izraz $x_j - x_k$ ni enak 0. Ta produkt je izračunan v prostoru $\mathbb{Z}_p$, kjer je p praštevilo in zato je $\mathbb{Z}_p$ obseg. Ker je produkt neničelnih števil vedno neničelen v obsegu, je $\det(A) \neq 0$. Ker pa je determinanta neničelna ima sistem enolično rešitev nad obsegom $\mathbb{Z}_p$. To pove, da lahko vsako združenje t članov določi ključ K v tej delitveni shemi.
Pokažimo še, da množica z manj kot t člani ne more odkriti ključa. Kot smo opisali prej, bo $t - 1$ članov dobilo $t - 1$ enačb s t neznankami. Recimo, da predpostavijo, da je y_0 vrednost ključa K. Ker je ključ enak $a_0 = a(0)$, dodajo sistemu še to enačbo. Tako imajo t enačb in t neznank. Matrika je spet Vandermondova. Kot prej, bodo dobili enolično rešitev sistema. Zatorej za vsako vrednost y_0 dobijo enoličen polinom $a_{y0}(x)$, tako da velja $y_j = a_{y0}(x_j)$, $1 \leq j \leq t - 1$ in $y_0 = a_{y0}(0)$.
Zato ne moremo nobene vrednosti ključa izključiti kot resnično vrednost in tako skupina $t - 1$ članov ne more dobiti nobene informacije o ključu K.

■

Analizirali smo Shamirjevo shemo z vidika reševanja linearnih enačb nad obsegom $\mathbb{Z}_p$. Obstaja še druga metoda, ki sloni na Lagrangevi interpolacijski formuli za polinome. Lagrangeva interpolacijska formula je eksplicitna formula za enolične polinome $a(x)$ največ stopnje t. Formula se glasi:

$$a(x) = \sum_{j=1}^{t} y_j \prod_{1 \leq k \leq t, k \neq j} \frac{x - x_k}{x_j - x_k}.$$

Z lahkoto preverimo pravilnost formule, če vstavimo $x = x_j$. Vsi izrazi v vsoti razen j-tega izraza, ki je y_j, izginejo. Tako dobimo polinom stopnje $t - 1$, na katerem leži t točk (x_j, y_j), $1 \leq j \leq t$. V 2. poglavju smo pri interpolaciji pokazali, da je polinom stopnje $t - 1$ enolično določen s t urejenimi pari in zato da interpolacija pravi polinom. Množica B s t člani lahko izračuna polinom $a(x)$ z uporabo te interpolacijske formule. Vendar stvar lahko poenostavimo, saj člani ne potrebujejo celega polinoma $a(x)$. Dovolj je, da izračunajo konstanto $K = a(0) = a_0$. Zato lahko izračunajo sledeč izraz, ki ga dobimo, če vstavimo $x = 0$ v Lagrangevo interpolacijsko formulo:

$$K = \sum_{j=1}^{t} y_j \prod_{1 \leq k \leq t, k \neq j} \frac{x_k}{x_j - x_k}.$$

Definirajmo

$b_j = \prod_{1 \leq k \leq t, k \neq j} \frac{x_k}{x_j - x_k}$, $1 \leq j \leq t$ (vrednosti b_j lahko izračunamo prej in so lahko javne).

Potem velja $K = \sum_{j=1}^{t} b_j y_j$. Zato je ključ linearna kombinacija t zasebnih delov.

Poglejmo še poenostavljeno konstrukcijo te delitvene sheme v posebnem primeru $t = w$. Ta konstrukcija bo delovala za vsako množico ključev $\mathcal{K} = \mathbb{Z}_m$ z množico delov ključa $\mathcal{S} = \mathbb{Z}_m$. (Za to shemo ne zahtevamo, da je m praštevilo in ni potrebno, da je $m \geq w + 1$.) Če želi delivec D deliti ključ $K \in \mathbb{Z}_m$, izpelje naslednji protokol:

KONSTRUKCIJA 3.2: (soglasna t-t delitvena shema)

1. Delivec D skrivaj izbere (neodvisno in naključno) t – 1 elementov iz $\mathbb{Z}_m$, y_1, ..., y_{t-1}
2. Delivec D izračuna $y_t = K - \sum_{i=1}^{t-1} y_i \bmod m$.
3. Za $1 \le i \le t$ dodeli delivec D del y_i članu P_i.

Trditev 3.2: *Soglasna t-t delitvena shema po konstrukciji* 3.2 *je popolna.*

Dokaz: Opazimo, da lahko t članov izračuna K s formulo

$$K = \sum_{i=1}^{t} y_i \bmod m .$$

Očitno je, da prvih $t - 1$ članov ne more izračunati K, saj dobijo $t - 1$ neodvisnih in naključnih števil za svoj del. Poglejmo, kaj lahko naredi $t - 1$ članov iz množice $\mathcal{P}\backslash\{P_i\}$, kjer je $1 \le i \le t - 1$. Teh t – 1 članov ima dele $y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_{t-1}$ in velja

$$K - \sum_{i=1}^{t-1} y_i .$$

Če člani seštejejo te dele, dobijo $K - y_i$. Vendar ne vedo naključne vrednosti y_i in zato nimajo nobene informacije o vrednosti ključa K. Tako dobimo *t-t* delitveno shemo. ■

Primer 3.3:
Člani $\{P_1, P_3, P_5\}$ lahko izračunajo b_1, b_2 in b_3 po zgornji formuli. Dobili bi

$$b_j = \frac{x_3 x_5}{(x_1 - x_3)(x_1 - x_5)} \bmod 17 = 3 * 5 * (-2)^{-1} * (-4)^{-1} \bmod 17 = 4 .$$

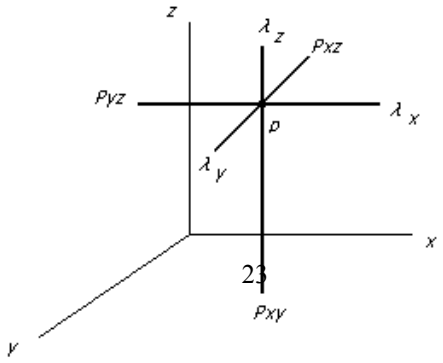
Podobno bi dobili tudi $b_2 = 3$ in $b_3 = 11$.Potem bi s svojimi deli 8, 10 in 11 dobili $K = 4 * 8 + 3 * 10 + 11 * 11 \bmod 17 = 13$.

▲

Shamir je videl, da lahko točke razdeli tako, da članom z večjimi pooblastili da več točk in s tem ustvari nivoje. Če je $t = 4$ dodeli članom prvega nivoja po dve točki, članom drugega nivoja pa po eno točko. Tako lahko dva člana prvega nivoja ali pa štirje člani drugega nivoja odkrijejo skrivnost. Možno je tudi sodelovanje po nivojih (en član prvega nivoja in dva člana drugega nivoja). Več o tem bomo povedali v naslednjem poglavju.

3.3. BLAKLEYEVA KONSTRUKCIJA

Poglejmo si še Blakleyevo konstrukcijo sheme za delitev skrivnosti. Ogledali pa si bomo še kakšna je varnost v shemah pri njegovi konstrukciji. Kasneje bomo to konstrukcijo primerjali s Shamirjevo.
Blakleyeva konstrukcija sheme za delitev skrivnosti je bolj geometrična. Za zasebne dele informacije je uporabljal izraz senca. Motivacijo za ta izraz vidimo na sliki 3.2.

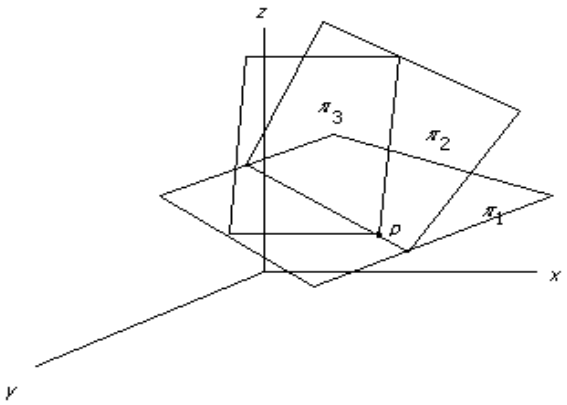


Slika 3.2: Blakleyeva konstrukcija.

Skrivnost je v tem primeru točka p v 3-razsežnem evklidskem prostoru $\mathbb{R}^3$. Točko p smo projecirali vzdolž x-osi na ravnino yz in prišli do sence točke p, ki jo označimo s p_{yz}. Podobno projeciramo točko p vzdolž y-osi in vzdolž z-osi. Dobimo senci p_{xz} in p_{xy}. Zasebni deli informacije so te tri sence p_{yz}, p_{xz} in p_{xy}. Tako dobimo 2-3 delitveno shemo. Omenimo samo, da to ni natančen opis Blakleyevega izraza senca, čeprav je ekvivalentno temu. Član i, $i \in \{ x, y, z\}$ ve, da je njegova senca projekcija skrivnosti p vzdolž i-osi. Torej ve, da točka p leži na premici λ_i, ki gre skozi njegovo podano senco in je vzporedna i-osi. Ker se vse tri premice λ_i, $i \in \{x, y, z\}$ sekajo v točki p, lahko vsak par članov določi točko p. Vsak posamezen član pa ve le to, da p leži na premici, ki jo pozna le on. Ta primer zadostuje, da lahko z njim prikažemo pomembno lastnost Blakleyeve konstrukcije shem za delitev skrivnosti. Vsak član ima prednost pri iskanju skrivnosti pred zunanjimi napadalci, ker ima svoj zasebni del informacije. Poglejmo si to bolj podrobno.
Osnovna Blakleyeva shema za delitev skrivnosti ni prikazana v evklidskem prostoru $\mathbb{R}^n$, ampak v končnem projektivnem prostoru PG(n, q) in njegova konstrukcija senc ni tako intuitivna kot smo mi prikazali na primeru 2-3 delitvene sheme. V tem primeru smo v prostoru PG(3, q), kjer leži na vsaki premici $q + 1$ točk in imamo $q^3 + q^2 + q + 1$ točk v celotnem prostoru PG(3, q). Verjetnost, da bi zunanji napadalec uganil točko p (predpostavimo, da vse točke v PG(3, q) izbiramo z enako verjetnostjo), je $(q - 1)/(q^4 - 1) \approx O(q^{-3})$, medtem ko je verjetnost, da član ugane točko p enaka $(q - 1)/(q^2 - 1) \approx O(q^{-1})$. Torej Blakleyeva shema za delitev skrivnosti ni popolna.

Premice λ_i, $i \in \{x, y, z\}$ smo izbrali tako, da so zaporedoma vzporedne x, y in z osi in s tem poenostavili primer. V projektivnem prostoru PG(3, q) ni vzporednih premic. Za projeciranje točke p lahko izbiramo poljubno med tremi različnimi premicami na katerih ta leži. Če gledamo točko p kot točko v PG(3, q) prostoru, obstaja $q^2 + q + 1$ možnih projekcij točke p (tj. premic, ki jih podaja točka p in točke na ravnini kamor smo projicirali točko p). Te projekcije določajo $q^2 + q + 1$ točk, ki ležijo v ravnini na katero projiciramo točko p. Vsak par teh premic se seka v točki p in tako jih lahko uporabimo kot zasebne dele informacije v 2-w delitveni shemi, kjer velja $w \leq q^2 + q + 1$.
Tako smo motivirali Blakleyevo uporabo izraza senca. Če izberemo namesto projekcij točke p vzdolž premice, premice v ravninah na katere smo prej točko p projicirali, potem bodo geometrični objekti, ki jih definirajo te premice in točka p, ravnine. To so tudi vse ravnine, ki ležijo v prostoru PG(3, q) in na katerih leži točka p. V tem primeru vsaka trojica teh ravnin, ki gre skozi točko p in se ne seka v skupni premici, določa točko p s svojim presekom. V splošnem velja, da se t naključno izbranih hiperravnin ($(t - 1)$-razsežnih podprostorov v prostoru PG(t, q)) skoraj gotovo seka v eni točki (glej J. W. P. Hirschfeld, Projective Geometries Over Finite Fields). Blakleyeva konstrukcija za t-w delitvene sheme se poslužuje tega geometričnega rezultata. Skrivna točka p je na naključna točka v prostoru PG(t, q) in w senc je

izbranih med $(q^t - 1)/(q - 1)$ hiperravninami na katerih leži točka p. Če je število q dovolj veliko in število vseh članov w ni preveliko, je verjetnost, da bi poljubna podmnožica t takih senc imela več kot eno točko skupno, poljubno blizu nič. Če to ni dovolj, je enostavno pregledati, če vsi pogoji neodvisnosti, v tej izbrani množici senc, veljajo. Osnovna Blakleyeva konstrukcija sheme v prostoru PG(3, q) ni sestavljena iz množice premic λ_i, ampak iz množica hiperravnin π_i na katerih leži točka p. Dobili smo 3-w delitveno shemo prikazano na sliki 3.3.



Slika 3.3: 3-w delitvena shema s presekom hiperravnin.

V prostoru PG(3, q) obstaja $q^2 + q + 1$ takih ravnin, ki vsebuje točko p, tako da za vsako število članov w, $3 \leq w \leq q^2 + q + 1$, lahko sestavimo 3-$w$ delitveno shemo. Ponovimo še, da ta shema ni popolna, saj smo videli, da zunanji napadalec ugiba točko p v prostoru PG(3, q), medtem ko člani ugibajo točko p na ravnini. Zdaj vidimo tudi, da se intuitivnost senc na sliki 3.3 ne vidi tako dobro kot na sliki 3.2, kjer je senca točke p, točka p_{ij}, $i \neq j$.

3.4. FORMALNA DEFINICIJA

V tem poglavju si bomo ogledali formalne matematične definicije za popolne sheme za delitev skrivnosti, da spoznamo matematično podlago shem za delitev skrivnosti. Sheme za delitev skrivnosti predstavimo z množico delitvenih pravil. **Delitveno pravilo** je funkcija iz množice članov $\mathcal{P}$ v množico delov ključa $\mathcal{S}$:

$$f: \mathcal{P} \rightarrow \mathcal{S}.$$

Delitveno pravilo predstavlja možno delitev zasebnih delov informacije članom, kjer je $f(P_i)$ del, ki je dodeljen članu P_i, $1 \leq i \leq w$. Naj bo za vsak ključ $K \in \mathcal{K}$, $\mathcal{F}_K$ **množica delitvenih pravil**, ki ustrezajo ključu K. Le-ta je javno znana. Definirajmo še množico vseh delitvenih pravil sheme $\mathcal{F} = \bigcup_{K \in \mathcal{K}} \mathcal{F}_K$.

Če je $K \in \mathcal{K}$ vrednost ključa, ki ga želi delivec D deliti, potem bo izbral delitveno pravilo $f \in \mathcal{F}_K$ in s tem razdelil dele. To je čisto splošen primer na katerem lahko pogledamo sheme za delitev skrivnosti. Vsako od obstoječih shem lahko opišemo s tem, da določimo katera delitvena pravila bomo uporabili.
Uporabno je zapisati pogoje, ki bodo zagotovili, da množica delitvenih pravil za shemo realizira dostopne množice. Za to si bomo ogledali porazdelitev ključev.

Vrednost P_K je **porazdelitev** ključa K na množici ključev $\mathcal{K}$. Za vsak ključ $K \in \mathcal{K}$, bo delivec D izbral delitveno pravilo v množici $\mathcal{F}_K$ glede na porazdelitev $P_{\mathcal{F}K}$. S temi porazdelitvami lahko direktno izračunamo porazdelitev na seznamu delov, ki jih dobi neka podmnožica članov B (pooblaščena ali nepooblaščena). To naredimo tako, da za množico $B \in \mathcal{P}$ definiramo množico $\mathcal{S}(B) = \{f|_B : f \in \mathcal{F}\}$, kjer je funkcija $f|_B$ zožitev delitvenega pravila f na množico B (tj. $f|_B : B \to \mathcal{S}$ je definirana z $f|_B(P_i) = f(P_i)$ za vse člane $P_I \in B$). $\mathcal{S}(B)$ je množica možnih delitvenih pravil članom iz množice B. Delitveno verjetnost na množici $\mathcal{S}(B)$, označeno s $P_{\mathcal{S}(B)}$, izračunamo na sledeč način:

- Najprej velja $P_{\mathcal{S}(B)}(f_B \mid K) = \sum_{\{f \in \mathcal{F}_K : f|_B = f_B\}} P_{\mathcal{F}K}(f)$ za vse $f_B \in \mathcal{S}(B)$ in $K \in \mathcal{K}$.
- Potem je za $f_B \in \mathcal{S}(B)$

$$P_{\mathcal{S}(B)}(f_B) = \sum_{K \in \mathcal{K}} P_{\mathcal{F}}(f_B \wedge K) =$$
$$= \sum_{K \in \mathcal{K}} P_{\mathcal{K}}(K) P_{S(B)}(f_B \mid K) =$$
$$= \sum_{K \in \mathcal{K}} P_{\mathcal{K}}(K) \sum_{\{f \in \mathcal{F}_K : f|_B = f_B\}} P_{\mathcal{F}K}(f) .$$

Poglejmo zdaj formalno definicijo za popolne sheme za delitev skrivnosti.

Definicija: *Naj bo Γ dostopna množica in naj bo $\mathcal{F} = \prod_{K \in \mathcal{K}} \mathcal{F}_K$ množica delitvenih pravil. $\mathcal{F}$ je popolna shema za delitev skrivnosti, ki realizira dostopno množico Γ, če zadošča naslednjima pogojema:*

1. *Za vsako pooblaščeno podmnožico članov $B \in \mathcal{P}$ ne obstajata delilni pravili $f \in \mathcal{F}_K$ in $f' \in \mathcal{F}_{K'}$ z $K \neq K'$, za katere bi veljalo $f|_B = f'|_B$ (vsaka delitev delov članom, v pooblaščeni podmnožici B, določa vrednost ključa.)*
2. *Za vsako nepooblaščeno podmnožico članov $B \in \mathcal{P}$ in za vsako delitev delov $f_B \in \mathcal{S}_B$, velja $P_{\mathcal{K}}(K|f_B) = P_{\mathcal{K}}(K)$ za vsak ključ $K \in \mathcal{K}$. (Pogojna porazdelitev na množici ključev $\mathcal{K}$, če imamo podane delitve delov f_B nepooblaščeni podmnožici B, je enaka začetni porazdelitvi na množici ključev $\mathcal{K}$. Z drugimi besedami, delitev delov članom iz podmnožice B ne poda nobene informacije o vrednosti ključa.)*

Porazdelitev ključa K pri delitvenem pravilu f_B (označimo z $P_{\mathcal{K}}(K|f_B)$) lahko izračunamo po formuli ( ) iz 2. poglavja:

$$P_{\mathcal{K}}(K \mid f_B) = \frac{P_{\mathcal{S}(B)}(f_B \mid K) P_{\mathcal{K}}(K)}{P_{\mathcal{S}(B)}(f_B)} .$$

Za lažjo predstavo si poglejmo primer.

Primer 3.4:

Imamo množico članov $\mathcal{P} = \{P_1, P_2, P_3, P_4\}$. Vzemimo dve množici delitvenih pravil $\mathcal{F}_0$ in $\mathcal{F}_1$, ki vsebujeta 16 enako verjetnih delitvenih pravil. V tabeli vsaka vrstica v $\mathcal{F}_0$ in $\mathcal{F}_1$ predstavlja eno delitveno pravilo.

$\mathcal{F}_0$			
P_1	P_2	P_3	P_4
0	0	0	0
0	1	1	3
0	2	3	1
0	3	2	2
1	0	4	0
1	1	5	3
1	2	7	1
1	3	6	2
2	4	0	0
2	5	1	3
2	6	3	1
2	7	2	2
3	4	4	0
3	5	5	3
3	6	7	1
3	7	6	2

$\mathcal{F}_1$			
P_1	P_2	P_3	P_4
0	0	1	1
0	1	0	2
0	2	2	0
0	3	3	3
1	0	5	1
1	1	4	2
1	2	6	0
1	3	7	3
2	4	1	1
2	5	0	0
2	6	2	2
2	7	3	3
3	4	5	1
3	5	4	2
3	6	6	0
3	7	7	3

Tabela 3.1: Delitvena pravila shem za delitev skrivnosti

Dobimo popolno shemo za delitev skrivnosti za vsako porazdelitev ključa. V tem primeru ne bomo vsega preverjali, ampak si bomo ogledali nekaj tipičnih primerov uporabe pogojev v definiciji. Podmnožica $\{P_2, P_3\}$ je pooblaščena. Dela, ki ju člana P_2 in P_3 dobita določata enoličen ključ. Lahko vidimo, da se vsaka delitev delov tema dvema članoma v delitvenem pravilu zgodi največ enkrat, v množici $\mathcal{F}_0$ ali $\mathcal{F}_1$. Recimo, če P_2 dobi 3 in P_3 dobi 6, potem mora biti to osmo delitveno pravilo v $\mathcal{F}_0$. Zato je ključ 0, ker je to pravilo v množici $\mathcal{F}_0$. Če pa je $B = \{P_1, P_2\}$, je to nepooblaščena podmnožica. Ni težko videti, da vsaka delitev delov tema dvema članoma ustreza največ enemu delitvenemu pravilu v množici $\mathcal{F}_0$ in največ enemu delitvenemu pravilu v množici $\mathcal{F}_1$.

To pomeni, da $P_{S(B)}(f_B \mid K) = \frac{1}{16}$ za vsak $f_B \in \mathcal{S}(B)$ in za $K = 0, 1$.

Izračunajmo še $P_{S(B)}(f_B) = \sum_{K \in \mathcal{K}} P_{\mathcal{K}}(K) \sum_{\{f \in \mathcal{F}K : f|_B = f_B\}} P_{\mathcal{F}K}(f) = \sum_{K=0}^{1} P_{\mathcal{K}}(K) * \frac{1}{16} = \frac{1}{16}$.

Uporabimo še Beyesevo formulo za izračun $P_{\mathcal{K}}(K|f_B)$:

$$P_{\mathcal{K}}(K \mid f_B) = \frac{P_{S(B)}(f_B \mid K) P_{\mathcal{K}}(K)}{P_{S(B)}(f_B)} = \frac{\frac{1}{16} * P_{\mathcal{K}}(K)}{\frac{1}{16}} = P_{\mathcal{K}}(K),$$

Torej velja tudi drugi pogoj za podmnožico B. Podobne izračune naredimo tudi za druge pooblaščene in nepooblaščene množice in vsi zadoščajo pogojema. Torej imamo res popolno shemo za delitev skrivnosti.

▲

Poglejmo si še en pojem, ki povezuje informacije, ki jih morajo skrivati člani, in učinkovitost shem za delitev skrivnosti. V splošnem merimo učinkovitost sheme za delitev skrivnosti po razmerju informacij.

Definicija: *Za popolno shemo za delitev skrivnosti, ki realizira dostopno množico Γ, je* ***razmerje informacij*** *za člana P_i količina*

$$\rho_i = \frac{\log_2 |\mathcal{K}|}{\log_2 |\mathcal{S}(P_i)|}.$$

$\mathcal{S}(P_i)$ označuje množico možnih delov, ki jih član P_i lahko dobi. Velja $\mathcal{S}(P_i) \subseteq \mathcal{S}$. ***Celotno razmerje informacij*** *za shemo označimo s ρ in je definirano kot:*

$$\rho = \min\{\rho_i : 1 \le i \le w\}.$$

Poglejmo si motivacijo za to definicijo. Ker ključ K dobimo iz končne množice $\mathcal{K}$, si lahko ključ K predstavljamo kot bitno zaporedje dolžine $\log_2|\mathcal{K}|$, torej je vsebina informacije ključa K dolga $\log_2|\mathcal{K}|$ bitov. Na podoben način je lahko del, ki ga dobi član P_i, predstavljen kot bitno zaporedje dolžine $\log_2|\mathcal{S}(P_i)|$. Tako je ρ_i razmerje števila bitov v delu, ki ga član dobi, s številom bitov v ključu.

V Shamirjevi shemi, če gledamo skrivnost kot točko, je razmerje informacij enako 1. V shemah si želimo čim večje razmerje informacij. Velja pa naslednja trditev:

Trditev 3.3: *V vsaki popolni shemi za delitev skrivnosti, ki realizira dostopno množico Γ, je $\rho \le 1$.*

Dokaz: Imamo popolno shemo za delitev skrivnosti, ki realizira dostopno množico Γ. Vzemimo množica $B \in \Gamma_0$ in vzemimo enega člana $P_j \in B$. Definirajmo $B' = B \setminus \{P_j\}$. Vzemimo delitveno pravilo $g \in \mathcal{S}(B)$. Vidimo, da $B' \notin \Gamma$, zato delitev delov $g|_{B'}$ ne da nobene informacije o ključu. Zato za vsak ključ $K \in \mathcal{K}$ obstaja delitveno pravilo $g^K \in \mathcal{F}_K$, da velja $g^K|_{B'} = g|_{B'}$. Ker za množico B velja $B \in \Gamma$, mora veljati $g^K(P_j) \neq g^{K'}(P_j)$, če je $K \neq K'$. Zato je $|\mathcal{S}(P_j)| \ge |\mathcal{K}|$ in tako je $\rho \le 1$. ■

Ker je $\rho = 1$ optimalna situacija za popolne sheme, rečemo takim shemam **idealne sheme**. V idealnih shemah za delitev skrivnosti je poljubna točka, ki si jo izberemo v prostoru v katerem delujemo, z enako verjetnostjo ali skrivna točka ali pa točka, ki je bila podana kot zasebni del informacije. Shamirjeve sheme so torej idealne sheme za delitev skrivnosti. Blakleyeve konstrukcije shem so v splošnem daleč od idealnih, saj mora imeti vsak član dovolj informacij, da lahko identificira svojo senco ($(k-1)$-razsežno hiperravnino). To zahteva k koordinat, torej k elementov iz obsega GF(q). Po drugi strani pa ima nedovoljeno sodelovanje $k-1$ članov le linearno negotovost skrivnosti p, saj se njihovih $k-1$ hiperravnin sekaja v premici, ki vsebuje

točko p. To pomeni, da ugibajo le eno koordinato od vsega $q + 1$ točk, vsak član pa varuje k elementov, $k \geq 2$, iz GF(q) za svoj zasebni del informacije.

3.5. SPLOŠNI MODELI

Shamirjeve in Blakleyeve sheme so osnovni modeli za konstrukcijo ostalih shem za delitev skrivnosti. Kakorkoli sta ta dva majhna primera različna, se v določenih pogledih ujemata. Vendar mi želimo ravno na razlikah preučiti in razumeti sheme za delitev skrivnosti.
V podrazdelku 3.5.1. si bomo ogledali razlike med njima. Primerjali bomo:

- Kako v posameznih shemah sestavljamo in delimo podatke in kakšen vpliv ima to na odkrivanje skrivnosti?
- Kako se konstrukciji razlikujeta v samem postopku in na kaj moramo pri posamezni konstrukciji paziti?
- Kakšna je varnost v posameznih konstrukcijah?
- Kolikšna je količina informacij, ki jo skrivajo člani?

V podrazdelku 3.5.2. si bomo pogledali kako izgledajo te sheme, če jih pogledamo z vidika kriptografije in kriptografskih ključev.
V podrazdelku 3.5.3. pa bomo vpeljali tudi splošnejšo terminologijo prostorov, ki jo bomo uporabljali v naslednjih poglavjih.

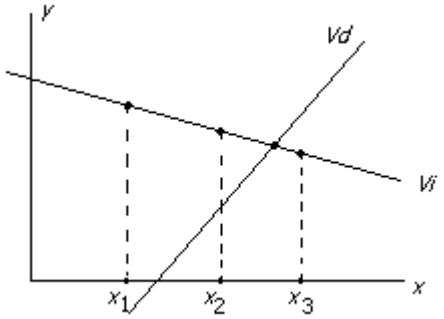
3.5.1. RAZLIKE PRI SHAMIRJEVIH IN BLAKLEYEVIH SHEMAH

Lotimo se postopnega primerjanja teh shem za delitev skrivnosti. Najprej bomo razlike le omenili in malce opisali, kasneje pa bomo pomembnejše razlike tudi analizirali.
Brez izgube splošnosti lahko rečemo, da je skrivnost vedno točka p v nekem primerno izbranem prostoru. Naloga sheme za delitev skrivnosti je, da vsaki pooblaščeni množici dovoljuje dostop do skrivnosti in vsaki nepooblaščeni množici to prepreči. Tem pogojem zadostujeta Shamirjeva in Blakleyeva shema, ki smo si ju ogledali na t-w delitvenih shemah, kjer mora t ali več članov sodelovati, da pridejo do skrivnosti. Poseben primer je bil $t = w$ oziroma soglasna delitvena shema.
Najprej pa poglejmo, kako lahko delimo dele članom v shemah. Obstajata dva različna načina, kako lahko razdelimo zasebne dele informacije članom, tako da pooblaščene množice lahko odkrijejo skrivnost, nepooblaščene pa ne. V prvem primeru (Shamir) je skrivnost skrita dokler ne združimo čisto vseh informacij, medtem ko se pri Blakleyu prostor, v katerem leži skrivnost, zmanjšuje, dokler ne ostane le še sama skrivnost. Obstaja mnogo uporab in primerov za ta dva razreda. Najbolj naravne rešitve vsebujejo kombinacije teh dveh razredov. Pri realnih uporabah so lahko te sheme in sodelovanja zelo zapletena.
V banki potrebujemo za odpiranje trezorja sodelovanje dveh podpredsednikov *ali* sodelovanje treh višjih uradnikov[1]. Da realiziramo tako delitveno shemo, moramo osnovni model shem za delitev skrivnosti razširiti oziroma posplošiti in narediti večnivojsko shemo. O njej bomo govorili v naslednjem poglavju.
V Shamirjevih shemah ima vsak član točko na polinomu $a(x)$ stopnje $t - 1$, na katerega lahko gledamo kot geometričen objekt. Torej polinom $a(x)$ določa t članov

[1] Lahko bi kombinirali tudi sodelovanje podpredsednika in dveh višjih uradnikov.

oziroma njihovih t zasebnih delov informacije. To bomo posplošili tako, da bo geometrični objekt (ponavadi m-razsežen prostor vsebovan v nekem prostoru S višje dimenzije), ki ga napenjajo zasebni deli informacije članov pooblaščene množice, kazal na skrivno točko p v nekem drugem geometričnem objektu (ponavadi tudi podprostor prostora S). Večino naših konstrukcij bo take oblike.
V Blakleyevih shemah imajo člani za svoje zasebne dele informacije geometrične objekte, po njegovi konstrukciji so to hiperravnine, ki vsebujejo točko p. V enostavni delitveni shemi se vsaka podmnožica takih t objektov seka ravno v točki p.
Poglejmo si najmanjši možni primer sheme za delitev skrivnosti. To je 2-w delitvena shema. Shamirjevo konstrukcijo vidimo na sliki 3.4. V tem primeru je $a(x)$ linearen polinom.

KONSTRUKCIJA 3.3: (2-razsežen prostor skrivnosti)



Slika 3.4: Posplošena Shamirjeva shema za delitev skrivnosti.

1. *Premica V_d je javno znana.*
2. *Zasebne dele informacije predstavlja w paroma različnih točk na premici V_i, ki so dodeljene članom te sheme.*
3. *Presek premice V_i in V_d je skrivna točka $p = (x_p, y_p)$.*

Trditev 3.4: *Shema po konstrukciji* 3.3 *ima naslednje lastnosti:*

- *Negotovost točke p je le $H(p) = \log_2(q)$ bitov.*
- *Člani hranijo skrivno le y-koordinato svoje točke in pri deljenju zasebnih delov premica V_i ne sme biti vzporedna y-osi.*
- *Negotovost točke p je v primeru zunanjega napadalca kot tudi notranjega člana enaka $H(p) = \log_2(q)$ (tj. Shema je popolna).*

Dokaz:

- Pri konstrukciji 3.3 leži skrivna točka p na javno znani premici V_d. Torej iščemo le točko na premici. Negotovost točke p je $H(p) = \log_2(q)$.
- Če v afini ravnini AG(2, q) uporabimo koordinate za opis točke $p_i = (x_i, y_i)$, potem je dovolj (za varnost te sheme za delitev skrivnosti), da ima vsak član v lasti le po eno koordinato (recimo y_i). Pri tem deljenju zasebnih in javnih delov, premica V_i v afini ravnini ne sme biti vzporedna y-osi, saj bi bili tako javni deli vsi enaki $x_i = x_p$ za vsak i in tako lahko le iz javnih delov odkrili premico V_i in s tem tudi skrivnost p.
- Kar želimo poudariti je verjetnost, ki jo imajo nepooblaščene množice, da odkrijejo skrivnost p:
  1. Zunanji napadalec ve, da obstaja premica V_d in premica V_i, ki seka premico V_d v točki p. Iz javnih delov informacije, ne more ugotoviti več kot to, da

točka p leži na premici V_d. Ker vsaka od q točk na premici V_d leži na enakem številu premic, ki gre skozi njih in niso vzporedne y-osi, so lahko vse te premice kandidat za premico V_i. Torej je nasprotnikova negotovost skrivne točke p enaka $H(p) = \log_2(q)$. To je njegova verjetnost, da ugane točko p s pomočjo naključnih točk na V_d.

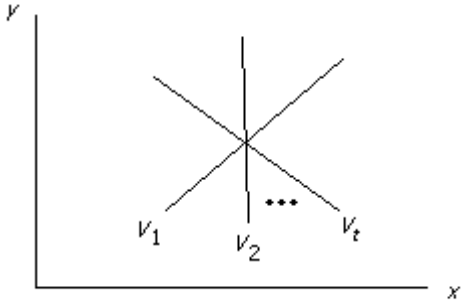
2. Poglejmo si negotovost notranjega člana. Član pozna svoj zasebni del informacije p_i na premici V_i. Pozna še javne abscise x_j, $j \neq i$ drugih članov in premico V_d. Vsaka točka p' na V_d določa enolično premico, ki gre skozi p' in p_j in je lahko neznana premica V_i. Negotovost točke p je enaka kot za zunanjega napadalca, ki nima dostopa do zasebnih delov informacije, $H(p) = \log_2(q)$.

To sta edina dva primera, ki sta pomembna, saj nobena kombinacija združenj med zunanjim napadalcem in članom ne more odkriti več kot član sam. Torej je to 2-w popolna delitvena shema.

■

Poglejmo si še Blakleyevo konstrukcijo za 2-w delitveno shemo.

KONSTRUKCIJA 3.4: (1-razsežen prostor skrivnosti)



Slika 3.5: Presek premic, ki določajo točko p.

1. V tem primeru so zasebni deli informacije premice na katerih leži točka p.

Trditev 3.5: *Shema po konstrukciji* 3.4 *ni popolna.*

Dokaz: Za zunanjega napadalca je vsaka točka v ravnini enako verjetna za skrivnost p, zato je negotovost točke p enaka $H(p) = \log_2(q^2) = 2\log_2(q)$. Notranji član pa ve, da mora točka p ležati na njegovi premici in zato je negotovost enaka $H(p) = \log_2(q)$. Zato ta shema ni popolna, saj imajo člani več informacij kot zunanji napadalci.

■

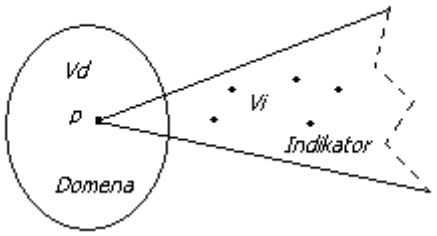
Obe shemi zagotavljata enak minimalen nivo varnosti pred nepooblaščenim odkritjem skrivnosti. Iz tega vidika, sta obe shemi enako dobri. Pogledati moramo še druge faktorje kot so, za kakšno količino in vsebino informacij mora biti vsak član odgovoren. Ker je ravnina 2-razsežna, vidimo, da imajo lahko člani za zasebne dele informacije le količino informacij, ki je ekvivalentna vrednosti ene koordinate, to je $\log_2(q)$ bitov. S tem bo zagotovljena tudi celovitost informacije. Varnost lahko merimo tudi z najmanjšo negotovostjo, ki jo imajo nepooblaščeni člani oziroma nepooblaščene množice pri odkrivanju skrivnosti p ($\log_2(q)$ v obeh primerih).

3.5.2. KRIPTOGRAFSKI KLJUČI

Oglejmo si prejšnji konstrukciji s pomočjo kriptografije [1]. Ko smo definirali točko p na premici V_d, smo merili varnost z negotovostjo točke p. Kot smo videli je bila ta enaka tako za člane kot za zunanje napadalce. Poglejmo ta primer malo drugače. Recimo, da je V_i kriptografski ključ, ki šifrira besedilo (ordinato) zasebnih delov informacije v tajnopis (absciso). To se ujema z našim dogovorom, da je treba varovati vrednost ordinate in da lahko vrednost abscise objavimo. Skrivnost je dešifrirana vrednost tajnopisa (abscise x_p, skrivne točke p), ki jo dobimo s pomočjo ključa V_i. Če je v enostavni geometrični konstrukciji 2-w delitvene sheme premica V_i definirana kot kriptografska transformacija, ne sme biti vzporedna y-osi, da lahko preslika y-os na x-os. Če bi bila premica V_i vzporedna y-osi, bi bili lahko zasebni deli informacije odkriti.
Izračunajmo negotovost ključa v tem primeru. Zunanji napadalec ve, da je V_i premica, ki ni vzporedna y-osi. Med $q^2 + q$ premicami je takih le q^2 premic, saj je q premic vzporednih y-osi. Zato je negotovost $H(V_i) = \log_2(q^2) = 2\log_2(q)$, to pa je dvakrat negotovost ordinate y_p, zašifrirane vrednosti skrivnosti p. Premica V_d je v tej implementaciji premica vzporedna y-osi na kateri leži točka p.
Poglejmo si še negotovost skrivne točke p za zunanjega napadalca. Obstaja $q + 1$ premic skozi vsako točko na premici V_d, med njimi tudi sama V_d, ki pa ni kandidat za premico V_i. Imamo torej q^2 potencialnih ključev (premic v AG(2, q), ki niso vzporedne y-osi), ki so porazdeljeni, tako da gre q premic skozi vsako od q točk na premici V_d. Zato velja $H(p) = \log_2(q)$.
Poglejmo si zdaj primer notranjega člana. Le-ta pozna točko na neznanem ključu V_i. Obstaja $q + 1$ premic skozi to točko in q od njih je potencialnih ključev. Torej je negotovost za vsakega člana enaka $H(V_i) = H(p) = \log_2(q)$.

3.5.3. TERMINOLOGIJA IN ANALIZA KONSTRUKCIJ

Pogledali si bomo, kaj lahko ugotovimo iz zgornjih primerov in uvedli novo terminologijo za skrivnost in prostore, ki smo jih uporabili pri konstrukcijah. Na koncu pa bomo analizirali različne konstrukcije.
Konstrukciji 3.3 in 3.4 vsebujeta vse pomembne lastnosti splošnih modelov, ki jih bomo uporabljali pri dveh tipih shem za delitev skrivnosti ne glede na to kako zapletene bodo in kakšne dodatne lastnosti bodo imele. V prvem tipu shem obstaja geometrični objekt (algebraične vrste, v splošnem linearen podprostor v prostoru višje dimenzije), ki ga določa pooblaščena množica točk v njem. Ta geometrični objekt seka drug geometričen objekt le v eni točki, točki p, s katero je skrivnost določena. En izmed teh dveh geometričnih objektov je vedno skriven (vsaj dokler ne pride do pooblaščenega sodelovanja med člani), medtem ko je drugi ponavadi javen. Javnega imenujemo domena V_d, saj gledamo nanj kot množico kjer je skrita skrivnost p. Drugega, ki ga razdelimo med člane, imenujemo indikatorska množica oziroma podprostor V_i, saj kaže na točko p v podprostoru V_d. Poglejmo si sliko 3.6.



Slika 3.6: Predstavitev nove terminologije.

Velja: $\dim(V_d) + \dim(V_i) = \dim(S)$ in $\dim(\text{Lin}^* (V_d \cap V_i)) = 0$.
Ena skrivnost ima lahko več indikatorskih množic ali več domen, odvisno od vrste sodelovanja v shemi, ki jo realiziramo. V konstrukciji 3.3 je bila indikatorska množica V_i premica, ki smo jo določili s parom točk. Premico V_i bi lahko nadomestili tudi s stožernico (določeno s tremi točkami) ali kubično krivuljo (določeno s štirimi točkami, ki ne ležijo na kvadratni krivulji). V naših primerih se bomo z V_i in V_d ponavadi omejili na linearne podprostore v prostorih višje dimenzij. V primeru, ko velja $\dim(V_i) = t - 1$ in $w = t$, tako da potrebujemo vse zasebne dele informacije, da napnemo podprostor V_i, dobimo soglasno *t-t* delitveno shemo.
Pri drugem tipu shem si bomo ogledali le *t-t* soglasne delitvene sheme. S podanim parametrom *t* je shema implementirana v *t*-razsežnem prostoru $S = \text{PG}(k, q)$. Zasebni deli informacije so naključno izbrane hiperravnine ($(k - 1)$-razsežni podprostori prostora *S*), ki se skoraj gotovo (z večanjem števila *q*) sekajo le v eni točki, v točki *p*. To je posplošitev konstrukcije 3.3 z enim parom premic v ravnini, $t = 2$, in konstrukcije 3.4 s tremi ravninami v prostoru, $t = 3$. Tako lahko t-w delitvene sheme takega tipa naredimo za vse *w*, $t \le w \le (q^{k-1})/(q - 1)$.
Večinoma se bomo zanimali le za sheme prvega tipa, kjer je *S* projektivni prostor $\text{PG}(n, q)$ nad končnim obsegom $\text{GF}(q)$. Naši primeri pa bodo konstruirani v afinem prostoru $\text{AG}(n, q)$, zaradi analogije evklidskim prostorom.
Naše konstrukcije uporabljajo enostaven rezultat projektivne geometrije imenovan rang formula:

$$r(U) + r(V) = r(U \cap V) + r(U \cup V) \qquad (1)$$

Formula velja za vse podprostore *U* in *V* v prostoru $S = \text{PG}(n, q)$. Vrednost $r(x)$ poda rang podprostora *x*. Velja še $r(x) = \dim(x) + 1$ in da ima prazen podprostor rang 0 ter dimenzijo –1. Formula (1) ne velja v afinem prostoru. V afinem prostoru $\text{AG}(3, q)$ obstaja par vzporednic oziroma par premic, ki se ne sekajo in katerih unija je ravnina:
$r(U \cap V) = 0$
$r(U \cup V) = 3$.
$r(U) + r(V) = 2 + 2 \neq r(U \cap V) + r(U \cup V) = 0 + 3$.
Intuitivno je morda bolje, če v (1) zamenjamo rang z dimenzijo:

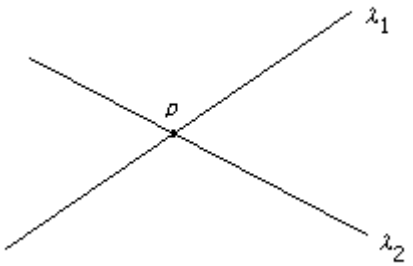
$$\dim(U) + \dim(V) = \dim(\text{Lin}(U \cap V)) + \dim(\text{Lin}(U \cup V)) \qquad (2)$$

Konstrukcije pri katerih je unija prostorov V_i in V_d cel prostor *S* in presek točka *p*, kjer je *p* točka, omogočajo popolno *t-w* delitveno shemo za vsako izbiro parametrov *t* in *w*.

* Lin je linearna ogrinjača prostorov.

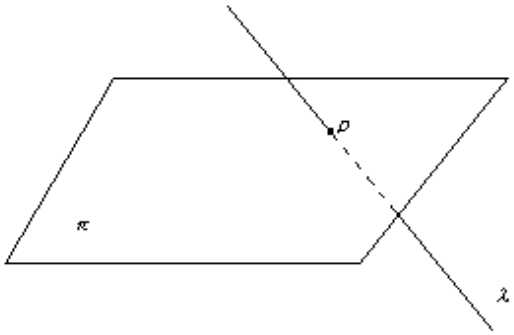
Za dano število q je mogoče izbrati razsežnost in s tem kardinalnost domene V_d tako, da negotovost nepooblaščene množica zadošča varnostnim pogojem shem za delitev skrivnosti. Naj bo $dim(V_d) = m$. Prostor S, ki vsebuje domeno V_d, naj bo n-razsežen in naj velja $m + k - 1 = n$. Naj bo V_i $(k - 1)$-razsežen podprostor izbran tako, da je $\dim(\text{Lin}(V_i \cap V_d)) = 0$. Zasebni deli informacije so točke različne od točke p v podprostoru V_i izbrane tako, da vsaka podmnožica k točk napenja podprostor V_i in noben podprostor, ki ga napenja manj kot k točk, ne vsebuje točke p. To zagotovi, da bo lahko vsaka množica k ali več članov prišla do podprostora V_i in s tem do točke p. Še vedno pa bo vsaka točka v domeni V_d enako verjeten kandidat za točko p pri sodelovanju manj kot k članov. Oglejmo si nekaj primerov konstrukcij.

1. Ogrinjača dveh različnih nevzporednih premic λ_1 in λ_2 definira ravnino. Presek premic λ_1 in λ_2 pa določa točko p:



Slika 3.7: Presek dveh premic določa točko p.

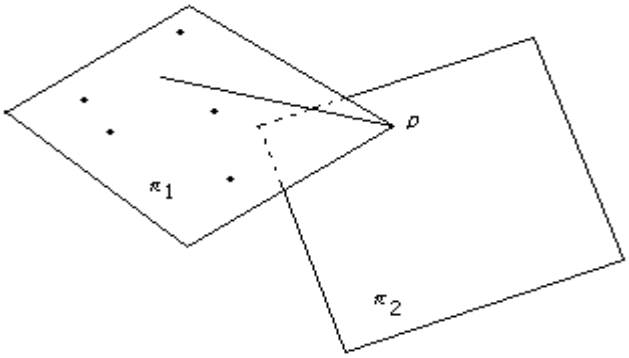
2. Podobno ogrinjača ravnine π in premice λ, ki ne leži v ravnini, definira 3-razsežen prostor. Presek ravnine π in premice λ pa je točka p:



Slika 3.8: Presek premice in ravnine v točki p.

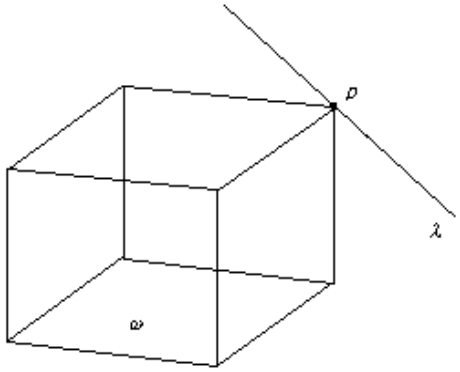
V ravnini ali pa v 3-razsežnem prostoru sta to edini konstrukciji tega tipa. V naslednjih primerih, kjer je S 4-razsežni prostoru, bo prišla formula (2) do izraza.

3. Ravnini, ki razpenjata 4-razsežen prostor, se sekata v eni sami točki, saj velja $\dim(\text{Lin}(U \cap V)) = \dim(\text{Lin}(U \cup V)) - \dim(U) - \dim(V) = 4 - 2 - 2 = 0$. To prikazuje slika 3.9.



Slika 3.9:Presek dveh 3-razsežnih prostorov.

4. Podobno imata 3-razsežni podprostor ω in premica λ, ki napenjata 4-razsežen prostor S, skupno le eno točko p.



Slika 3.10: 3-razsežni prostor in premica določata točko p.

Zaenkrat nam slike 3.7-3.10 prikazujejo vse kar moramo vedeti o delitvenih shemah. Na sliki 3.7 smo videli, da lahko 2-w delitveno shemo implementiramo s konstrukcijo, v kateri izberemo w točk na eni premici za zasebne dele informacije. Konstrukcija na sliki 3.8 je drugačna. 2-w delitvena shema je mogoča le, če so zasebni deli informacije točke na premici. Veliko več shem pa je možnih, če so zasebni deli informacije točke v ravnini. Če jih izberemo tako, da nobena trojica točk ni kolinearna in noben par ni kolinearen s točko p, potem vsaka trojica določa ravnino in s tem točko p. Noben par točk ali le ena točka pa ne more določiti točke p (točka p je v tem primeru skrivna točka na javni premici λ). Enake opombe veljajo za konstrukcijo na sliki 3.9 le s to izjemo, da je lahko točka p katerakoli točka na ravnini.

4. VEČNIVOJSKE IN VEČSKUPINSKE SHEME ZA DELITEV SKRIVNOSTI

V tem poglavju si bomo pogledali **večnivojske** in **večskupinske** sheme za delitev skrivnosti ter geometrijsko ozadje, ki nam pomaga pri konstrukcijah. Večnivojske in večskupinske sheme so zelo uporabne pri delitvi skrivnosti. Da bi jih bolje razumeli bomo predstavili konstrukcije, ki nam povejo kako te sheme delujejo. Sheme morajo biti seveda enostavne, da jih lažje uporabljamo. Zato jih bomo skušali kar se da poenostaviti.
V razdelku 4.1. bomo govorili o večnivojskih shemah, ki nam bodo prikazale kakšna pooblastila imajo člani po nivojih. Ogledali si bomo odvisne in neodvisne sheme za delitev skrivnosti.
V razdelku 4.2. bomo pogledali večskupinske sheme in kakšne so možne konstrukcije za popolnoma varne večskupinske sheme za delitev skrivnosti.
V razdelku 4.3. si bomo ogledali posplošitev večnivojskih in večskupinskih shem. Začeli bomo z izbiro indikatorja in domene in minimaliziranje števila članov v shemah nato pa si bomo ogledali kombinacijo med večnivojskimi in večskupinskimi shemami. Opisali pa bomo tudi vse uporabljene geometrije in zapisali formule po katerih smo dobili število podprostorov v nekem afinem oziroma projektivnem prostoru.
Ponovimo oznake, ki jih uporabljamo v konstrukciji shem. Podprostor ključev oziroma podprostor v katerem skrivnost skrivamo (domena) je označen z V_d. Podprostor zasebnih delov informacij (indikatorski podprostor) smo označili z V_i (za indikatorski podprostor bomo uporabili še oznaki V_1 in V_2, ki bosta označevala prvi in drugi nivo večnivojske sheme). Naše konstrukcije predstavljamo v prostoru S, ki ga V_d in V_i razpenjata.

4.1. VEČNIVOJSKA SHEMA ZA DELITEV SKRIVNOSTI

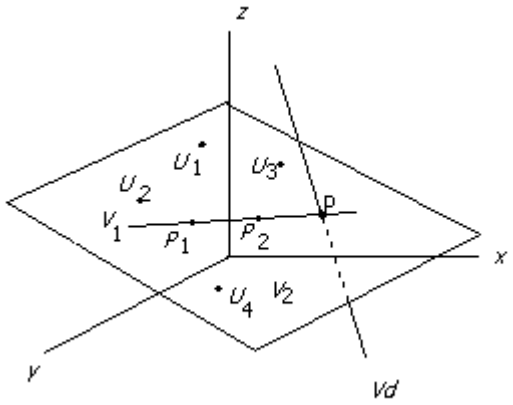
Poglejmo si najprej večnivojske sheme in njihove konstrukcije. Zanima nas kako lahko povezujemo nivoje med seboj in kakšna so pooblastila po nivojih.

Poglejmo si primer banke. Tu si izberemo tri različne nivoje katerih člani lahko odobrijo transakcijo denarja pod določenimi pogoji, ki jih bomo opisali. Poglejmo si tri take kombinacije:

- dva podpredsednika lahko delujeta namesto predsednika, torej lahko odobrita transakcijo denarja (do neke določene vsote);
- trije višji upravniki to naredijo namesto podpredsednikov;
- en podpredsednik in dva višja uradnika lahko sprožita transakcijo (s tem so nivoji med seboj povezani).

To bi pomenilo, da vsak sodelujoči lahko deluje v svojem razredu oziroma nivoju, hkrati pa še v vsakem nižjem nivoju od svojega. Oglejmo si to v konstrukciji 4.1.

KONSTRUKCIJA 4.1: (2 nivoja, 1-rezsežen prostor skrivnosti)



Slika 4.1: Popolna delitvena shema pri transakciji denarja.

1. *Imamo m višjih uradnikov $U_1,..., U_m$ in n podpredsednikov $P_1,..., P_n$ (na sliki* 4.1 *so uradniki in podpredsedniki predstavljeni s točkami).*
2. *Izberemo premico V_1. Vsakemu Podpredsedniku $P_1,.., P_n$ dodelimo po eno točko s premice V_1, ki seka premico V_d (ki je javni podatek) v točki p.*
3. *Izberimo ravnino V_2. Višjim uradnikom $U_1,..., U_m$ dodelimo vsakemu po eno od točk iz ravnine V_2 vendar te točke ne smejo ležati na premici V_1. Vsak par točk višjih uradnikov je nekolinearen s točkami, ki so dodeljene podpredsednikom iz premice V_1 in nekolinearen s točko p.*

Premica V_d je javna informacija in jo poznajo vsi člani sheme.
Poglejmo nekaj enostavnejših lastnosti te konstrukcije, ki jih ne bomo dokazovali.

Trditev 4.1: *Shema za delitev skrivnosti poteka po konstrukciji* 4.1. *Potem velja naslednje:*

1. *Vsaka dvojica podpredsednikov določi premico V_1 in s tem točko p, ki je v našem primeru iskana skrivnost.*
2. *Trojica višjih uradnikov s svojimi dodeljenimi točkami določi ravnino V_2 in z njenim presekom s premico V_d določijo točko p.*
3. *Par višjih uradnikov s svojima točkama iz ravnine V_2 in en podpredsednik s svojo točko iz premice V_1 tudi določijo ravnino V_2 in s tem skrivno točko p.*

■

Vsak del zasebne informacije je enako velik (v našem primeru imajo vsi člani točke za svoje zasebne dele informacije), vendar so nekateri deli informacije močnejši oziroma učinkovitejši od drugih.

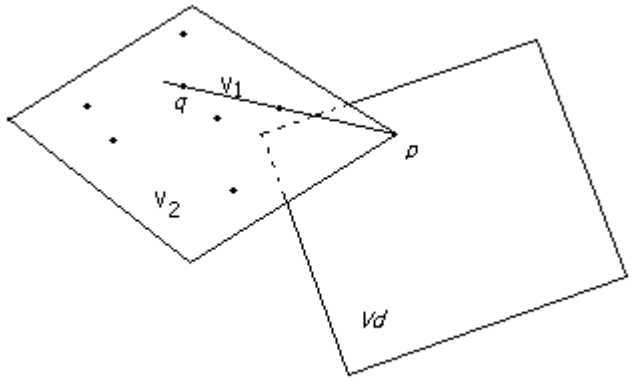
V podrazdelku 4.1.1. si bomo pri večnivojskih shemah ogledali kakšne so zahteve, da zagotovimo varnost in do kakšne mere lahko posplošimo večnivojske sheme za delitev skrivnosti, da s tem ne bomo izpostavili skrivnosti.
V podrazdelku 4.1.2. si bomo pogledali večnivojske sheme in njihove lastnosti.
V podrazdelku 4.1.3. in 4.1.4. pa si bomo ogledali konstrukcije večnivojskih shem z odvisnimi in neodvisnimi nivoji in razliko med tema dvema konstrukcijama.
Ker pa vse te sheme predstavimo le v treh dimenzijah, bomo v podrazdelku 4.1.5. predstaviti še splošno konstrukcijo večskupinskih shem.

4.1.1. VAROVANJE SKRIVNOSTI

Sedaj si bomo pogledali kako velik mora biti prostor v katerem skrivamo skrivnost, da zadošča varnostnim zahtevam shem za delitev skrivnosti. Opisali pa bomo tudi pogoje za javne dele informacije, tako da bo skrivnost ostala skrita ne glede na naše objavljene podatke in posplošene konstrukcije. Pri posploševanju želimo minimalizirati količino zasebnih delov informacije, ki jo mora vsak član skrivati.

V prejšnjem primeru smo skrili skrivnost v 1-razsežen prostor v 2-nivojskei shemi. Prvi nivo je bila 2-*n* delitvena shema, kjer je *n* število podpredsednikov. Sedaj želimo skriti skrivnost v 2-razsežen prostor. Poglejmo si konstrukcijo v kateri sedaj namesto podpredsednikov uvedemo prvi nivo in namesto višjih uradnikov uvedemo drugi nivo.

KONSTRUKCIJA 4.2: (2 nivoja, 2-razsežen prostor skrivnosti)



Slika 4.2: Shema za delitev skrivnosti v 4-razsežnem prostoru.

1. *Imamo n članov prvega nivoja in m članov drugega nivoja.*
2. *Izberemo ravnini V_2 in V_d v* 4*-razsežnem prostoru, tako da prostora ne ležita v skupnem* 3*-razsežnem prostoru. Torej imata skupno le eno točko. Naj bo to točka p. (V bistvu lahko uporabimo enak postopek kot smo ga uporabili za konstrukcijo ravnine V_2, kjer smo imeli podano premico V_d, tako da je bila točka preseka ravno točka p.)*
3. *Izberemo točko q v ravnini V_2, $q \neq p$. Premica V_1 skozi točki p in q določa n točk, ki jih dodelimo članom prvega nivoja.*
4. *Člani drugega nivoja dobijo vsak po eno točko v ravnini V_2, tako da velja:* • *Nobena dodeljena točka ne leži na premici V_1,* • *noben par dodeljenih točk točk ni kolinearen s točko p ali s kakšno točko, ki jo ima član iz prvega nivoja.*

Trditev 4.2: *Večnivojska shema po konstrukciji* 4.2 *je varna.*

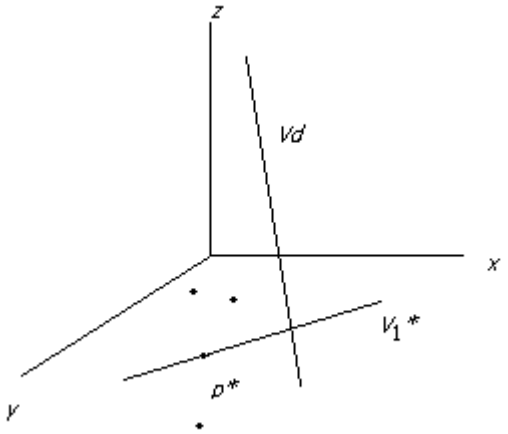
Dokaz: Za varnost zahtevamo, da nepooblaščena množica članov ali pa zunanji napadalec ne morejo odkriti skrivnosti s svojimi deli informacije. To pomeni, da lahko skrivno točko le ugibajo. V konstrukciji 4.2 smo točke smo razdelili tako, da lahko le pooblaščene množice odkrijejo skrivnost. Poglejmo si kaj se zgodi, če sodeluje nepravilo število članov. Dva člana drugega nivoja lahko skupaj določata le

premico, ki sicer seka domeno V_d, vendar ne v točki *p,* ker smo točke iz drugega nivoja tako izbrali. Tako lahko le ugibata skrivno točko v domeni V_d. Enako se zgodi, če sodelujeta en član prvega nivoja in le en član drugega nivoja. Zunanji napadalec pa pozna le javno domeno V_d in v njej ugiba skrivno točko *p*.

■

Če bi te sheme poskušali posplošiti ali poenaostaviti, bi s tem lahko ogrozili varnost. Sedaj se lotimo minimaliziranja količine informacij, ki bi jo moral vsak posamezen član hraniti, s pomočjo projekcije. Pri posplošitvi konstrukcije 4.1. v 3-razsežnem prostoru *S*, bomo skrili le eno komponento, dve pa objavili: (x_j, y_j, z_j). Z mastnim tiskom je označena skrita komponenta. Javni sta koordinati x_j in y_j, torej je znana projekcija zasebne točke p_j, ki jo ima *j*-ti član, na *xy* ravnino.
Če to naredimo, je skrivnost izpostavljena tudi zunanjim napadalcem in ne le nedovoljenemu združenju notranjih članov. Poglejmo si zakaj se je to zgodilo in kaj vse lahko ugotovimo le s poznavanjem javnih delov informacije.

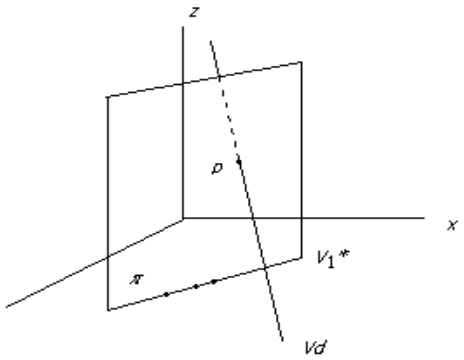
KONSTRUKCIJA 4.3: (2 nivoja, 1-razsežen prostor skrivnosti)



Slika 4.3: Projekcija skrivnosti in domene na *xy* ravnino.

1. *Sama konstrukcija je enaka konstrukciji* 4.1 *s to razliko, da je zasebna le koordinata z, koordinati x in y pa objavimo.*

Poglejmo si kje nastane problem in po kako lahko pride zunanji napadalec do skrivne točke p.



Slika 4.4: Ravnina, ki je vzporedna *z*-osi v kateri je skrivna točka *p*.

Trditev 4.3: *Naj bodo zasebni deli informacije razdeljeni po konstrukciji* 4.3. *Kdorkoli pozna javne dele informacije o skrivnosti (v našem primeru to pomeni njihovo projekcijo vzdolž z-osi na xy ravnino) pozna tudi projekcijo premice V_1 na premico V_1^* in s tem lahko odkrije skrivno točko p.*

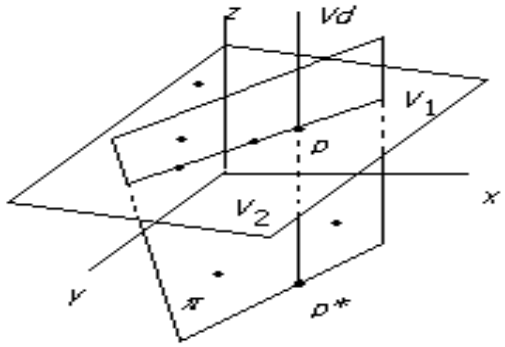
Dokaz:

- Napadalec potrebuje le javne dele dveh točk, da določi premico V_1^*.
- Vemo, da premica V_1 leži na ravnini π, ki je vzporedna z-osi in vsebuje premico V_1^*.
- V resnici je neznana premica V_1 ena iz šopa premic, ki gredo skozi točko p v kateri se premica V_d seka z ravnino π. Vendar tu ni najpomembneje, da določimo premico V_1, ampak njeno sekališče, točko p, s premico V_d.
- Iz tega sledi, da točko p odkrijemo le s poznavanjem javnih delov informacije o skrivnosti, saj premica V_d ne leži v ravnini π. Vemo pa, da je ravnina π vzporedna z z osjo in vsebuje projekcijo premice V_1, torej premico V_1^*. Tako je ravnina π natanko določena, kot tudi njen presek s premico V_d in to je skrivna točka p.

■

Vrnimo se sedaj nazaj na naš problem, kjer smo objavili preveč informacij in je tako skrivnost izpostavljena. Da to preprečimo, mora za premico V_d veljati še nekaj dodatnih pogojev. Problem izgine, če projekcija premice V_d na xy ravnino leži na premici V_1^*, to pomeni, da leži premica V_d na ravnini π.
Poglejmo si poseben primer, ko je premica V_d vzporedna z-osi, torej je njena projekcija enaka točki p^* na premici V_1^*.

KONSTRUKCIJA 4.4: (2 nivoja, 1-razsežen prostor skrivnosti)



Slika 4.5: V prostoru si izberemo še ravnino V_2, ki ni vzporedna ravnini π.

1.	*Točka p^* je projekcija točke p vzdolž z-osi. Torej velja* $\text{proj}_z(p) = p^*$.
2.	*V_1 in V_d sta torej različni premici v ravnini π, kjer se vsaj ena od njiju projicira na V_1^*.*
3.	*Vzemimo še ravnino V_2, ki vsebuje premico V_1 in zato tudi točko p. Ravnina V_2 ni enaka ravnini π in ne more biti vzporedna z-osi, zatorej je njena projekcija vzdolž z-osi cela xy ravnina.*
4.	*Premica V_d je vzporedna z-osi, tako da je točka p^* slika cele premice V_d pri projekciji. Sicer bi bila projekcija premice V_d cela premica V_1^* in projekcija točke p, točka p^*, neznana.*

Trditev 4.4: *Večnivojska shema po konstrukciji* 4.4 *je varna.*

Dokaz: Pri trditvi 4.3 smo dokazali, da lahko le z javnimi deli informacije odkrijemo skrivnost p. V dokazu te trditve smo videli, da zunanji napadalec to lahko naredi tako, da preko projekcij določi lokacijo skrivnosti p v domeni V_d. Ker pa je sedaj domena V_d skrita v smeri projekcije (t.j. leži cela v ravinini V_2), je shema varna.

■

Problem s katerim smo se srečali pri deljenju zasebnih in javnih delov informacije o skrivnosti, ki ogroža varnost shem za delitev skrivnosti, je pogost pri vseh večskupinskih shemah.

Poglejmo si splošen primer tega problema na 2-nivojski shemi prikazani v konstrukciji 4.2. Prostor S je bil 4-razsežen prostor in prostor v katerem je skrivnost je bil 2-razsežen. Tako bi bile zasebne informacije oblike (x_j, y_j, $\boldsymbol{z_j}$, $\boldsymbol{w_j}$), kjer sta javni informaciji koordinati x_j in y_j, ostali dve koordinati pa sta zasebni. Premica V_1 se projicira na premico V_1^* v xy ravnini. V tem primeru ima vlogo ravnine π, ki je bila definirana na premici V_1^* po konstrukciji 4.4, 3-razsežen prostor Z, vzporeden z in w osi in vsebuje premico V_1^*. Ker je prostor S 4-razsežen, lahko ravnina V_d seka prostor Z v premici ali pa je vsebovana v prostoru Z. Po rang formuli bi moral biti prostor S 6-razsežen, da bi lahko vseboval dva disjunktna podprostora in 5-razsežen, da bi ta dva podprostora imela le eno skupno točko.
Poglejmo si še enkrat, kaj mora veljati za podprostor V_d. Če velja $S \cap V_d = r$, kjer je r premica, potem shema ne more biti popolna, saj bi bil dvom o skrivnosti $O(q)$ namesto $O(q^2)$, če uporabimo javne dele zasebnih informacij skrivnosti. Torej mora veljati $V_d \subset S$. To ne pove:

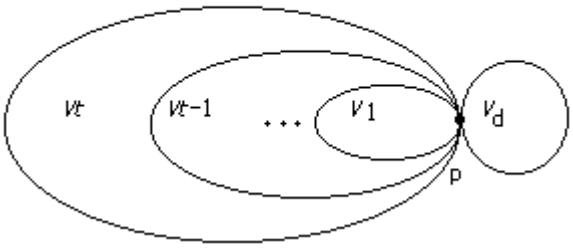
$\text{proj}_{z,w}(V_d) = \text{proj}_{z,w}(V_1)$
ampak le:
$\text{proj}_{z,w}(V_d) \subset \text{proj}_{z,w}(V_1)$.

To je analogno primeru, kjer je bila $\text{proj}_z(V_d)$ točka p^* ali pa cela premica V_1^*.
V prvem primeru smo vzeli premico V_d , ki je vzporedna z-osi, tako da je $\text{proj}_z(V_d) = p^*$, $p^* \in V_1^*$. Enako velja v drugem primeru, ko vzamemo premico V_d, ki vzporedno z-osi in w-osi, tako da je $\text{proj}_{z,w}(V_d) = p^*$, $p^* \in \text{proj}_{z,w}(V_1) = V_1^*$.
Če tako konstruiramo domeno V_d, potem bodo zasebni deli informacije čisto izgubljeni v projekciji in bo tak shema za delitev skrivnosti zato varna.

4.1.2. KONSTRUKCIJA VEČNIVOJSKE SHEME

Poglejmo splošno konstrukcijo t-nivojske sheme z d-razsežno skrivnostjo, kjer je potrebno število sodelujočih na j-tem nivoju k_j,. Velja $k_t > k_j > ... > k_1$ in vsak član na j-tem nivoju lahko sodeluje na vseh nižjih nivojih.

KONSTRUKCIJA 4.5: (t-nivojev, d-razsežen prostor skrivnosti)



Slika 4.6: Konstrukcija večnivojskih shem za delitev skrivnosti.

1. *Začnemo z n-razsežnim prostorom* S = PG(n,q), *kjer je* $n = d + k_t - 1$. *Podprostor* V_d *prostora* S *je d-razsežen in je vzporeden koordinatam* x_d , x_{d-1} ,..., x_1.
2. *S skrivno točko p in podprostorom* V_d *konstruiramo* $(k_t - 1)$*-razsežen podprostor* V_t *prostora S, ki se seka s podprostorom* V_d *samo v točki p.*
3. *Naslednji prostor, ki ga definiramo je* $(k_{t-1} - 1)$*-razsežen podprostor* V_{t-1} *podprostora* V_t, *ki vsebuje skrivno točko p.*
4. Postopek ponavljamo dokler na koncu ne dobimo verige podprostorov: $V_t \supset V_{t-1} \supset ... \supset V_1$ *zaporedoma dimenzij* $k_t - 1$, $k_{t-1} - 1$, ..., $k_1 - 1$. *Vsi ti prostori pa vsebujejo p.*

Trditev 4.5: *Večnivojska shema po konstrukciji* 4.5 *je varna in popolna.*

Dokaz: Zasebni deli informacije so izbrani, tako da ima podprostor V_j rang k_j in da ne ležijo v nobenem podprostoru višje stopnje (nivoju višje prioritete). Poglejmo to pri konstrukciji 4.1. Točki iz ravnine V_2, ki sta bili zasebna dela informacije drugega nivoja, nista smeli ležati na premici V_1. Noben par dodeljenih točk oziroma zasebnih delov informacije ni smel biti kolinearen s kako točko, ki je zasebni del informacije na premici V_1 in te točke niso smele biti enake točki p.
To pove, da točke v j-tem razredu morajo ležati v
$V_j \setminus \bigsqcup_{i=1}^{j-1} V_i$, tako da bo rang vsake množice k_j točk vzetih iz vseh zasebnih točk v $\bigsqcup_{i=1}^{j} V_i$
s točko p, ravno k_j .

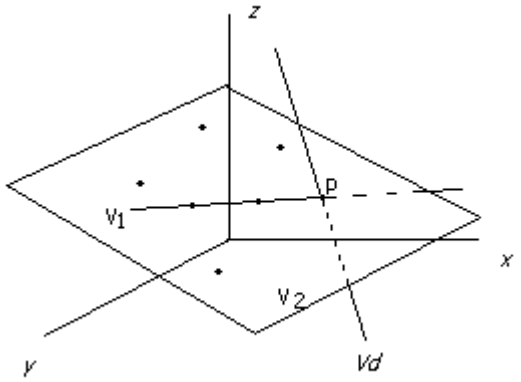
Pod temi pogoji bo gotovo lahko vsak član deloval na nižjem nivoju od svojega. Zasebne informacije bodo oblike: (x_n, ..., x_{d+1}, $\boldsymbol{x_d, ..., x_2, x_1}$). Shema bo popoln, ker je skrivnost izgubljena v projekciji po prvih d koordinatah. ■

4.1.3. NEODVISNI NIVOJI

Pri večnivojskih shemah lahko člani med seboj po nivojih sodelujejo ali pa tudi ne. Oglejmo si konstrukcijo, če člani med nivoji ne morejo sodelovati in varnost, ki jo zagotavlja ta shema.

Člani imajo spet različna pooblastila za sprožitev akcije. To smo opisali v primeru predsednika banke in dvema podpredsednikoma ali pa s tremi višjimi uradniki. Če ne bi bilo potrebe, da lahko podpredsednik deluje namesto višjih uradnikov, potem lahko trivialno sestavimo shemo za tako sodelovanje. To bi bila neodvisna 2-n in 3-m shema za ta dva razreda članov. Vsaka od teh dveh shem pa pripelje do skrite točke p.
Predpostavimo, da je število q dovolj veliko, da je verjetnost $1/(1+q)$ izbire točke p dovolj majhna, da zagotavlja varnost. Podprostor V_d pa je v tem primeru premica. Razsežnost dveh indikatorskih podprostorov mora biti $k - 1$. To pomeni 1-razsežna za prvi nivo, 2-razsežna za drugi nivo. To lahko vidimo v naslednji konstrukciji.

KONSTRUKCIJA 4.6: (2-nivoja, 1-razsežen prostor skrivnosti)



Slika 4.7: Konstrukcija večnivojske sheme za delitev skrivnosti z neodvisnimi nivoji.

1. *Premica V_1 ne leži na ravnini V_2 ampak premica V_1 in ravnina V_2 sekata premico V_d v točki p.*
2. *Zasebni deli informacije prvega nivoja je n točk s premice V_1, ki niso enake točki p.*
3. *Zasebni deli informacije za drugi nivo pa je m točk na ravnini V_2, različnih od točke p, ki jih izberemo, tako da nobena trojica ni kolinearna in noben par teh točk ni kolinearen s točko p.*

Trditev 4.6: *Nivoji so po konstrukciji* 4.6 *neodvisni, kar pomeni, da nobena točka s premice V_1 in dvojica točk iz ravnine V_2 ne morejo definirati ravnine, ki seka premico V_d v točki p.*

Dokaz: Če bi želeli nivoji sodelovati in skupaj določiti točko p, bi za to potrebovali par točk iz ravnine V_2, ki je sta kolinearni s točko p. To pa je v nasprotju z izbiro točk. Če pa bi vzeli dve točki iz ravnine V_2 in točko s premice V_1, bi skupaj definirali ravnino, ki ne seka V_d v točki p.

■

4.1.4. SODELOVANJE MED NIVOJI

Če želimo, da bi lahko član prvega nivoja sodeloval z dvema članoma drugega nivoja, da skupaj pridejo do točke p, potem mora premica V_1 ležati v ravnini V_2 in mora izbira točk za člane drugega nivoja zadostovati naslednjima pogojema:

- nobena točka iz drugega nivoja ne sme ležati na premici V_1,
- noben par točk iz drugega nivoja ni kolinearen s kako točko, ki je bila dodeljena članom prvega nivoja.

Drugi pogoj je zelo pomemben, ker bi sicer lahko trije člani, dva iz drugega nivoja in en iz prvega, s svojimi točkami določili le premico, ki ne seka premico V_d in tako ne bi mogli določiti točke p. Videli bomo, da ni težko zadostiti tem pogojem. Konstrukcija te 2-nivojske sheme, kjer lahko člani višjega nivoja sodelujejo s člani nižjih nivojev, je enaka konstrukciji 4.1.

4.2. VEČSKUPINSKA SHEMA

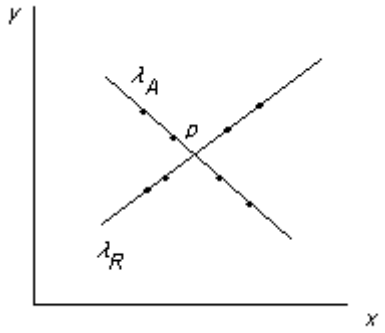
Druga vrsta pomembnih shem, ki jih bomo opisali so večskupinske sheme, ki so razširitev večnivojskih shem za delitev skrivnosti. Pri vseh shemah za delitev skrivnosti, ki smo jih do sedaj opisali so vsi člani, kljub temu da imajo različna pooblastila, v isti skupini. Poznamo veliko situacij, kjer je potrebnih za sodelovanje več skupin, katerih želje so zelo divergentne. Zato naredimo večskupinske sheme, da lahko z njimi upoštevamo želje vseh skupin.

Za primer vzemimo mirovni sporazum med državami. Za sporazum potrebujemo dva člana iz ameriške strani in dva člana iz ruske strani. Označevali jih bomo kot skupina A in skupina R. Po čem se ta večskupinska shema razlikuje od enostavne t-w delitvene sheme ali pa od večnivojske sheme? Razlikujejo se v tem, da ni važno koliko članov iz ene skupine se strinja z akcijo. Še vedno potrebujemo pooblaščeno množico članov tudi iz druge strani oziroma skupine. V našem primeru bomo razdelili zasebne dele informacije le na dva dela, vendar šele določena uporaba bo povedala koliko delov potrebujemo, da sestavimo učinkovito večskupinsko shemo za delitev skrivnosti.
V podrazdelku 4.2.1. si bomo ogledali različne konstrukcije in jih primerjali med seboj po varnosti in uporabi. Konstrukcije si bomo najprej ogledali na primeru, ko bomo imeli le dve skupini, nato pa bomo konstruirali splošno večskupinsko shemo.

4.2.1. KONSTRUKCIJE VEČSKUPINSKIH SHEM ZA DELITEV SKRIVNOSTI

Pomembno je, da se zavedamo zakaj večskupinske sheme sploh želimo sestaviti in kako uporabni bodo. Da pa so uporabne, morajo biti sheme najprej varni. Za to moramo poskrbeti v vsaki konstrukciji.
Za uporabo večskupinskih shem moramo opisati člane sheme in kdo od njih lahko sproži akcijo. Sheme so lahko tako enostavne, da potrebujejo le dva člana za odobritev akcije, kot v primeru odpiranja trezorja v banki ali pa primer soglasja dveh častnikov v vojski, da lahko izstrelita raketo. Vendar, kot bomo videli pri naslednjih primerih soglasja med državami, so lahko te sheme zelo komplicirane, saj imajo lahko člani različne možnosti sodelovanja in odobravanja akcij oziroma odkrivanja skrivnosti.
Pogledali si bomo nekatere možne konstrukcije večskupinskih shem in njihove lastnosti. Analizirali bomo, če vse te konstrukcije zagotavljajo varnost takih shem za delitev skrivnosti. Spet bomo začeli z najmanjšim možnim primerom, da prikažemo najpomembnejše stvari pri večnivojski shemi. Dve državi sodelujeta in se morata soglasno strinjati za sprožitev želene akcije.
Recimo, da imamo državi Rusija in Amerika, z oznakama R in A, in je vsaka skupina sestavljena iz štirih članov. V vsaki skupini se morata strinjati vsaj dva, da lahko odda država svoje stališče oziroma mnenje. V tem primeru soglasje štirih ameriških članov in enega ruskega ne bi smelo sprožiti akcije, ker manjka soglasje še najmanj enega ruskega člana. Ogledali si bomo tri različne konstrukcije te dvočlanske sheme za delitev skrivnosti.

KONSTRUKCIJA 4.7: (2 skupini, dva 1-razsežna indikatorska podprostora)



Slika 4.8: Indikatorski (državni) premici v večskupinske sheme za delitev skrivnosti.

1. Vsakemu članu v posamezni skupini (državi) damo po eno točko iz njihove indikatorske (državne) premice.
2. Točke *p* ne smemo dodeliti.

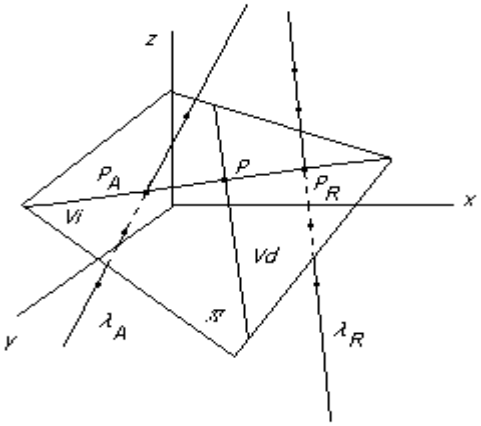
Trditev 4.7: *V shemi po konstrukciji* 4.7 *lahko za zasebne dele informacije delimo le q od* $q + 1$ *točk. Večskupinska shema po tej konstrukciji je varna, vendar ni popolna.*

Dokaz: Če bi en od članov dobil točko *p* kot njegovo zasebno informacijo, ne bi vedel, da je ravno to iskana skrivnost. To bi veljalo, tudi če ne bi sodelovala dva člana iz druge skupine. Vendar, če bi vzeli le tega člana iz ene skupine, ki je dobil za svoj podatek točko *p* in dva člana iz druge skupine, bi skupaj lahko ugotovili, da je tista točka, ki jo ima ta član res točka, ki jo iščemo, ker bi skupaj videli, da vse tri točke ležijo na isti premici. Torej za zasebne dele informacije lahko delimo le q od $q + 1$ točk. Ta shema je idealna vendar ni popolna, saj lahko vsaka skupina ugotovi, da točka *p* leži na premici, ki jo lahko določijo iz dveh točk. Shema ima lastnost, da nobeno nedovoljeno sodelovanje med skupinama ne more odkriti točke *p* in verjetnost, da bi en član uganili točko *p* je enaka verjetnosti neke točke v obsegu GF(q), $1/q$.

■

Oglejmo si naslednjo izboljšano konstrukcijo. 2-w shem, $w > 2$ lahko definira le premico kot indikatorski podprostor in zato je edino kar lahko skupine naredijo (drugi sicer tega ne morejo), da lahko definirajo svoje indikatorske premice λ_A in λ_R. Tako lahko uporabimo ti dve indikatorski premici, da najprej dobimo posamezni točki p_A *in* p_R iz vsake skupine, ki določata premico na kateri leži točka *p.* Nato pa s presekom z domeno dobimo točko *p*. Lahko pa uporabimo indikatorski premici λ_A in λ_R, da napneta indikatorsko ravnino V_i, ki s presekom z domeno V_d določa točko *p*.
Prvi način je nekako lažji in ga je lažje posplošiti. Poskrbeti moramo, da državni premici, definirani s točkama članov posamezne države, določata indikatorski podprostor V_i, ki z domeno V_d kaže na točko *p*. To moramo narediti tako, da so vsi pogoji sodelovanja in varnosti izpolnjeni. En način za to bomo prikazali s konstrukcijo 4.8.

KONSTRUKCIJA 4.8: (2 skupini, trije 1-razseženi indikatorski podprostori)



Slika 4.9: Določanje skrivne točke *p* s pomočjo državnih premic.

1. *Naj bo prostor S* vektorski *prostor nad obsegom* GF(q^3) *in naj bo* π *ravnina, ki leži v prostoru S. V ravnini* π *izberimo premici* V_i *in* V_d *. Izberimo še indikatorski premici* λ_A in λ_R*, ki ne ležita na ravnini* π*.*
2. *Za zasebne dele informacije točke dodelimo članom v posameznih skupinah zaporedoma m in n točk na indikatorskih premicah* λ_A in λ_R*, od katerih nobena ne leži na ravnini* π*. Te točke dodelimo članom v posameznih skupinah.*
3. *Vsak par točk članov iste skupine določa indikatorsko premico svoje skupine in s tem točko* p_A *oziroma* p_R*, kateri premica seka ravnino* π*.*
4. *Točki* p_A *in* p_R *določata indikatorsko premico* V_i *in s tem sekališče p z domeno* V_d*.*

Poglejmo si pogoje za zasebne dele informacije.

Trditev 4.8: *Večskupinska shema po konstrukciji* 4.8 *je popolna in za zasebne dele informacije imamo na voljo le q od q* + 1 *točk.*

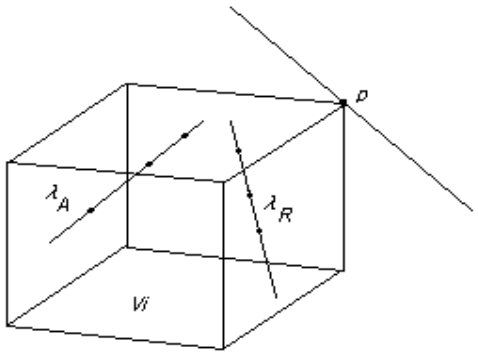
Dokaz: Član z eno izmed točko točk p_A in p_R in poznavanjem ravnine π lahko sam, brez sodelovanja z drugimi člani svoje skupine sodeloval z drugo skupino pri odkrivanju skrivnosti *p*. Ta shema je popoln, ker nobeno nedovoljeno sodelovanje ne pove nič več o točki *p*, vendar pa ni idealna. Shema predstavlja zahtevano sodelovanje in varnost, saj je verjetnost točke *p* enaka ugibanju neke točke v obsegu GF(*q*), to pa je 1/*q*.

■

Poglejmo si sedaj konstrukcijo za sheme kjer je en indikatorski podprostor 3-razsežen.Če si za indikatorski premici λ_A in λ_R izberemo mimobežnici v 3-razsežnem podprostoru V_i in točka *p* ne leži na nobeni od njiju, potem imamo geometrijsko osnovo za konstrukcijo sheme za delitev skrivnosti z želenimi lastnostmi.

KONSTRUKCIJA 4.9:

(en 3-razsežen in dva 1-razsežna indikatorska podprostora)



Slika 4.10: Konstrukcija dvoskupinske sheme v 4-razsežnem prostoru *S*.

1. *Naj bo S 4-razsežen prostor.*
2. *Naj bosta 3-razsežen podprostor V_i in 1-razsežen podprostor V_d prostora S, izbrana tako, da napenjata prostor S in njun presek naj bo ravno točka p.*
3. *Za zasebne dele informacije vzamemo m in n točk na indikatorskih premicah λ_A in λ_R, ki ležita v podprostoru V_i.*
4. *Po rang formuli dve mimobežni premici napenjata 3-razsežen podprostor V_i. Tako lahko vsak par članov iz prve skupine skupaj s parom članov iz druge skupine rekonstruira podprostor V_i. S tem je točka p določena.*

Problem je, kako izbrati zasebne točke, da ne bi nobena podmnožica članov, ki ne vsebuje vsaj enega para iz posamezne skupine, odkrila podprostor V_i. Potrebovali bomo naslednjo trditev:

Trditev 4.9: *Za dve mimobežnici λ_1 in λ_2 v 3-razsežnem prostoru in točko p, ki ne leži na nobeni od teh dveh premic, obstaja natanko ena premica, ki vsebuje točko p in seka premici λ_1 in λ_2.*

Dokaz: Premica λ_1 in točka p določata ravnino π_1. Premica λ_2 in točka p pa določata ravnino π_2. Ravnini π_1 in π_2 se sekata ravno v premici, ki vsebuje točko p in seka obe premici λ_1 in λ_2. Poglejmo si, kaj se zgodi, če obstajata dve premici, ki vsebujeta točko p in sekata premici λ_1 in λ_2. Skupaj bi določali ravnino. Ker bi ta ravnina vsebovala dve točki s premice λ_1 in dve točki s premice λ_2, bi to pomenilo, da premici λ_1 in λ_2 ležita v isti ravnini. To pa ne more veljati, ker sta mimobežnici. Trditev je s tem dokazana. ■

Trditev 4.10: *Pri večskupinski shemi po konstrukciji* 4.9 *za zasebne dele informacije ne smemo uporabiti točki p_1 in p_2. Uporabimo lahko le q od q + 1 točk iz vsake indikatorske premice.*

Dokaz:

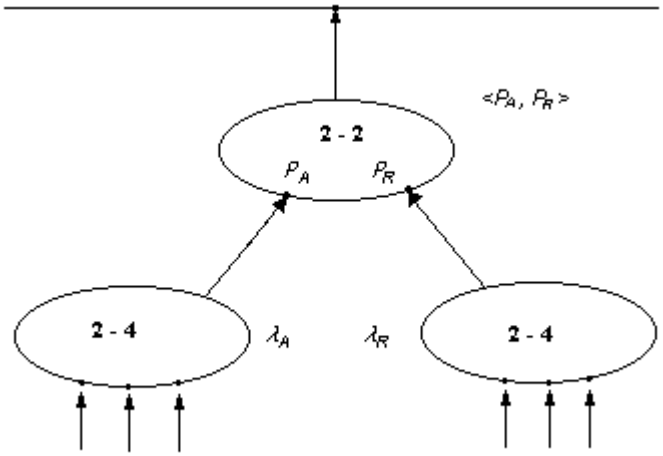
- Če bi obe točki uporabili kot zasebna dela informacije, bi lahko le dva člana, ki imata ti točki (vsak iz ene skupine), sama določila skrito točko p. To velja, ker točki p_1 *in* p_2 določata premico λ^*, ki seka premico V_d v točki p.

•Pokažimo še, da ne smemo nobene izmed točk p_1 *in* p_2 dodeliti kot zasebni del informacije. Predpostavimo, da leži točka p_1 na premici λ_A in je podana kot zasebni del informacije nekemu članu skupine *A*. Poglejmo, kaj lahko ugotovi ta član v sodelovanju še z dvema članoma iz skupine *R*. Člana skupine *R* lahko določita premico λ_R, ki je mimobežna premici V_d. Premici λ_R in V_d napenjata 3-razsežen podprostor, ki vsebuje premico λ^*, saj vsebuje dve njeni točki p_2 in *p*. Po trditvi 4.9 obstaja premica, ki gre skozi točko p_1 v 3-razsežnem podprostoru, ki ga napenjata premici λ_R in V_d. Ta premica seka premico λ_R in v točki p seka premico V_d. Torej nedovoljeno sodelovanje enega člana skupine *A*, ki pozna točko p_1 in dvema članoma druge skupine, lahko odkrije točko *p*.

Torej lahko res uporabimo le *q* od *q* + 1 točk iz vsake indikatorske premice posamezne skupine.

■

Poglejmo si najpomembnejšo stvar pri konstrukcijah 4.7-4.9. V prostoru *S* imamo 2-2 soglasno shemo. Kar pomeni, da potrebujemo obe točki p_A in p_R, da lahko določimo točko *p*. Vsaka od shem v posamezni skupini je 2-4 delitvena shema, ki določa točki p_A in p_R. Drugače povedano smo konstruirali mrežo in jo organizirali kot drevo shem za delitev skrivnosti (slika 4.11):



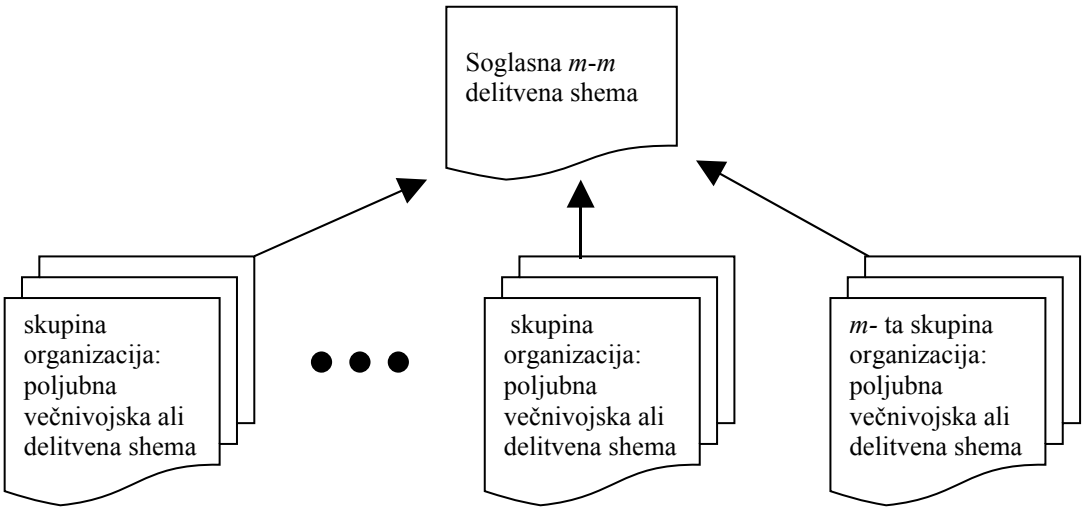
Slika 4.11: Drevo shem za delitev skrivnosti.

Oznaka $<p_A, p_R>$ označuje podprostor prostora *S*, v tem primeru premico, ki jo napenjajo točke v oklepajih. Ker so vsi podatki, ki jih imamo v naših shemah, točke v prostoru *S* ali v kakšnem podprostoru prostora *S*, lahko večino shem konstruiramo na tak način. Najverjetneje obstajajo monotone sheme za delitev skrivnosti, ki jih ni mogoče realizirati na ta način, čeprav ne poznamo nobenega primera. Vse primere, ki smo jih spoznali, znamo konstruirati z uporabo večskupinske sheme, ki ga lahko implementiramo kot drevo enostavnih shem za delitev skrivnosti.

Do sedaj smo si ogledali konstrukcijo 2-skupinske sheme. Oglejmo si bolj splošno konstrukcijo m-skupinske sheme.

Kot lahko vidimo na sliki 4.11, je lahko vsaka skupina znotraj organizirana kot poljubna *t-w* delitvena shema ali pa večnivojska shema. Skupine med seboj organiziramo in povežemo v soglasno *m-m* delitveno shemo, ki mora zadoščati vsem varnostnim zahtevam.

KONSTRUKCIJA 4.10: (m skupin)



Slika 4.12: Slošna konstrukcija m-skupinske sheme.

1. *Vzamemo m različnih skupin, ki so znotraj poljubno organizirane kot t-w delitvene ali večnivojske sheme (konstanti t in w sta odvisni od posamezne skupine). Taka organizacija je potrebna, saj mora vsaka skupina najprej sestaviti zasebni del informacije med svojimi člani in šele potem ga posreduje v skupno shemo.*
2. *Vsaka shema znotraj skupine mora biti varna in popolna.*
3. *Skupine podajo svoje zasebne dele informacije v m-m delitveno shemo, da lahko odkrijejo skrivnost p.*

Ker so vse sheme znotraj konstruirane tako, da so varne in popolne je naslednja trditev očitna.

Trditev 4.11: *Shema po konstrukciji* 4.10 *je varna in popolna.*

■

V tej splošni konstrukciji večskupinske sheme lahko vidimo, da je taka shema res razširitev večnivojske sheme. Konstrukcija poteka tako, da sestavimo več večnivojskih shem skupaj.

4.3. POSPLOŠITVE VEČNIVOJSKIH IN VEČSKUPINSKIH SHEM TER GEOMETRIJA

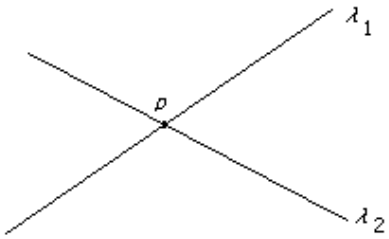
Do sedaj smo si pogledali kakšne sheme za delitev skrivnosti najraje uporabljamo. Vsako sodelovanje med člani mora vsebovati množico točk, ki napenja podprostor V_i. Podprostor V_i seka podprostor V_d v točki p. Sedaj bomo pokazali, kako je nekatere obstoječe sheme za delitev skrivnosti mogoče sestaviti oziroma kombinirati. Želimo tudi optimizirati število članov, saj s tem pripomoremo k varnosti. Pogledali si bomo kakšna je geometrična vloga domene in indikatorskih podprostorov.

V podrazdelku 4.3.1. si bomo ogledali posledice zamenjave indikatorskega podprostora in domene. S tem bomo lahko minimalizirali število članov v shemi. V podrazdelku 4.3.2. bomo pogledali kombinacijo večnivojske in večskupinske sheme. V podrazdelku 4.3.3. pa si bomo ogledali geometrične formule, ki nam povedo število podprostorov v poljubnem prostoru.

4.3.1. IZBIRA INDIKATORJEV IN DOMEN TER ŠTEVILO ČLANOV

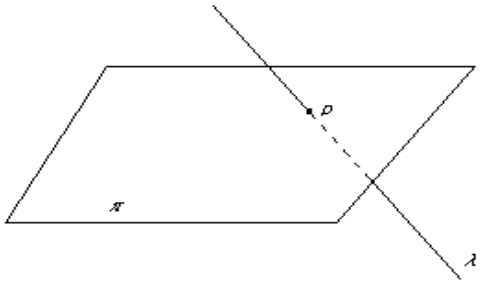
Najprej moramo eksplicitno izpostaviti pomemben rezultat, ki je v prejšnjih poglavjih ostal impliciten. Pogledali si bomo sliki konstrukcij dveh shem in kakšne sheme lahko dobimo, če sami izbiramo kateri podprostor bo domena V_d in kateri indikator V_i. Poglejmo si kako lahko domeno in indikator izbiramo na naslednjih primerih (slika 4.13 in 4.14).

1. Če je prostor S 2-razsežen in sta obe spremenljivki λ_1 in λ_2 premici v prostoru S, potem je vseeno katero vzamemo za podprostor V_i in katero za podprostor V_d. Taka prostora sta sebi dualna. Primer take sheme vidimo na sliki 4.13.



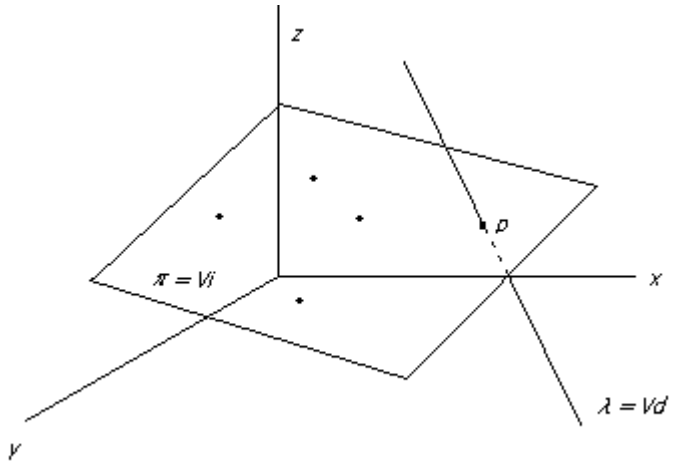
Slika 4.13: 2-4 delitvena shema

2. Če imamo dva podprostora U in V projektivnega prostora S, za katere velja $\dim(\mathrm{Lin}(U \cup V)) = \dim(S)$, $\dim(\mathrm{Lin}(U \cap V)) = 0$ in $\dim(U) \neq \dim(V)$. Opazimo, da obstajajo družine dualnih shem za delitev skrivnosti, odvisne od tega, katerega od podprostorov U ali V izberemo za indikatorski podprostor V_i. Na sliki 4.14 je prostor S 3-razsežen in podprostora sta ravnina π in premica λ. V tem primeru je zelo pomembno, kaj vzamemo za podprostor V_i. Ali je to ravnina π ali premica λ. Če vzamemo, da je λ indikatorski podprostor V_i, potem je edina možna shema, ki jo lahko konstruiramo, 2-w delitvena shema, $w \geq 2$. Če pa je $V_i = \pi$, potem imamo vsaj štiri različne sheme za delitev skrivnosti.



Slika 4.14: Primer različnih shem, ki so odvisni od izbire podprostorov.

Poglejmo si sedaj, kako smo to izbiri domene in indikatorja uporabili pri konstrukcijah shem za delitev skrivnosti, tako da smo imeli dovolj zasebnih delov informacije. Če so zasebne točke v ravnini π različne od točke p in za njih velja, da nobena trojica ni kolinearna in noben par ne leži na premici, ki vsebuje točko p, potem dobimo popolno 3-w delitveno shemo (slika 4.15).



Slika 4.15: 3-w popolna delitvena shema.

Razlogi za pogoje so očitni, saj smo jih že večkrat srečali (prvič v konstrukciji 4.1). Če bi kakšen par točk ležal na isti premici, ki vsebuje točko p, bi lahko le s tem parom točk določili točko p, saj premica, ki jo določata ti dve točki, seka premico V_d ravno v točki p. Če pa bi bile tri točke v ravnini π kolinearne, potem bi skupaj določale premico, ki je mimobežna premici V_d in tako ne bi mogli določiti točke p. Zaradi število točk na premici (v PG(n, q) je to število točk enako $q + 1$), moramo izbrati dovolj veliko število q, ki je red obsega GF(q). S tem je verjetnost, da bi uganili točko p v podprostoru V_d, ki je enaka $1/(q+1)$, dovolj majhna, da zagotavlja zahtevano varnost sheme.

Sedaj postavimo še eno zahtevo, ki je ponavadi trivialno izpolnjena, ko zadostimo varnostnim pogojem. Ta zahteva je število članov, ki nastopa v shemi. Maksimalno število članov, ki lahko sodeluje v shemi, bomo označili z L. V našem primeru lahko uporabimo le toliko točk, ki jih lahko izberemo v ravnini, v PG(3, q), da nobena trojica točk ne bo kolinearna. To število je enako $q + 1$, če je karakteristika GF(q) liha (to pomeni, da je q potenca lihega praštevila), in $q + 2$, če je $q = 2^{\alpha}$ za neko celo število α [4]. To smo dokazali v 2. poglavju pri stožernicah v Segrejevi teoriji.

Če je število q liho, množica $q + 1$ točk določa stožernico Ω v ravnini. Če pa je število q sodo, množica $q + 1$ točk poleg stožernice Ω določa tudi njeno jedro η (t.j. točka skupnega preseka $q + 1$ tangent na stožernici [10]).

Ukvarjali se bomo le z obsegi lihe karakteristike. V tem primeru lahko določimo natančno zgornjo mejo za maksimalno število članov L, ki lahko sodeluje v 3-w delitveni shemi.

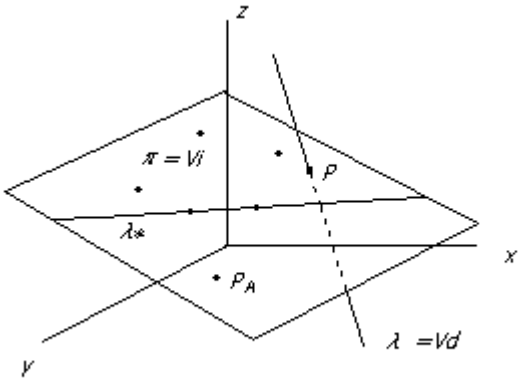
Če je točka p, notranja točka stožernice Ω (to pomeni, da točka p ne leži na nobeni izmed tangent stožernice Ω), potem je število članov $L = (q + 1)/2$. To je očitno, saj mora vsaka premica, ki vsebuje točko p in še eno točko stožernice Ω, vsebovati še neko drugo točko stožernice Ω. Sicer bi bila vsaka taka premica tangenta stožernice

Ω. To pa je v nasprotju s predpostavko, da točka p leži v notranjosti stožernice Ω. Samo eno od teh dveh točk lahko uporabimo za zasebni del informacije.
Če pa je p zunanja točka stožernice Ω, potem jo vsebujeta dve tangenti stožernice Ω. Ostalih $q - 1$ točk lahko z istim razlogom kot prej uredimo po parih in po eno točko od vsakega para uporabimo za zasebni del informacije. Pri štetju točk moramo upoštevati še dve točki, kjer se tangenti skozi točko p dotikata stožernice Ω.. Torej je število članov $L = (q + 3)/2$.
V uporabi shem za delitev skrivnosti želimo visoko varnost. To pomeni veliko vrednost števila q in relativno malo članov. Zato je malo verjetno, da bo število članov vplivalo na red obsega nad katerim delamo.

4.3.2. KOMBINACIJA VEČSKUPINSKE IN VEČNIVOJSKE SHEME

Nadaljujmo z večskupinskimi shemami, ki jih lahko realiziramo s konstrukcijo na sliki 4.16. Imamo ravnino $\pi = V_i$, ki jo napenja premica λ^* in neka točka p', ki ne leži na premici λ^*. Če uporabimo to dejstvo lahko realiziramo dvoskupinsko shemo.
Spet vzemimo za primer soglasje med državami. Predvidevajmo, da želi Amerika narediti shemo za delitev skrivnosti s svojimi 15 NATO zavezniki. Nadzorovala bi uporabo nuklearnega orožja v NATO, tako da bi morali vsaj dve državi iz Evrope sodelovati, da bi lahko sprožili orožje, medtem ko bi imela Amerika pravico veto nad nadzorovanjem vseh ostalih držav. To bi pomenilo, da četudi bi se vseh 15 evropskih držav strinjalo z uporabo orožja, tega ne bi mogle storiti brez dovoljenja Amerike. Pomeni pa tudi, da Amerika sama ali pa Amerika s še eno evropsko državo iz NATA ne bi mogla sama sprožiti orožja. Dvočlanska shema prikazana v konstrukciji 4.11 realizira tak tip delitve moči.

KONSTRUKCIJA 4.11: (16 skupin, 1-razsežen prostor skrivnosti)



Slika 4.16: Konstrukcija večskupinske sheme z enim članom, ki ima večjo moč.

1. *Vzemimo prostor S in v njem izberimo ravnino π in premico V_d, ki ne leži v ravnini π.*
2. *Naj bo λ^* premica v ravnini π, ki ne vsebuje točke p, kar pomeni, da je premica λ^* mimobežna domeni V_d v prostoru S. Za zasebne dele informacije, ki jih dodelimo* 15 *skupinam (vsem razen skupine A), izberemo točke s premice λ^*.*
3. *p_A je točka v ravnini π, $p_A \neq p$. To točko dodelimo skupini A. p_A ne leži na nobeni taki premici, ki vsebuje točko p in eno izmed točk iz premice λ^*, ki so bile dodeljene ostalim* 15 *skupinam.*
4. *Dve izmed* 15 *skupin lahko določita premico λ^*, ki je mimobežna premici V_d.*
5. *Točka p_A in premica λ^* določata ravnino π in s tem točko p.*

Trditev 4.12: Shema *po konstrukciji* 4.11 *je popolna*. *Premica, ki vsebuje točki p in p_A, seka premico λ^* v točki, ki je ne smemo uporabiti za zasebni del informacije. V shemi lahko sodeluje q članov.*

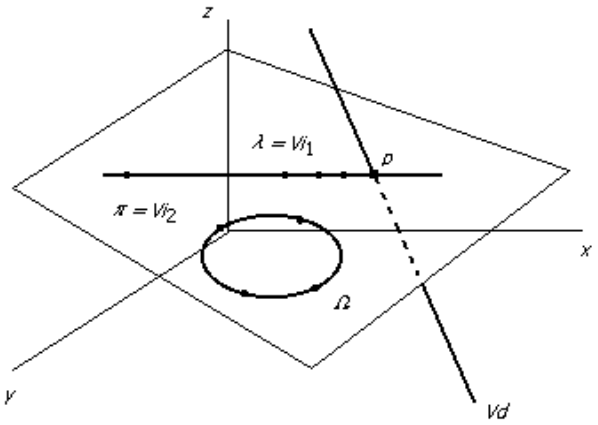
Dokaz: Če bi imela ena izmed 15 skupin (evropske članice NATO) točko preseka premice, ki vsebuje točki p in p_A, in premice λ^* za zasebni del informacije, bi lahko skupina A (Amerika) le s tem članom določila skrivnost p.
Ker velja $p \neq p_A$ in imamo w premic določenih s točko p_A in w zasebnih točk na premici λ^*, ki so mimobežne premici V_d, imajo vse nepooblaščene množice enako možnost, da odkrijejo točko p kot zunanji napadalci. Torej je ta shema popolna. ■

Zdaj nas zanima, kako lahko vpletemo večnivojske sheme v večskupinske. Govorili smo že o 2-nivojski shemi prikazani v konstrukciji 4.1, kjer smo imeli dva nivoja članov. Dovoljeno sodelovanje je bilo:

- med dvema članoma prvega nivoja,
- med tremi člani drugega nivoja,
- med enim članom prvega nivoja in dvema članoma drugega nivoja.

Tudi ta shema je ena izmed tistih, ki jih lahko realiziramo po konstrukciji na sliki 4.16. Ne bomo ponavljali analize varnosti za to shemo, ampak bomo analizirali le zgornja mejo števila članov, ki jo ta shema lahko podpira.

Prvi pogoj za izbiro točk za zasebne dele informacije drugega nivoja je, da nobena trojica točk ne sme biti kolinearna. Ugotovili smo, da pri lihem številu q lahko na neki stožernici Ω uporabimo največ $q + 1$ točk od vsega $q^2 + q + 1$ točk v ravnini π.



Slika 4.17: Kombinacija večskupinskih in večnivojskih shem.

Ker mora premica $\lambda = V_{i1}$ vsebovati točko p in točka p ne sme biti zasebni del informacije, je lahko le q od $q + 1$ točk s premice λ dodeljenih kot zasebni deli informacije. Točke drugega nivoja w_3 na stožernici Ω določajo $\binom{w_3}{2} = O((w_3)^2)$ različnih premic (sekant stožernice Ω), kjer vsaka od njih seka premico λ v točki, ki je ne moremo porabiti kot zasebni del informacije za člane prvega nivoja. Sicer bi ti trije člani lahko določili le mimobežnico premici V_d in tako bi bile lahko vse točke na premici V_d kandidati za točko p. To pa je v nasprotju s sodelovanjem, ki ga zahtevamo. Vidimo, da so za $w_3 > \sqrt{q}$ vse točke na premici λ nedovoljene za uporabo in s tem je prvi nivo prazen. V resnici velja, da bo pri poljubni izbiri premice λ in števila w_3, če je število w_3 malo večje od $\sqrt{q}$, to gotovo res. Če število w_3 pravilno izberemo, potem je mogoče uporabiti q članov tudi, če je število $w_3 = (q + 1)/2$. Torej poglejmo, kako izbiramo število w_3.

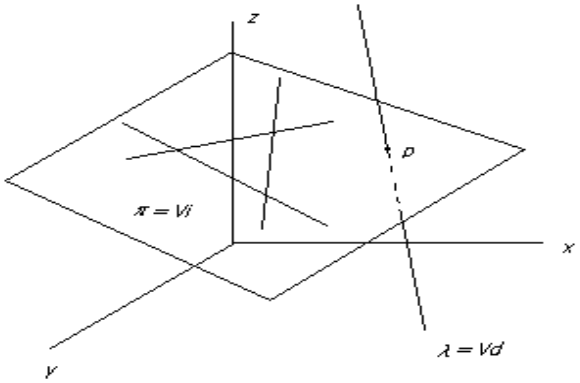
Vzemimo stožernico Ω in še neko zunanjo premico λ stožernice Ω (to je premica, ki ne vsebuje nobene točke stožernice Ω) v projektivni ravnini $\pi = PG(2, q)$, kjer je q liho število. Potem lahko premica λ deli $q + 1$ točk na stožernici Ω na množice moči k za vsak k, ki deli $q + 1$, tako da $\binom{k}{2}$ sekant stožernice Ω seka premico λ le v k točkah.

Primer 4.1:

Če je $q = 23$, potem zunanja premica λ deli 24 točk na stožernici Ω zaporedoma na 6 množic moči 4, 4 množice moči 6, 3 množice moči 8, dve množici moči 12, tako da za vsako od teh množic zaporedoma 6, 15, 28, 66 sekant seka premico λ zaporedoma v 4, 6, 8 ali 12 točkah. Če so vse točke w_3 za člane drugega nivoja izbrane na tak način, potem lahko ostalih 20, 18, 16, 12 točk na premici λ dodelimo kot zasebne ali javne dele informacije članom prvega nivoja. To pomeni, da lahko q od $q^2 + q + 1$ točk v ravnini izberemo za zasebne dele informacije, če izberemo število w_3 tako, da deli $q + 1$.

▲

Število q nam ponavadi zagotovi veliko večje število članov, ki lahko sodelujejo v shemi, kot ga sploh potrebujemo. Omeniti je potrebno, da obstaja drugačna izbira zasebnih delov informacije za 2-w delitveno shemo, ki je zasnovana na sliki 4.18. Vsak par premic v ravnini π napenja to ravnino. Tako lahko za zasebne dele informacije uporabimo w različnih premic, ki ne ležijo na točki p.



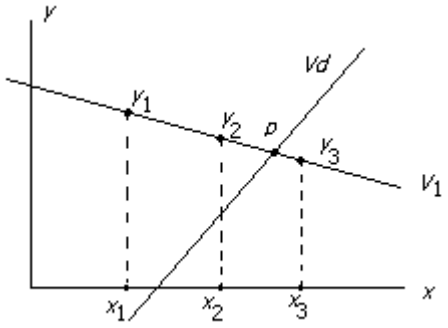
Slika 4.18: 2-w delitvena shema s premicami.

Ker je ravnina 2-razsežna, je shema na sliki 4.18 ekvivalentna 2-w shemi, ki temelji na točkah na premici (v ravnini π), kot smo videli za shemi v konstrukciji 4.1. Edina prednost je, da je lahko število članov L v tem primeru večje. Ena izmed točk, ki leži na premici in je določena z dvema zasebnima točkama iz sheme v konstrukciji 4.1, mora biti skrita točka p. V tem primeru je število članov $L = q$. Število premic v projektivni ravnini pa je $q^2 + q + 1$, medtem ko je število premic, ki vsebuje točko p enako $q + 1$. Zatorej obstaja q^2 premic, ki ne vsebuje točke p. V tem primeru pa je število članov $L = q^2$.

Ta obravnava nam je pokazala, koliko različnih shem za delitev skrivnosti lahko implementiramo iz majhne geometrične konstrukcije dveh podprostorov, ki napenjata prostor S in imata le eno skupno točko.

4.3.3. ANALIZA VARNOSTI I IN GEOMETRIČNE FORMULE

Posvetili se bomo še matematičnim in geometričnim formulam, ki smo jih uporabljali v naših konstrukcijah. Pogledali bomo kako s pomočjo matematičnih in geometričnih formul izračunamo varnost v shemah za delitev skrivnosti.



Slika 4.19: Enostavna 2-*w* delitvena shema.

Pri enostavni 2-*w* shemi na sliki 4.19 moramo preučiti dve točki za varnost sheme. Prva je, da mora biti shema varna pred vsemi nedovoljeni sodelovanji z zunanjim napadalcem in notranjim članom ali le med notranjimi člani. Druga pa je povezana z dejstvom, da ni treba vseh informacij vzeti za skrivne informacije. To dvoje moramo upoštevati tudi pri drugih shemah. V shemi na sliki 4.19 je javno znano, da skrivna točka p leži na premici V_d. Torej je verjetnost zunanjega napadalca, da odkrije točko p, enaka kot v prostoru $S = \mathrm{AG}(2, q)$, to je $P_d = 1/|V_d| = 1/q$.

Za analizo varnosti si zamislimo situacijo, da si zunanji napadalec poveča možnosti z uporabo javnih informacij (abcise x_j zasebnih delov informacije). Ve samo, da je indikator V_i premica, ki ni vzporedna y-osi (razlog za to smo povedali v drugem poglavju), vendar obstaja q takih premic čez vsako točko na premici V_d in čez vsako točko na vertikali (x_j, y) za vsak x_j. Ker so vse enako možne za premico V_i, je verjetnost, da bi uganil premico V_i, enaka $1/q^2$. Zato bi bilo bolje, če bi ugibal kar točko p. Pomembno je, da je število možnosti (za premico V_i) enako za vsako izbiro točke p.

Poglejmo si natančneje geometrijo v ozadju. Do sedaj smo nenatančno in zato nepravilno uporabili pojem podprostor in tako bomo tudi nadaljevali, da bi s tem prikazali geometrični objekt v afinem prostoru, ki je ali podprostor ali pa izomorfen podprostoru. Tem podprostorom pravilneje rečemo afini podprostori in le taki afini podprostori, ki vsebujejo izhodišče so pravi podprostori. V AG(2, q) je le $q + 1$ premic, ki vsebuje (0, 0) in so pravi podprostori prostora AG(2, q). Ostale premice so 1-afini prostori (1-razsežni afini prostori izomorfni AG(1, q)). Natančni bomo le pri teh naslednjih rezultatih.

Rezultat, ki ga potrebujemo je formula, ki nam pove število k-razsežnih podprostorov ali k-afinih prostorov v PG(n, q) ali AG(n, q), ki vsebujejo dan t-razsežen podprostor oziroma t-afin prostor. Za to definiramo funkcijo $\varphi(n, k; q)$:

$$\varphi(n,k;q) = \begin{cases} 1, k = 0 \\ \prod_{i=0}^{k-1} \left[\dfrac{q^n - q^i}{q^k - q^i} \right], 1 \le k \le n \end{cases} \quad (1)$$

Število različnih k-afinih podprostorov v AG(n, q) je

$q^{n-k} \varphi(n, k; q)$ (2)

in število različnih k-afinih podprostorov, ki vsebuje dan t-afin prostor je

$\varphi(n - t, k - t; \mathrm{q})$. (3)

Enačba (2) pravi, da je celotno število premic, 1-afinih prostorov v AG(2, q) enako $q^{2-1}\varphi(2, 1; q) = q^2 + q$ in število premic, ki leži na točki je po enačbi (3) enako $\varphi(2, 1; q) = q + 1$. Te rezultate smo že uporabljali.
Podobno izračunamo število k-razsežnih podprostorov v PG(n, q) po formuli

$$\varphi(n + 1, k + 1; q) \tag{4}$$

in število k-razsežnih podprostorov, ki vsebuje dan t-dimenzionalni podprostor, po formuli

$$\varphi(n - t, k - t; q). \tag{5}$$

Enačba (4) pravi, da je število 1-razsežnih podprostorov v PG(2, q) enako $\varphi(3, 2; q) = q^2 + q + 1$ in število 1-razsežnih podprostorov, ki leži na dani točki, pa je enako $\varphi(2, 1; q) = q + 1$.
Da bi videli, kako lahko te formule uporabimo pri izračunavanju varnosti shem za delitev skrivnosti, naj bo $\dim(V_i) = m$, $\dim(V_d) = s$ in kot vedno naj velja:

- $\dim(\mathrm{Lin}(V_i \cup V_d)) = \dim(S) = n$
- $\dim(\mathrm{Lin}(V_i \cap V_d)) = 0$.

Predpostavimo, da pri nedovoljenem sodelovanju k' članov ti združijo svoje podatke, da bi dobili skrivnost p. Njihove točke napenjajo podprostor T, za katerega je $\dim(T) = t \leq k' - 1$. $T \cap V_d = \varnothing$, saj velja $T \subset V_i$ in $V_i \cap V_d = p$. Sicer bi lahko z nedovoljenim sodelovanjem odkrili točko p. Zato ima podprostor, ki ga napenja k' točk in neka točka p' v V_d, dimenzijo $t + 1$ in velja $t + 1 \leq k'$.
Ne glede ali smo v prostoru AG(n, q) ali PG(n, q), enačbi (3) in (5) povesta, da je število $(t + 1)$-razsežnih podprostorov oziroma $(t + 1)$-afinih podprostorov, ki ležijo na $k' + 1$ točkah, enako $\varphi(n - t - 1, k - t - 1; q)$, za vsako izbiro točke p' v domeni V_d. Torej je vsaka točka enako verjeten kandidat za točko p, če združimo zasebne informacije pri nedovoljenem sodelovanju. Tako pri nedovoljenem sodelovanju ni mogoče povečati možnosti pri ugibanju podprostora V_i med vsemi m-razsežnimi podprostori, ki vsebujejo k' znanih točk in neko točko p' v domeni V_d, saj je teh veliko za vsako izbiro točke p'. Zato je taka shema popolna.
Pomembno pri minimaliziranju delov informacije, ki jih moram skrivati, se pojavi v resnični uporabi. Te informacije moramo namreč hraniti v spominu ali pa jih morajo člani rekonstruirati iz zasebnih šifer s pomočjo memorijskih ključev za enkratno uporabo. Torej nam to minimaliziranje delov informacije zelo pomaga pri shranjevanju le-teh.

5. GRAFI IN GEOMETRIJA V VEČSKUPINSKIH SHEMAH

Do sedaj smo si ogledali geometrijo v večskupinskih shemah za delitev skrivnosti, v tem poglavju pa bomo analizirali kako je ta povezana z grafično predstavitvijo oziroma realizacijo shem za delitev skrivnosti. Najprej je treba poudariti, da se bomo tu omejili le na brezpogojno varne, popolne in monotone sheme za delitev skrivnosti.
V podpoglavju 5.1. bomo začeli s predstavitvijo večskupinskih shem s pomočjo grafov. Opisati moramo osnovno terminologijo in oznake. Ogledali si bomo koliko različnih shem obstaja pri različnem številu sodelujočih skupin.
Nato bomo v podpoglavju 5.2. pogledali geometrično predstavitev večskupinskih shem in kako sta grafična in geometrična predstavitev povezani.
V podpoglavju 5.3. bomo omenili kakšna so varna in zaupna sodelovanja. Pomembno bo tudi do kakšne mere lahko sheme posplošimo in kaj se zgodi, če si skupine med seboj izmenjujejo oziroma zaupajo svoje zasebne dele informacije.

5.1. GRAFIČNA PREDSTAVITEV VEČSKUPINSKIH SHEM

Najprej moramo opisati kako bomo označevali sodelovanja med skupinami in kako bodo naši grafi predstavljeni. Zatem pa si bomo pogledali različne tabele shem za delitev skrivnosti pri različnem številu skupin.
Vzemimo najprej le dve skupini v naših shemah za delitev skrivnosti. Tu obstajata le dva načina kontrole nad deljenjem skrivnosti:

- vsaka skupina lahko posamezno sproži akcijo,
- za sprožitev akcije potrebujemo soglasje obeh skupin.

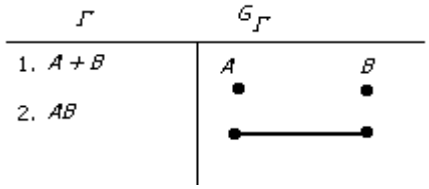
Prva situacija se ujema s situacijo, ko potrebujemo kodo za odpiranje trezorja in oba podpredsednika imata to kodo. Torej lahko trezor odpre en sam, brez sodelovanja z drugim. Druga pa ustreza situaciji, ko v ameriški vojski potrebujemo dva ključa za izstrelitev rakete in to oba naredita istočasno (dva častnika morata istočasno obrniti vsak svoj ključ).
Skupine v shemah bomo označili z velikimi črkami A, B,… in uporabili bomo znaka + in *, za katera velja:

+ bo pomenil logično ALI, v našem primeru je to prva situacija,
* pa pomeni logični IN. To pa je druga situacija v našem primeru.

V primeru dveh skupin imamo torej dve možnosti kakšna bo shema:

- $\Gamma = A + B$
- $\Gamma = AB$ (krajše za $A * B$)

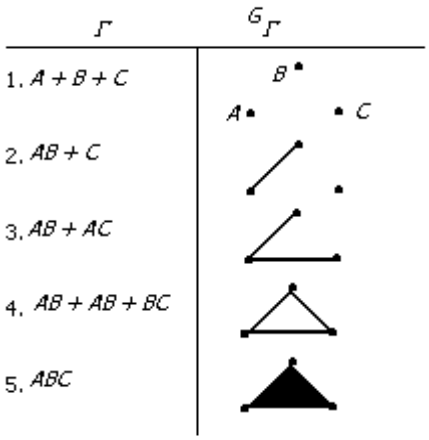
To lahko predstavimo grafično:



Slika 5.1: Prikaz sodelovanja dveh skupin s pomočjo grafov.

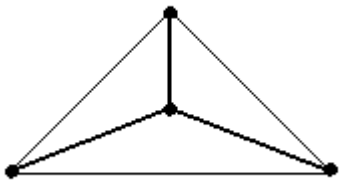
Na desni strani daljica prikazuje, da se mora v primeru A+B strinjati le ena skupina za sprožitev akcije. Ta situacija je opisana z grafom, ki vsebuje le dve točki, kjer je vsaka točka zadostna za sprožitev akcije. V drugem primeru AB se morata strinjati obe skupini za sprožitev akcije oziroma za pridobitev skrivnosti in to je na grafu prikazano s povezavo, ki povezuje točki A in *B*.

V primeru treh skupin je situacija nekoliko bolj zanimiva, saj v tem primeru dobimo za delitveno shemo 5 možnosti:

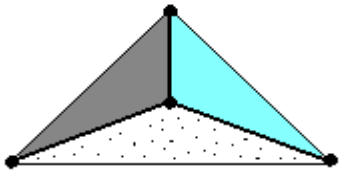


Slika 5.2: Grafi shem pri sodelovanju treh skupin.

Neoznačeni grafi shem G_Γ, v desnem stolpcu tabele, so korespondentni ekvivalentnemu razredu večskupinskih shem. Večskupinske sheme, prikazane v stolpcu Γ, dobimo, ko predpišemo sodelovanje med skupinami.

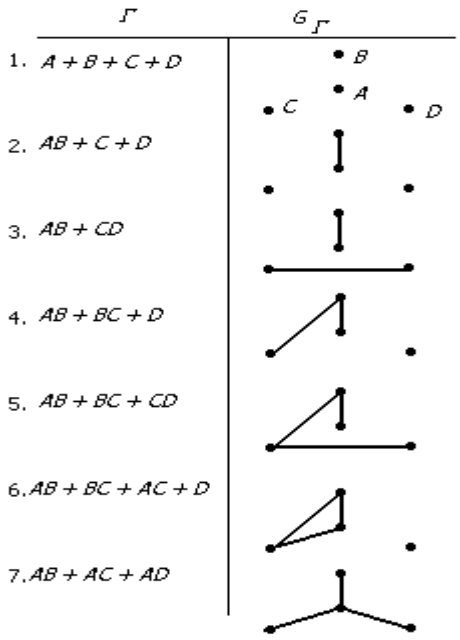


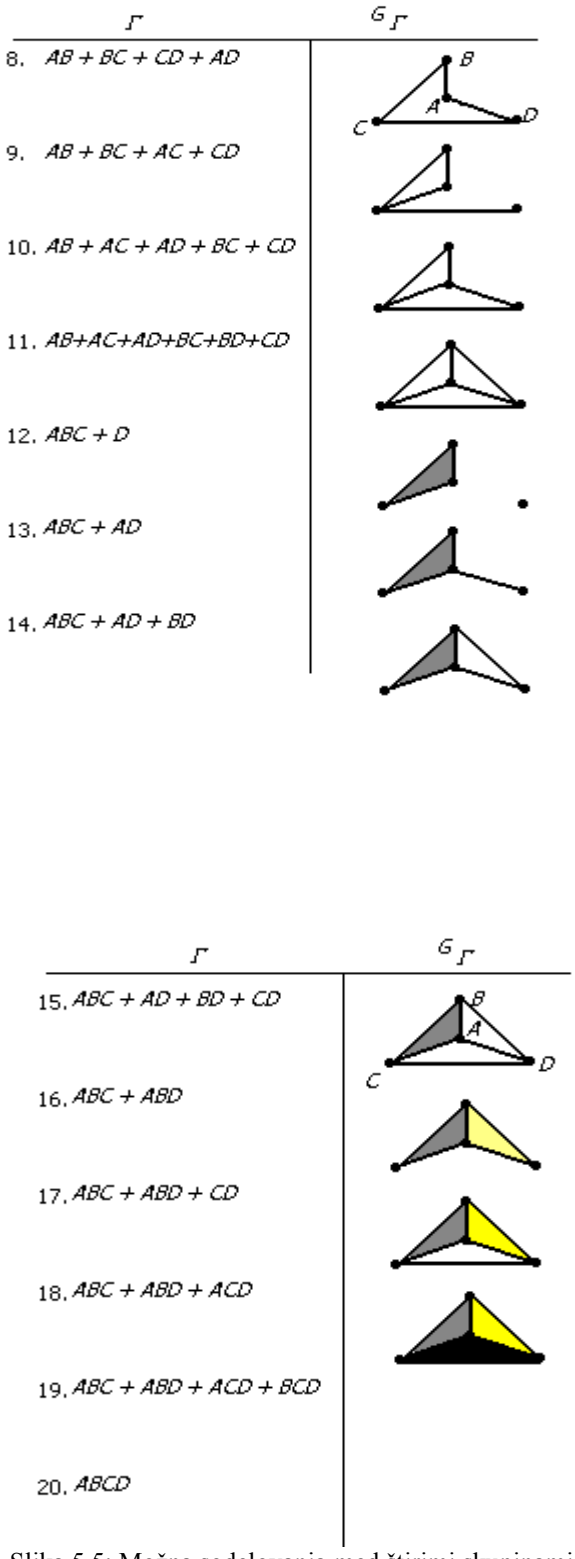
Slika 5.3: 2-4 delitvena shema



Slika 5.4: Večskupinska shema, v kateri vsak par od treh skupin s soglasjem določene četrte skupine lahko sproži želeno akcijo.

Četrta skupina na sliki 5.4 ima nekakšno pravico veto, kar pomeni, da je njen podatek oziroma soglasje potrebno za sprožitev akcije (ostale tri skupine, brez četrte, te akcije ne morejo sprožiti). Vendar kljub tej njeni pravici veto sama, brez ostalih skupin, akcije ne more sprožiti. Ta oblika sheme je lahko uporabna v našem primeru sodelovanja med Ameriko in Evropo, ki smo ga pogledali v prejšnjem poglavju (glej konstrukcijo 4.11).
Slika 5.5 prikazuje 20 večskupinskih shem, ki so možne pri sodelovanju štirih skupin. V stolpcu Γ so prikazane možne večskupinske sheme. Sheme 1, 11, 19 in ustrezajo 1-4, 2-4, 3-4 in 4-4 delitvenim shemam.

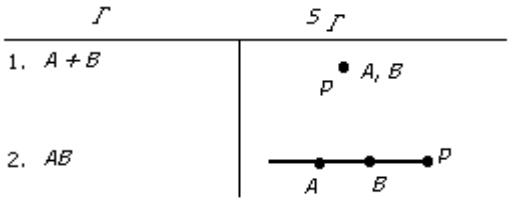




Slika 5.5: Možna sodelovanja med štirimi skupinami.

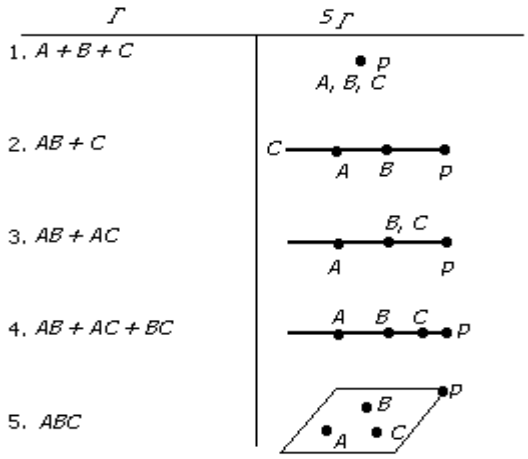
5.2. GEOMETRIČNA KONSTRUKCIJA SHEM ZA DELITEV SKRIVNOSTI

Sedaj bomo prikazali kako lahko povežemo grafično in geometrično predstavljene sheme za delitev skrivnosti. Poglejmo si še enkrat, kako geometrično lahko predstavimo sheme za delitev skrivnosti.
Najprej si poglejmo nekaj primerov in konstrukcij geometričnih predstavitev shem, da ponazorimo razliko pri konstrukciji. Nato pa bomo uporabili izreke s katerimi lahko povezujemo geometrično in grafično predstavitev shem za delitev skrivnosti.
Če je večskupinska shema dovolj enostavna, potem je tudi njena geometrična upodobitev očitna. To je res v primeru dveh shem, kjer sodelujeta le dve skupini:



Slika 5.6: Geometrična predstavitev sheme za delitev skrivnosti z dvema skupinama.

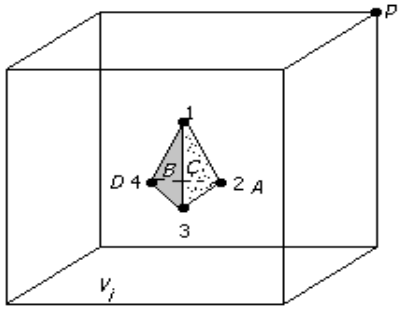
Pri geometričnih predstavitvah uporabljamo le geometrične objekte in zato je za predstavitev sheme, kjer zadostuje za sprožitev akcije le zasebni del informacije ene skupine, dovolj le ena točka. Vidimo, da je geometrična predstavitev enaka kot smo je vajeni iz prejšnjega poglavja. To pomeni, da potrebujemo podprostor v katerem skrivamo skrivnost (domeno) in indikatorski prostor, ki kaže na skrivnost. Njun presek nam poda našo skrivno točko *p*.
Geometrične predstavitve shem za delitev skrivnosti, prikazane s petimi možnimi večskupinskimi shemami, kjer sodelujejo tri skupine, so tudi zelo enostavne:



Slika 5.7: Geometrična predstavitev shem za delitev skrivnosti s tremi skupinami.

V splošnem to ne bo res, ker zahtevamo bolj formalno konstrukcijo geometričnih shem. Sheme za delitev skrivnosti, prikazane na sliki 5.5 ni tako enostavno konstruirati. Za primer bomo uporabili večskupinsko shemo 5 iz slike 5.5. Ni si tako težko izmisliti primera za geometrično shemo za delitev skrivnosti, ki ustreza shemi Γ, vendar sama konstrukcija ni tako lahka. Recimo, da je indikatorski prostor V_i 3-razsežen, potem edino možno shemo dobimo s konstrukcijo 5.1.

KONSTRUKCIJA 5.1:



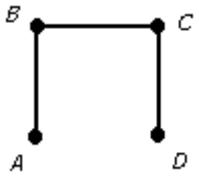
Slika 5.8: Predstavitev večskupinske sheme kjer je indikatorski prostor 3-razsežen.

1. *Štiri točke* 1, 2, 3 *in* 4 *so izbrane v smeri urinega kazalca. Vzemimo* 4 *ravnine, kjer nobena izmed njih ne sme vsebovati točke p. Vsaka trojica točk* 1,2,3 *in 4 leži v eni izmed ravnin.*
2. *Skupini A in D dobita zaporedoma točki* 2 *in* 4 *kot svoja zasebna dela informacije. Skupini B dodelimo ravnino, na kateri ležijo točke* 1, 3 *in* 4. *Skupini C pa dodelimo ravnino na kateri ležijo točke* 1, 2 *in* 3.
3. *Podprostor, ki ga določata skupini A in B ali B in C ali C in D razpenjajo 3-razsežen indikatorski podprostor* V_i. *Velja tudi, da noben drug par ne more razpenjati* V_i.
4. *Točka skupine A leži v ravnini, ki je bila dodeljena skupini C, katera po definiciji ne vsebuje točke p. Podobno velja za točko skupine D, ki leži v ravnini, ki smo jo dodelili skupini B.*
5. *Točki* 2 *in* 4 *določata premico, ki leži na dveh ravninah, ki ne vsebujeta točke p in zatorej ta premica ne vsebuje točke p.*

Trditev 5.1: *Shema, prikazana s konstrukcijo* 5.1*, je popolna monotona geometrična shema za delitev skrivnosti.*

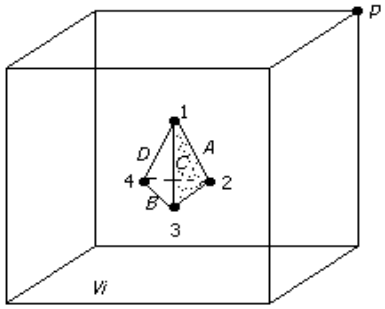
■

Poglejmo sedaj simetrije, ki jih najdemo v geometričnih predstavitvah shem za delitev skrivnosti, saj si bomo z njimi pomagali povezati grafične in geometrične predstavitve shem.
Graf sheme G_Γ za 2-4 delitveno shemo lahko narišemo tako, da poudarimo simetrijo:



Opazimo lahko, da imata grafična predstavitev G_Γ in geometrična predstavitev S_Γ, enako grupo avtomorfizmov. To je res tudi za ostale manjše primere katere smo do sedaj srečali. Če bi to lahko posplošili na vse primere in bi bilo to močno orodje pri konstrukciji geometričnih predstavitev shem S_Γ. Na žalost to ni vedno res kot bomo videli v naslednji konstrukciji.

KONSTRUKCIJA 5.2:



Slika 5.9: Nesimetrična shema za delitev skrivnosti..

1. *Dodelitev privatnih delov informacije: skupina A dobi daljico s točkama* 1 *in* 2*, skupina B dobi daljico s točkama* 3 *in* 4*, skupina C dobi ravnino s točkami* 1*,* 2*,* 3*, in skupina D dobi daljico s točkama* 1 *in* 4*.*

Trditev 5.2: *Shema po konstrukciji* 5.2 *je popolna in monotona, vendar skupine med seboj niso enakovredne.*

■

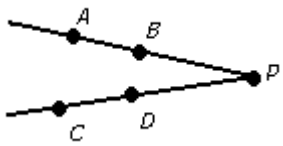
Poglejmo si izreke, ki veljajo za sheme, ki jih dobimo po združitvi več večskupinskih shem v eno samo shemo. S temi izreki bomo povezali grafične predstavitve shem z geometričnimi predstavitvami. Večina jih je očitnih, ker izhajajo iz lastnosti shem, zato jih ne bomo dokazovali.

Izrek 5.3: *Če je hipergraf, ki predstavlja večskupinsko shemo G_Γ, disjunkten, potem je geometrično predstavitev sheme S_Γ mogoče konstruirati kot unijo neodvisnih geometričnih shem posameznih komponent hipergrafa G_Γ, ki vse kažejo na točko p v domeni V_d.* ■

Primer 5.1:
Ta izrek lahko uporabimo v tretji shemi na sliki 5.5.

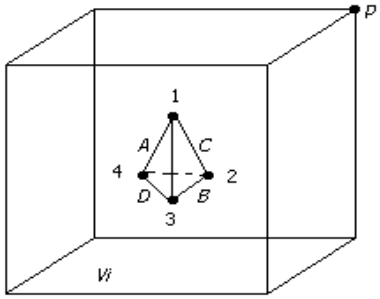
$\Gamma = AB + CD$.

Ker vsebuje hipergraf sheme G_Γ dve komponenti, bomo po izreku 5.3 imeli dva indikatorska podprostora v shemi za delitev skrivnosti, ki oba kažeta na točko p in z unijo teh dveh dobimo geometrično predstavitev S_Γ.



Slika 5.10: Dva indikatorska podprostora sestavljata geometrično predstavitev S_Γ.

Zanimivo je primerjati to enostavno predstavitev s tisto, ki vsebuje samo en podprostor. To pomeni konstrukcijo brez pomoči izreka 5.3:



Slika 5.11: Geometrična predstavitev sheme za delitev skrivnosti $\Gamma = AB + CD$ le z enim indikatorskim podprostorom.

Očitno je, da skupini s točkama A in B določata 3-razsežen prostor V_i in s tem določita točko p.

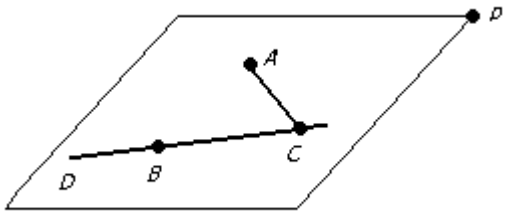
Izrek 5.4: *Geometrična predstavitev večskupinske sheme Γ, kjer je lahko Γ deljen na produkte disjunktnih logičnih izrazov, je prostor, ki ga napenjajo geometrične predstavitve posameznih faktorjev.*

■

Izrek 5.4 lahko uporabimo v trinajsti večskupinski shemi na sliki 5.5:

$\Gamma = ABC + AD = A(BC + D)$

Ko uporabimo izrek 5.4, lahko enostavno konstruiramo tako shemo za delitev skrivnosti:



Slika 5.12: Konstrukcija sheme za delitev skrivnosti po izreku 5.4.

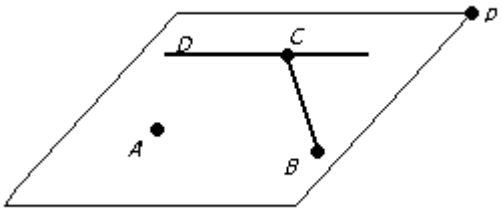
Izrek 5.5*: Geometrično predstavitev večskupinskih shem, v kateri lahko shemo Γ razstavimo na vsoto produktov, ki disjunktno ločijo spremenljivke, lahko predstavimo kot unijo geometričnih predstavitev iz izrekov* 5.3 in 5.4.

■

Opomba: V izreku disjunktno ločiti spremenljivke pomeni, da izpostavimo kar se da.

Izrek 5.4 lahko uporabimo v štirinajsti večskupinski shemi na sliki 5.5:

$\Gamma = ABC + AD + BD = (AB)C + (A + B)D.$
Ta konstrukcija izgleda takole:



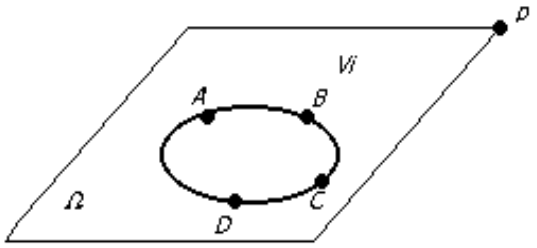
Slika 5.13: Konstrukcija sheme za delitev skrivnosti po izreku 5.5.

Izrek 5.6: *Večskupinsko shemo Γ, katere predstavitev hipergrafa je $G_\Gamma = K_{w,t}$ t..j. poln hipergraf, sestavljen iz vseh $\binom{w}{t}$ t-lic, lahko predstavimo z množico t linearno neodvisnih točk v (t – 1)-razsežnem indikatorskem prostoru.*

Dokaz: Γ sestoji iz $\binom{w}{t}$ podmnožic s t skupinami od w skupin. To je enostavna t-w delitvena shema. Imamo t linearno neodvisnih točk v $(t - 1)$-razsežnem prostoru. Nobena podmnožica j točk, $2 \le j \le t - 1$, ne more ležati v podprostoru, ki je manjši od $(j - 1)$-razsežnega prostora. Torej, ker je podprostor V_i edini $(t - 1)$-razsežen prostor, mora vsaka podmnožica t točk napenjati V_i.

■

Izrek 5.6 lahko uporabimo v enajsti in devetnajsti večskupinski shemi na sliki 5.5. Konstrukcija geometrične predstavitve S_{11} je očitna. Konstrukcija geometrične predstavitve S_{19} pa je bolj zanimiva. Sestavljena je iz štirih točk v ravnini V_i, noben par ni kolinearen s točko p.



Slika 5.14: Uporaba izreka 5.6 pri konstrukciji sheme za delitev skrivnosti.

Krivulja Ω, ki leži na štirih točkah A, B, C in D, je stožernica. To pomeni, da v obsegu lihe karakteristike v množici točk v prostoru V_i , nobena trojica ni kolinearna. Enaka konstrukcija bi veljala za 3-w delitveno shemo.
Če točka p leži na stožernici Ω, bi bila maksimalna vrednost w-ja lahko q, če pa točka p ne leži na stožernici Ω pa $(q + 1)/2$. Razlog za to je, da vsaka sekanta stožernice Ω,

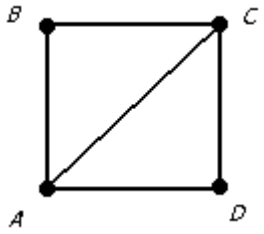
skozi točko *p*, lahko leži samo na eni izmed točk Ω, ki jo uporabimo za zasebnii del informacije.

Izrek 5.7: Če na hipergrafu, ki predstavlja večskupinsko shemo, ležita dve ali več neodvisnih in izomorfnih točk, lahko vse te točke identificiramo v reduciranem hipergrafu, ki predstavlja isto večskupinsko shemo.

■

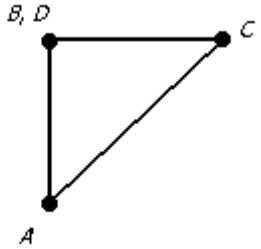
Ta izrek je od vseh izrekov do sedaj najbolj uporaben. Velja za mnoge od shem na sliki 5.5. Na deseti shemi na sliki 5.5 bomo pogledali njegovo uporabnost:

$\Gamma = AB + AC + AD + BC + CD.$



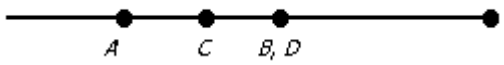
Slika 5.15: Delitvena shema z uporabo izreka 5.7.

Točki *B* in *D* sta neodvisni in izomorfni in zatorej ju po izreku 5.7 lahko identificiramo. Poenostavitev hipergrafa izgleda sedaj takole:



Slika 5.16: Poenostavitev konstrukcije na sliki 5.15.

Za to predstavitev velja izrek 5.6 in en izmed rezultatov geometrične predstavitve je:



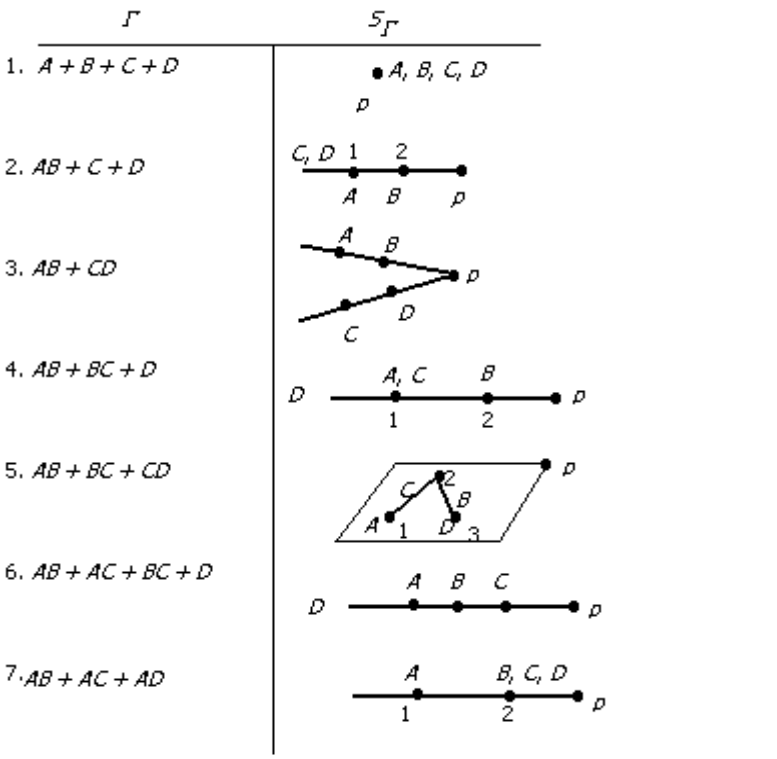
Slika 5.17: Geometrična predstavitev desete sheme na sliki 5.5.

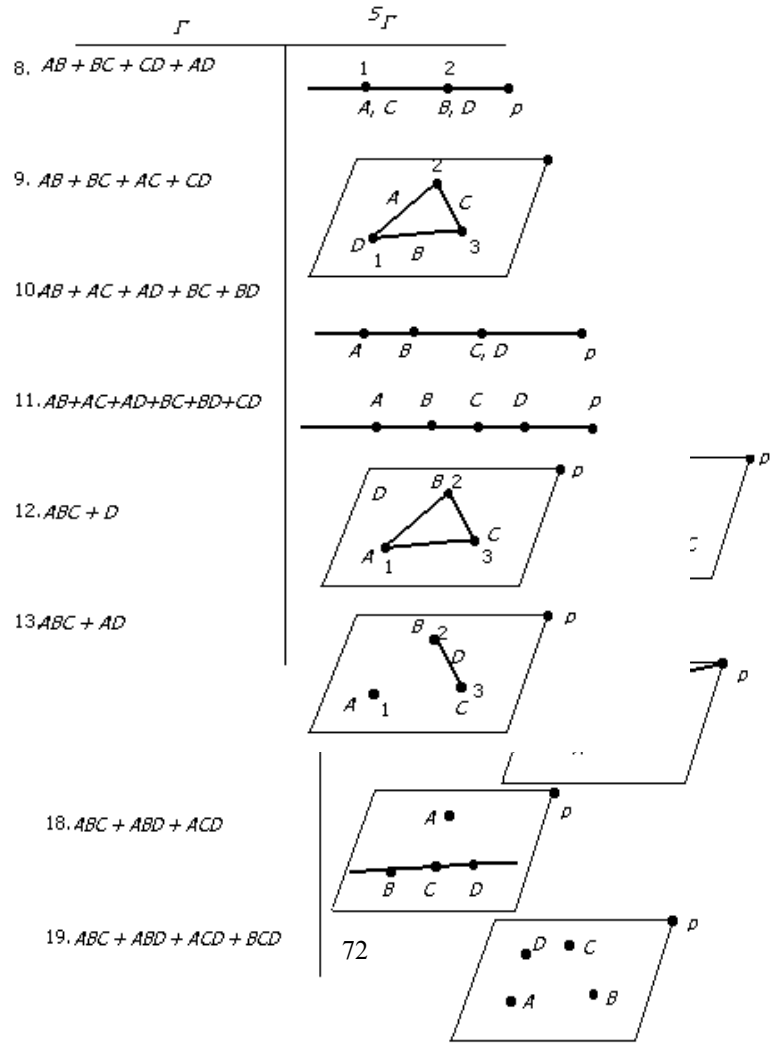
Skoraj tako uporabna kot izrek 5.7 je propozicija, ki dovoljuje konstruktorju, da dodaja nove skupine obstoječi shemi za deljenje skrivnosti, če imajo nove skupine isto moč kot ena že katera od obstoječih skupin.

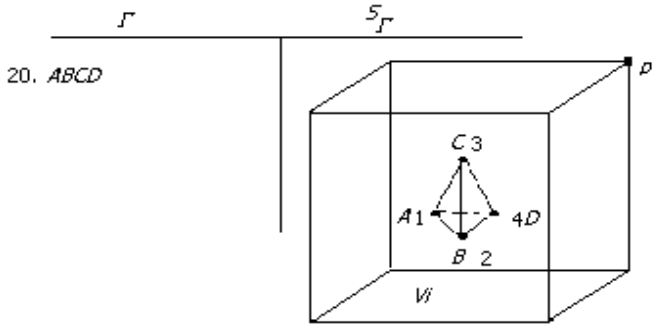
Propozicija 5.8: *Če imamo podano predstavitev večskupinske sheme, lahko dodelimo poljubno velik del informacije poljubno mnogo skupin, ki so neodvisne in izomorfne po moči.*

■

Na sliki 5.18 imamo prikazane geometrične predstavitve shem za deljenje skrivnosti, ki predstavljajo sheme iz slike 5.5. Nekatere izmed teh konstrukcij so enostavne, nekatere druge pa so postale enostavne s pomočjo danih izrekov. Vendar ostajajo predstavitve, ki sploh niso tako očitne.







Slika 5.18: Poenostavljene geometrične predstavitve shem pri sodelovanju štirih skupin.

5.3. ZAUPNO SODELOVANJE

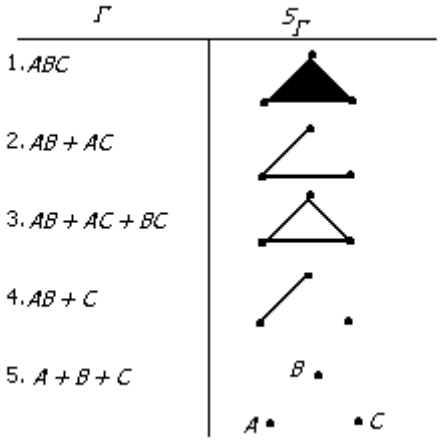
Sedaj si bomo pogledali še kaj se zgodi, če si skupine med seboj zaupajo in izmenjujejo svoje zasebne dele informacije. Do sedaj smo vedno privzeli, da skupine ne bodo objavile svojih zasebnih delov informacije razen v trenutku, ko želijo sprožiti akcijo. S tem nismo predpostavili, da lahko vsem skupinam popolnoma zaupamo. Obstajajo celo študije takih shem, kjer nekaterim skupinam ne smemo zaupati.

Realno gledano obstaja možnost, da neka skupina deli svoj zasebni del informacije z nekom, ki mu zaupa. Posledica tega je lahko presenetljiva (za center za distribucijo ključev, ki je nastavil tako shemo). Če vzamemo dve skupini pri predstavitvi sheme $\Gamma = AB$ (druga shema na sliki 5.3) in če skupina A zaupa skupini B in ji tako zaupa svoj zasebni del informacije, lahko zatem skupina B sama sproži akcijo. S tem se spremeni pravilo sodelovanja. Vendar v logiki delitve nadzora ni simultanosti, le določitev katere informacije so potrebne za sprožitev akcije. Skupina A je dala torej svojo informacijo skupini B, ki jo lahko prosto uporablja brez dovoljenja skupine A. In tako deljenje ključev lahko pričakujemo.

Poglejmo še večskupinsko shemo $\Gamma = AB + AC + AD$ (sedma shema na sliki 5.5 in 5.8). Namen centra za distribucijo ključev v tem primeru je, da se mora A strinjati z vsaj enim od B, C ali D, da je lahko akcija sprožena. O tem smo že govorili v primeru sporazumov, ko ima Amerika pravico veto nad drugimi državami, vendar sama ne mora sprožiti akcije. V tem primeru skupina A potrebuje vsaj še eno skupino za sprožitev akcije. Recimo, da skupina A zaupa svoj zasebni del informacije dvema skupinama B in C. Vendar vsaki skupini le en del. Skupini B in C sestavita to informacijo in imata cel zasebni del informacije skupine A. Skupina B oziroma C sama ne sme sprožiti akcije. Shemo Γ nadomestimo z novo shemo : $\Gamma' = AB + AC + AD + BCD$, kjer lahko sedaj skupine B, C in D brez A sprožijo akcijo. Posledica tega zaupanja je bolj presenetljiva od prejšnjega primera, saj smo uporabili nadomestilo, da smo lahko odstranili pooblaščeno skupino. Tukaj smo ga nadomestili s podmnožico drugih skupin. Rezultat je, da lahko druge množice skupin sprožijo akcijo. V prvem primeru smo skupino A čisto odstranili v drugem pa smo jo nadomestili z dvema drugima skupinama, B in C:

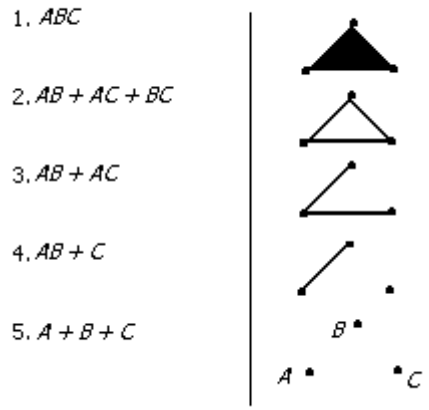
$ABC \rightarrow BCBC \rightarrow BC$ in $AD \rightarrow BCD$.

Torej, če neka podmnožica skupin zaupa svoje zasebne dele informacije drugi podmnožici skupin, lahko na koncu dobimo drugačno shemo za delitev skrivnosti od prvotne. Ko center za distribucijo ključev sestavi shemo za delitev skrivnosti, mora implicitno pregledati in sprejeti vse možne večskupinske sheme, ki jih lahko dobimo iz prvotne sheme, kot rezultat zaupanja med skupinami, saj ne more vedeti in nadzorovati deljenja zasebnih delov informacije med skupinami.
Obstajajo sodelovanja, ki jih ne moremo dobiti iz nobenega zaupanja med skupinami. Sheme $\Gamma = AB$ ne moremo dobiti iz nobenega zaupanja med skupinami iz sheme $\Gamma = A + B$, saj če lahko vsaka skupina posebej sproži akcijo ne more druga skupina storiti nič, da bi to preprečila. Zaupanje samo poveča moč skupin, ki sodelujejo in ne more vzeti nobenega pooblastila prvotnim podmnožicam, ki so imele možnost sprožitve akcije.
Možnosti shem, ki jih s pomočjo zaupanja dobimo iz prvotne sheme, lahko predstavimo z mrežo shem za delitev skrivnosti. V primeru dveh skupin, shema AB prevlada nad shemo $A + B$ in zaupanje, ki je potrebno, da pridemo do sheme $A + B$ iz sheme AB je, da mora skupina A zaupati skupini B obratno. Za tri skupine je situacija malo bolj zapletena. Očitno je, da shema ABC prevlada nad vsemi ostalimi večskupinskimi shemami in shemo $A + B + C$ prevladajo vse ostale večskupinske sheme, ki jih pri zaupanju lahko dobimo. Vrstni red teh shem pa moramo analizirati. Shema $AB + AC$ nadvlada shemi $AB + AC + BC$, saj če skupina A zaupa hkrati skupini B in skupini C (A nadomestimo z BC), dobimo $AB + AC \rightarrow BCB + BCC \rightarrow BC$ in $\Gamma' = AB + AC + BC$.
Podobno $AB + AC + BC$ nadvlada $AB + C$ in pri tem mora skupina A zaupati skupini C. Troskupinske sheme so razvrščeni na sliki 5.19:



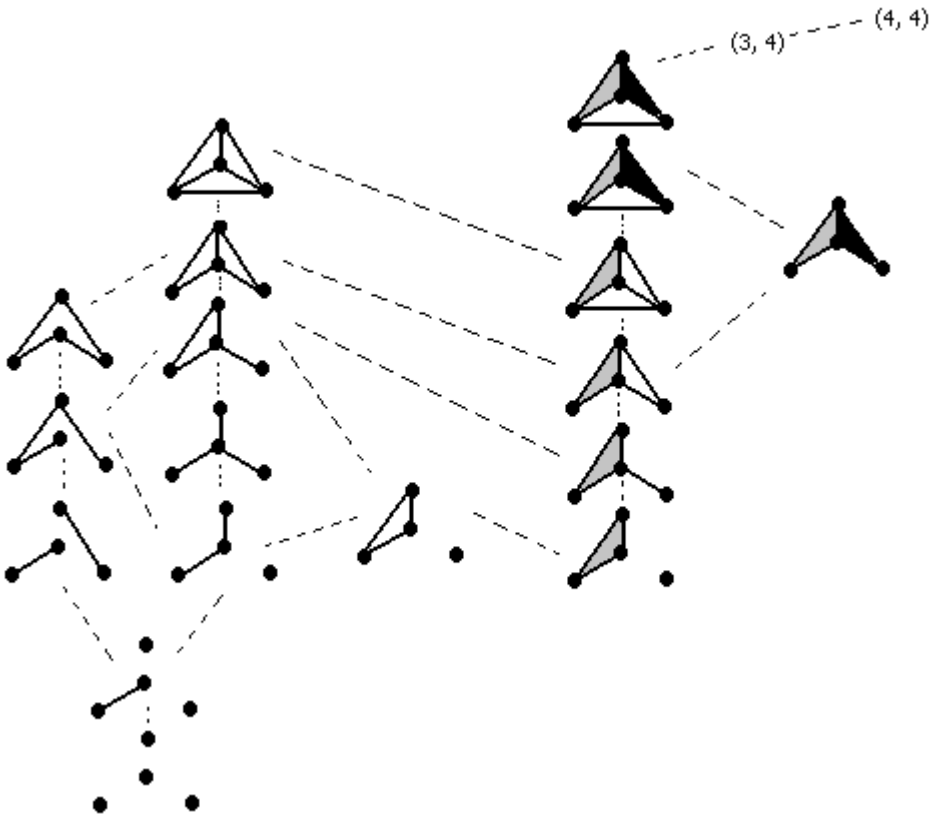
Slika 5.19: Troskupinske sheme za delitev skrivnosti kjer je vrstni red določen po nadvladi.

V geometrični mreži hipergrafov, kjer je vrstni red določen po množicah (povezavah), ki so vključene, je ta vrstni red drugačen:



Slika 5.20: Troskupinske sheme kjer je vrstni red določen po vključenih množicah.

Zamenjava vrstnega reda $AB + AC + BC$ in $AB + AC$ v teh dveh mrežah je proti primer za ekvivalenco med geometrično mrežo in mrežo večskupinskih shem, ki smo jo sestavili (mreža hipergrafov). Trenutno vemo le kakšno je razmerje med tema dvema mrežama. Slika 5.21 prikazuje geometrično mrežo za tri skupine.



Slika 5.21:Geometrična mreža za tri skupine.

Mrežo za večskupinske sheme še vedno raziskujejo tudi za tako majhno število skupin. Postavimo dve vprašanji:

Vprašanje 5.1: Vzemimo shemo za delitev skrivnosti Γ. Katere sheme za delitev skrivnosti lahko izpeljemo iz sheme Γ, kot rezultat zaupanja med skupinami.

Drugo vprašanje je zelo povezano s prvim vendar ni nujno enako:

Vprašanje 5.2: Karakterizirajte mrežo večskupinskih shem za *n* skupin!

Poglejmo razlog, da prvo vprašanje ni nujno ekvivalentno drugemu. Vzemimo za primer sheme Γ_1, Γ_2 in Γ_3. Večskupinsko shemo Γ_2 izpeljemo iz večskupinske sheme Γ_1 in shemo Γ_3 dobimo iz večskupinske sheme Γ_2, vendar ne obstaja nujno taka množica skupin, ki bi si zaupala, da bi dobili Γ_3 direktno iz Γ_1.

Odgovora na obe vprašanji sta zelo pomembna za preučevanje delitvenih zmožnosti, saj mora center za distribucijo ključev upoštevati vse sheme, ki jih lahko dobimo iz sheme Γ, saj le s tem lahko zagotovi varnost v shemi za delitev skrivnosti.

6. DELITEV KLJUČEV PREKO SHEM ZA DELITEV SKRIVNOSTI

V tem poglavju bomo analizirali praktično uporabo shem za delitev skrivnosti. Pogledali si bomo kakšni problemi se lahko pojavijo in kako jih lahko najlažje rešimo. Sheme za delitev skrivnosti sta Shamir in Blakley naredila v pomoč delitvi ključev v kriptosistemih, da bi preprečila to, da pooblaščene množice ne bi mogle priti do skrivnosti zaradi izgube ključa. Hkrati pa sta želela preprečiti, da bi prišle tudi nepooblaščene množice do ključa. V tem poglavju bomo raziskali tudi pomen shem za delitev skrivnosti kot način za delitev ključev v nekaterih uporabah.
Osnovna motivacija za razvoj večnivojskih shem je bila preprečitev tako imenovanih obglavitvenih napadov. Imamo informacijo, ki jo ima višji nivo in jo mora podati nižjemu nivoju, da lahko sprožimo akcijo (npr. sprožitev rakete). Napadalec lahko prepreči izmenjavo informacij s tem, da uniči višji nivo preden lahko ta deli informacijo z nižjim nivojem. Temu rečemo obglavitveni napad. Pri tem napadu se lahko zgodi, da nižji nivo brez informacije iz višjega nivoja, ne ve kaj bi storil ali pa pri svoji akciji ni dovolj učinkovit. Te posledice nas ne skrbijo. Skrbi nas le situacija, kjer nižji nivo ne more sprožiti akcije katero bi morali sprožiti, ker se je en ali več delov informacije izgubil zaradi obglavitvenega napada.
Večnivojske sheme so bile ustvarjene ravno zaradi tega problema. V takih situacijah lahko nižji nivo nadomesti višji nivo z določenim sodelovanjem članov v svojem nivoju. Poznamo veliko takih situacij in tu se pokaže, da je večnivojska shema dobra rešitev. Obstajajo akcije v katerih ali zakon ne dovoljuje nadomestitve višjega nivoja z nižjim ali pa višji nivo ne želi sodelovati in deliti informacije z nižjim nivojem.
Poglejmo si raketo, ki jo varuje dvanajst vojakov. Posledice, da bi bila raketa nedovoljeno izstreljena bi bile zelo velike, tako da ima pooblastilo za izstrelitev le

višji nivoji (predsednik). Torej, tudi če bi se vsi vojaki strinjali, da izstrelijo raketo, tega ne morejo narediti brez dovoljenja najvišjega nivoja.
Če ne bi bilo sheme za delitev skrivnosti, bi se višji nivo lahko branil pred obglavitvenim napadom le s tem, da bi pripravil raketo v smislu, da oznani stanje pripravljenosti. Vendar ravno v takih situacijah se največkrat kaj zalomi in raketa bi bila lahko nepravilno izstreljena. S potrebnim sodelovanjem *k* vojakov (recimo dveh vojakov) za izstrelitev rakete lahko zagotovimo večje zaupanje v pravo reakcijo v primeru bitke. To pomeni, da potrebujemo shemo v kateri ima (v normalni situaciji) le najvišji nivo pooblastitev za izstrelitev rakete. V stanju pripravljenosti pa lahko tudi vojaki s pravim sodelovanjem (*k*-12 delitvena shema) sprožijo akcijo oziroma izstrelijo raketo. Kako lahko to naredimo? Vojakom bi morali razdeliti informacije v stanju pripravljenosti na varen način. Vendar v takih trenutkih se lahko marsikdo zmoti, ko bi odkodiral ukaze za sprožitev rakete. Torej bi morali te dele razdeliti v naprej, vendar da bi te informacije lahko vojaki uporabljali le v stanju pripravljenosti in tudi če bi svoje zasebne dele združili v normalni situaciji, bi bila njihova negotovost kode enaka kot negotovost napadalca, da kodo ugane. Če dele razdelimo tako, potem v stanju pripravljenosti potrebujemo le en ukaz iz višjega nivoja, da sproži *k*-12 delitveno shemo pri vojakih. Torej če razdelimo informacije pred stanjem pripravljenosti, lahko te dele razdelimo na miren način, tako da pošljemo kurirja ali pa vsak vojak pride v štab po svoj zasebni del informacije. V stanju pripravljenosti, ko so komunikacije kod lahko izpostavljene, pa potrebujemo le en ukaz, da dovolimo sodelovanje med vojaki.
Poglejmo si še eno situacijo v primeru rakete. Recimo, da imamo več raket in želimo sprožiti le eno. Če vstavimo našo kodo za izstrelitev rakete oziroma vojaki sestavijo svoje zasebne dele informacij, da izstrelijo rakete, želimo da se ostale rakete ne izstrelijo in da je kakovost kontrole nad ostalimi ista. To bi sicer lahko storili tako, da vzamemo za vsako raketo drugo izstrelitveno kodo, vendar potem si bi moral vsak vojak zapomniti preveč informacij. Potrebujemo način, da lahko isti zasebni del informacije odkrije druge različne zasebne dele informacije.
Še en enako pomemben problem je ta, da se mora po preklicu stanja, pooblastitev nad nadzorom rakete vrniti višjemu nivoju. Torej potrebuje višji nivo ukaz, da prepreči sodelovanje vojakov in jim odvzame zmožnost za izstrelitev rakete. S preklicem pooblastitve pa ima sedaj višji nivo spet identično enako kontrolo nad raketo kot prej. Torej mora biti sistem obrnljiv in kontrola enaka brez, da bi spreminjali zasebne dele informacije. S tem se mora koda za sprožitev pooblastitve in koda za preklic pooblastitve za vsako delegacijo spremeniti, če je slednja to kodo uporabila ali ne.
Do sedaj obstajata vsaj dva načina s katerima lahko to naredimo. Prvi način je, da bi se kode za preklic spreminjale s časom, recimo enkrat na dan. Drugi način bi bil, da bi mehanizem, ki izračuna prave kode iz zasebnih delov informacije, imel seznam kod in le ena od teh kod bi delovala ob določenem času. Torej, če bi poslal višji nivo kodo za preklic pooblastitve, bi s tem raketa spremenila kodo, tako da bi lahko spet le višji nivo sprožil raketo. Stara koda, ki jo sestavijo vojaki, bi postala tako neuporabna. Ta primer, ki je sicer dovolj realen, smo uporabili, da prikažemo dve lastnosti shem za delitev skrivnosti:

- Četudi sodelujejo vsi člani nižjega nivoja ob nepravem času in sestavijo svoje dele, je njihova negotovost skrivnosti enaka kot negotovost napadalca, da ugane skrivnost. Torej morajo biti sheme za delitev skrivnosti popolni.
- Shemo za delitev skrivnosti je možno aktivirati z enim samim ukazom in s tem ukazom je možno odkrivati različne informacije (z uporabo istega dela informacije), če imamo več ukazov za izstrelitev rakete.

Da smo lahko ustvarili večnivojske in večskupinske sheme za delitev skrivnosti, smo morali prilagoditi indikatorski podprostor V_i, tako da smo naredili več neodvisnih indikatorjev (slika 4.7) ali pa več odvisnih indikatorjev (slika 4.1) ali več funkcijsko povezanih indikatorjev (sliki 4.12 in 4.13.). Da bi dobili sheme za delitev skrivnosti, ki smo jih opisali, bomo morali spremeniti tudi domeno V_d. Spremenili jo bomo tako, da je ne bomo podali kot javni del informacije ampak jo bomo objavili šele, ko bo podana koda za pooblastitev ali pa bomo imeli več domen (neodvisnih ali pa funkcijsko povezanih).
Očiten način za implementacijo take sheme bi bil, da razdelimo dele članom, vendar objavimo domeno šele, ko zares želimo, da člani lahko sodelujejo. Če torej sodelujejo vsi člani brez dovoljenja, je največ kar lahko naredijo to, da rekonstruirajo indikatorski podprostor in torej ugibajo skrivno točko p le iz indikatorskega podprostora. Zunanji napadalec pa še vedno ugiba skrivno točko v celem prostoru S. Vendar tu se pojavi problem, ki ga bomo analizirali na dveh primerih.
V primeru 2-w delitvene sheme iz slike 4.19, sta oba podprostora V_i in V_d, premici na ravnini S. Ker je ravnina S 2-dimenzionalna, določata dva zasebna dela informacije (dva elementa iz GF(q)) premico v afini ravnini AG(2, q). Dve točki potrebujemo tudi, da določimo domeno V_d. Problem je torej v tem, ker potrebujemo enako količino informacij, da določimo indikatorski podprostor in enako količino informacij, da določimo domeno. Torej bi morali za sprožitev delitvene sheme posredovati dve informaciji oziroma dve točki namesto ene. Vendar, ko enkrat z našimi zasebnimi deli informacije konstruiramo indikatorski podprostor, skrivna točka p ni več točka v ravnini S, vendar točka na indikatorskemu prostoru V_i, ki je v našem primeru premica. Torej potrebujemo le en podatek, da določimo točko p na premici.
Če konstruiramo 3-w delitveno shemo prikazano na sliki 3.9, kjer je S 4-razsežni prostor in je domena V_d ravnina, je problem še težji. V tem primeru damo štiri od šestih točk za zasebne dele informacije članom, da nastavimo shemo. Ostala dva dela pa podamo v kodi za odobritev pooblastitve članov v stanju pripravljenosti. V tabeli 5.1 je prikazana zahtevnost problema pri m-afinih podprostorih v n-razsežnem prostoru. Če sta podprostora V_i in V_d oba 3-razsežna dobimo lahko le 4-w delitveno shemo in prostor 3-afinih podprostorov je že 12-razsežen, kar pomeni, da potrebujemo 12 delov informacije, da določimo domeno V_d.

	m							
n	0	1	2	3	4	5	6	7
1	1							
2	2	2						
3	3	4	3					
4	4	6	6	4				
5	5	8	9	8	5			
6	6	10	12	12	10	6		
7	7	12	15	16	15	12	7	
8	8	14	18	20	20	18	14	8

Tabela 5.1. dimenzija prostora m-razsežnih afinih prostorov v n-dimenzionalnem prostoru.

Naše drugo poglavje smo namenili splošnim modelom shem za delitev skrivnosti. Imeli smo dva pristopa. En pristop je bil ta, da smo imeli zasebne dele informacije, ki so napenjali indikatorski podprostor, ki je kazal na skrivno točko. Drug pristop pa je bil ta, da smo s presekom dveh geometričnih objektov dobili skrivno točko p. Oba

pristopa sta nam zagotavljala popolno varnost, vendar drugi pristop sploh ne predstavlja popolne sheme za delitev skrivnosti. Pogledali smo si kako izgleda shema, če jo predstavimo s kriptografskimi ključi in ravno s tem lahko vidimo ekvivalenco pri varnosti med dvema pristopoma.
Pri odkrivanju skrivnosti smo iskali skrivno točko p v kateri je skrivnost. Torej točka p ni še skrivnost ampak iz nje z neko funkcijo skrivnost šele izračunamo. V nekaterih primerih je bila ta funkcija projekcija točke p na eno izmed osi. Sedaj glejmo točko p kot kriptografski ključ velik 56-bitov za DES (Data Encryption Standard) in naj bo koda za odobritev pooblastila kodirano besedilo, ki ga lahko odkodiramo s kriptografskim ključem [1]. Tako rešimo naše probleme z vojaki in raketo. Če vojaki sodelujejo pred stanjem pripravljenosti, lahko odkrijejo le ključ, vendar besedilo oziroma kode za pooblastitev višji nivo še ni poslal in tako je ključ neuporaben, saj ni kaj za odkodirati. Ni nam treba vsakič spreminjati zasebnih delov informacije, saj se da s fiksnim ključem odkodirati vsako zakodirano besedilo, ki ga pošlje vojakom višji nivo.
Poglejmo si implementacijo te sheme. Poglejmo enostavno 2-w delitveno shemo uporabljeno z DES algoritmom. V tem primeru imamo ravnino AG(2, 2^{56}). Vsak del informacije je velik 112-bitov in vsak član varuje 56-bitov. Domena V_d ali raje dva dela informacije, ki določata domeno V_d, bosta dana, ko bomo aktivirali shemo. V tem trenutku bo lahko vsaka dvojica določila podprostor V_i in s tem skrivnost p, ki je v tem primeru točka v AG(2, 2^{56}).
Ni razloga zakaj ne bi za funkcijo, ki spremeni točko p v iskano skrivnost, vzeli projekcijo na y-os. In ta projekcija je DES ključ. Pooblaščena množica lahko odkrije DES ključ vendar skrivnost lahko odkrijejo le, ko je shema aktivirana.
V primerih, kjer je sprejemljivo, da s pravim sodelovanjem lahko kadarkoli odkrijemo skrivnost, lahko kodirano besedilo (kodo za pooblastitev) podamo že takrat, ko delimo zasebne dele informacije. V primeru vojakov pa kodirano besedilo oziroma kodo za pooblastitev pošljemo šele, ko želimo, da člani odkrijejo skrivnost. Takrat pošlje višji nivo minimalno en del informacije članom na nižjem nivoju za vsako skrivnost posebej in tako lahko tudi nižji nivo sproži akcijo.

7. LITERATURA

[1] D. R. Stinson, Criptography: Theory and Practise, CRC Press, 1995.

[2] I. Vidav, Algebra, Mladinska knjiga, 1989.

[3] L.M. Batten, Combinatorics of Finite Geometries, Cambridge University Press, 1997.

[4] P.J. Cameron, Projective and Polar Spaces, London: University of London, 1992.

[5] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, Oxford: Clarendon Press, 1979.

[6] G. J. Simmons, Geometric shared secret and/or shared control schemes, v "Advances in Cryptology -- CRYPTO '90", A. J. Menezes and S. A. Vanstone, eds., *Lecture Notes in Computer Science* **537** (1991), 216-241.

[7] G. J. Simmons, An introduction to shared secret and/or shared control schemes and their application, v "Contemporary Cryptology, The Science of Information Integrity", G. J. Simmons, ed., IEEE Press, 1992, 441-497.

[8] J.H. Lint in R.M. Wilson, A Course in Combinatorics, Cambridge: Cambridge University Press, 1993.

[9] D.M. Cvetković, Kombinatorika : klasična i moderna, Beograd: Naučna knjiga, 1984.

[10] M.K. Bennett, Affine and Projective Peometry, New York [etc.]: John Wiley & Sons, cop. 1995