Vizualne sheme za deljenje skrivnosti

sta vpeljala Naor in Shamir leta 1994.

Sliko razdelimo na dele (pravzaprav na prosojnice) z belimi in črnimi pikami/kvadrati), rekonstruiramo pa jo tako, da nekaj prosojnic prekrijemo, tj. naložimo eno na drugo.

Sledimo Stinsonovemu članeku:

Visual Cryptography and Threshold Schemes, Dr. Dobb's Journal, #284, April 1998, pp. 36-43.

Oglejmo si $(2,2)$-stopenjsko shemo ($\square \to 0$, $\blacksquare \to 1$):

- če prekrijemo "**belo**" in "**belo**" dobimo "**belo**" ($0+0=0$, ODLIČNO!),
- če prekrijemo "**belo**" in "**črno**" dobimo "**črno**" ($0+1=1$, ODLIČNO!),
- če prekrijemo "**črno**" in "**črno**" dobimo "**črno**" ($1+1=1$, NE GRE!!!),

Naš vizualni sistem naredi booleanski *ali*, mi pa bi potrebovali booleanski *ekskluzivni ali*.

Naor in Shamir sta se domislila, da nadomestimo vsak kvadrat na sliki z nekaj manjšimi pravokotniki, ki bodo predstavljali dele skrivnosti. Število manjših pravokotnikov označimo z m.

Če je "sivina" črnih kvadratov (v t prekritih delih) temnejša kot sivina belih kvadratov, potem se sliko da prepoznati.

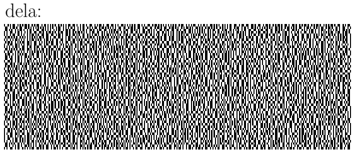
Želimo, da $t-1$ ali manj delov ne more ugotoviti nobene informacije o kvadratu.

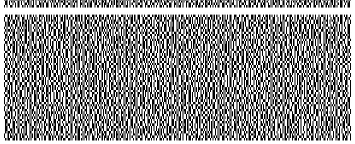
		delitev		
pixel	verjetnost	1. del	2. del	skupaj
$\square$	p=0.5			
	p=0.5			
$\blacksquare$	p=0.5			
	p=0.5			

Kvadrat (angl. piksel) P razdelimo na dva pravokotnika (dva dela), glej zgoraj.

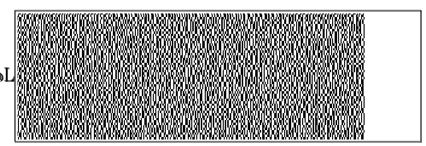
Varnost je zagotovljena, **kontrast**, tj. razmerje med črnim in belim, pa je 50%

Dva dela:





bL



Žal poskus, da bi dela sestavil skupaj ni uspel, tako da je potrebno res izpisati prejšnjo prosojnico in naložiti en del čez drugega (vendar pa se lahko zgodi, da vročina pri izpisu deformira prosojnice).

Za opis splošne sheme bomo uporabili binarni matriki M_0 in M_1 dimenzije $n \times m$.

Za vsak kvadrat P, naredimo naslednje korake.

1. Generiraj naključno permutacijo π množice $\{1,\dots,m\}$.
2. Če je P črn kvadrat, potem uporabi permutacijo π nad stolpci matrike M_1, sicer nad stolpci matrike M_0. Dobljeno matriko označimo s T_P.
3. Za $1 \le i \le n$, naj se i-ta vrstica matrike T_P sestoji iz m pravokotnikov kvadrata P v i-tem delu.

Primeri baznih matrik:

1. $(2,2)$-VTS z $m=2$ in $\gamma=1/2$

$$M_0 = \begin{pmatrix}1&0\\1&0\end{pmatrix}, \quad \text{in} \quad M_1 = \begin{pmatrix}1&0\\0&1\end{pmatrix}$$

2. $(2,3)$-VTS z $m=3$ in $\gamma=1/3$

$$M_0 = \begin{pmatrix}1&0&0\\1&0&0\\1&0&0\end{pmatrix}, \quad \text{in} \quad M_1 = \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$$

3. $(2,4)$-VTS z $m = 6$ in $\gamma = 1/3$

$$M_0 = \begin{pmatrix} 1&1&1&0&0&0\\ 1&1&1&0&0&0\\ 1&1&1&0&0&0\\ 1&1&1&0&0&0 \end{pmatrix}$$

in

$$M_1 = \begin{pmatrix} 1&1&1&0&0&0\\ 1&0&0&1&1&0\\ 0&1&0&1&0&1\\ 1&1&1&0&1&1 \end{pmatrix}.$$

4. $(3,3)$-VTS z $m = 4$ in $\gamma = 1/4$

$$M_0 = \begin{pmatrix} 0&1&1&0\\ 0&1&0&1\\ 0&0&1&1 \end{pmatrix}$$

in

$$M_1 = \begin{pmatrix} 0&0&1&1\\ 0&1&0&1\\ 1&0&0&1 \end{pmatrix}.$$

Sedaj vas gotovo že zanima kakšne lastnosti morata imeti matriki M_0 in M_1. Predno se poglobimo v to, si oglejmo še enkripcijo v primeru $(2,3)$-sheme.

V splošnem imamo $m!$ permutacij elementov množice $\{1,\dots,m\}$. V primeru $m = 3$ jih imamo torej 6:

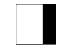
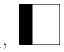
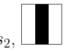
$$\pi_1 = (1,2,3),\quad \pi_2 = (1,3,2),\quad \pi_3 = (2,1,3),$$
$$\pi_4 = (2,3,1),\quad \pi_5 = (3,1,2),\quad \pi_6 = (3,2,1).$$

Naključno permutacijo lahko izberemo na primer z metanjem kocke.

Če hočemo zašifrirati črn kvadrat P in pade 4
konstruiramo N_P tako, da vzamemo zapo
drugi, tretji in prvi stoplec matrike M_1:

$$N_1 = \begin{pmatrix} 0&0&1\\ 1&0&0\\ 0&1&0 \end{pmatrix}.$$

Dobimo:

 za del s_1,  za del s_2,  za d

Naj bo sta x in y dva binarna vektorja in
število enic v x, booleanski ali nad vektorjem
pa označimo z x **or** y.

Binarni matriki M_0 in M_1 dimenzije $n \times m$, $n \le n$ sta **bazni matriki** za (t,n)-VTS (angl. visual threshold scheme) z

- m-kratno *ekspanzijo kvadrata* in
- relativnim *kontrastom* γ,

kadar za vsako podmnožico $\{i_1,\dots,i_p\} \subseteq \{1,\dots,n\}$, kjer je $p \le t$, velja

1. za $p = t$ je razlika velikosti nosilcev booleanskega ali vrstic $i_1,\dots,i_p$ matrik M_1 in M_0 vsaj γm,
2. za $p \le t-1$ sta matriki M_0 in M_1 omejeni na vrstice $i_1,\dots,i_p$, enaki do permutacije stolpcev.

Izrek (Naor in Shamir): *Za $n \in \mathbb{N}\backslash\{1\}$ obstaja (n,n)-VTS z $m = 2^{n-1}$ in $\gamma = 2^{1-m}$.*

Skica dokaz: Matriki M_0 in M_1 naj se zaporedoma sestojita iz vseh binarnih n-teric, ki vsebujejo sodo število enic in liho število enic. ■

Izrek (Blundo, De Santis in Stinson): *V vsaki popolni $(2,n)$-VTS velja*

$$\gamma \le \gamma^*(n) := \frac{\lfloor \frac{n}{2} \rfloor \lceil \frac{n}{2} \rceil}{n(n-1)}.$$

Ideja: Definirajmo

$$T = \{(i,j,c) \mid M_1(i,c) = 1,\ M_1(j,c) = 1\}.$$

Potem je

$$n(n-1)\gamma m \le |T| \le m \lfloor \frac{n}{2} \rfloor \lceil \frac{n}{2} \rceil. \quad ■$$

Konstrukcija $(2,n)$-VTS iz 2-(n,k,λ) designa

Spomnimo se, da je število blokov designa $\mathcal{D}$

$$nr/k = \lambda(n^2-n)/(k^2-k).$$

Naj bo M_1 incidenčna matrika designa $\mathcal{D}$ in M_0
dim. matrika, katere vsako vrstico sestavlja r
jim sledi $b - r$ ničel.

Naj bo $m = b$.

Poljubna vrstica matrik M_0 in M_1 vsebuje r enic, skalarni produkt poljubnih dveh vrstic matrike M_1 je enak λ. Zato ima nosilec *booleanskega ali* dveh vrstic matrike M_1 $2r - \lambda$ elementov, kontrast pa je enak

$$\gamma = \frac{2r - \lambda - r}{b} = \frac{r - \lambda}{b}.$$

Izrek *(Blundo, De Santis in Stinson)*:
Če obstaja 2-(n, k, λ)-design, potem obstaja $(2, n)$-VTS z ekspanzijo kvadrata $m = b$ in relativnim kontrastom $\gamma = (r - \lambda)/b$.

Posledica:
Če obstaja 2-$(4s-1, 2s-1, s-1)$-design, potem obstaja $(2, 4s-1)$-VTS z ekspanzijo kvadrata $m = 4s-1$ in optimalnim relativnim kontrastom $\gamma^*(4s-1) = s/(4s-1)$.

Natančen opis postopka za deljenje skrivnosti z vizualno kriptografijo, vse do konkretnega (večjega primera) in Hadamardjevih matrik, si oglejte na

`http://www.cacr.math.uwaterloo.ca/~dstinson/visual.html`

$(n \times n)$-dim. matrika H z elementi ± 1, za kat

$$HH^T = nI_n$$

imenujemo **Hadamardjeva matrika** reda

Taka matrika obstaja le, če je $n = 1$, $n = 2$ ali

Hadamardjeva matrika reda $4s$ je ekvivalentna 2-$(4s-1, 2s-1, s-1)$ designu.

Slavna **Hadamardjeva matrična dom** leta 1893 pravi, da obstaja Hadamardjeva matr $4s$ za vsak $s \in \mathbb{N}$.

Domneva je bila preverjena za vse $s \leq 107$.

$$n = 2: \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad n = 4: \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$n = 8: \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 \end{pmatrix}$$

Formalne definicije

Distribucijsko (delilno) pravilo je funkcija

$$f : \mathcal{P} \cup \{D\} \longrightarrow \mathcal{S} \cup \mathcal{K},$$

ki predstavlja eno izmed možnih razdelitev delov iz množice $\mathcal{S}$ ključa $K \in \mathcal{K}$ osebam iz $\mathcal{P}$ (oseba P_i dobi del $f(P_i)$).

Za vsak ključ $K \in \mathcal{K}$ (porazdelitev $p_{\mathcal{K}}$) naj bo $\mathcal{F}_K$ množica distribucijskih pravil, ki ustrezajo ključu K, tj. $\{f \in \mathcal{F} \mid f(D) = K\}$ (porazdelitev $p_{\mathcal{F}_K}$) in

$$\mathcal{F} = \bigcup_{K \in \mathcal{K}} \mathcal{F}_K.$$

Medtem ko so $\mathcal{F}_K$ javne, pa je delilec tisti, ki izbere za ključ $K \in \mathcal{K}$ distribucijsko pravilo $f \in \mathcal{F}_K$ ter razdeli dele.

Za $B \subseteq \mathcal{P}$ naj bo

$$\mathcal{S}(B) = \{f|_B \,:\, f \in \mathcal{F}\},$$

kjer je $\quad f|_B : B \longrightarrow \mathcal{S} \quad$ in

$$f|_B(P_i) = f(P_i) \quad \forall P_i \in B,$$

tj. množica vseh možnih distribucij delov oseb iz B.

Verjetnostno porazdelitev na $\mathcal{S}(B)$ označimo s $p_{\mathcal{S}(B)}$.

Naj bo $f_B \in \mathcal{S}(B)$. Potem za vse $f_B \in$ $K \in \mathcal{K}$ izračunamo verjetnostno porazdelitev

$$p_{\mathcal{S}(B)}(f_B) = \sum_{K \in \mathcal{K}} p_{\mathcal{K}}(K) \sum_{\{f \in \mathcal{F}_K \,:\, f|_B = f_B\}} p_{\mathcal{F}_K}$$

in

$$p_{\mathcal{S}(B)}(f_B/K) = \sum_{\{f \in \mathcal{F}_K \,:\, f|_B = f_B\}} p_{\mathcal{F}_K}(f).$$

Naj bo Γ struktura za deljenje skrivnosti in $\mathcal{F} = \bigcup_{K \in \mathcal{K}} \mathcal{F}_K$ množica distribucijskih pravil.

Potem je $\mathcal{F}$ **popolna shema za deljenje skrivnosti** *za strukturo dovoljenj, če velja*

1. *za vsako pooblaščeno množico oseb $B \subseteq \mathcal{P}$ ter poljubna distribucijska pravila $f \in \mathcal{F}_K$ in $f' \in \mathcal{F}_{K'}$, za katera je $f|_B = f'|_B$ velja $K = K'$*
2. *za vsako nepooblaščeno množico oseb $B \subseteq \mathcal{P}$ in za vsako distribucijo delov $f_B \in \mathcal{S}_B$, $p_{\mathcal{K}}(K/f_B) = p_{\mathcal{K}}(K)$ za vsak $K \in \mathcal{K}$.*

Prva lastnost pravi, da vsaka delitev delov članom poljubne pooblaščene množice B natanko določi vrednost ključa.

Druga lastnost pravi, da je distribucija pogojne verjetnosti na $\mathcal{K}$ pri dani delitvi delov f_B članom nepooblaščene množice B enaka distribuciji verjetnosti na $\mathcal{K}$.

Z drugimi besedami: člani nepooblaščene množice B nimajo nobene informacije o ključu.

Druga lastnost je zelo podobna konceptu popolne verjetnosti (od tu ime).

Verjetnost $p_{\mathcal{K}}(K/f_B)$ lahko izračunamo iz verjetnostne porazdelitve s pomočjo Bayesovega izreka:

$$p_{\mathcal{K}}(K/f_B) = \frac{p_{\mathcal{S}(B)}(f_B/K)p_{\mathcal{K}}(K)}{p_{\mathcal{S}(B)}(f_B)}$$

(glej primer 11.5, ki je povezan s primerom konjuktivne normalne forme).

Stopenjske sheme iz OA

Pravokotna škatla

$OA_\lambda(t,k,v)$ je taka $(\lambda v^t \times k)$-dimenzionalna
z v simboli, da se v vsakih t stolpcih vsaka
simbolov pojavi natanko λ-krat

(za $t = 2$ dobimo staro definicijo).

Naj bo M pravokotna škatla $OA_1(t, w+1, v)$
smo torej $\lambda = 1$) in A množica njenih simbolo

Skonstruirali bomo (t,w)-stopenjsko shemo, z
je $\mathcal{S} = \mathcal{K} = A$.

Stolpce matrike M označimo s $\mathcal{P} \cup \{D\}$, njene vrstice pa z v^t elementi množice $\mathcal{F}$. Vsaka vrstica f matrike M ustreza distribucijskemu pravilu, tj.

$$f(X) = M(f,X) \quad \text{za vsak } f \in \mathcal{F} \text{ in } X \in \mathcal{P} \cup \{D\}.$$

Potem je za vsak $K \in \mathcal{K}$:

$$\mathcal{F}_K = \{f \in \mathcal{F} \mid M(f,D) = K\}$$

in zato $|\mathcal{K}| = v^{t-1}$ za vsak $K \in \mathcal{K}$. Torej lahko za $K \in \mathcal{K}$ in $f \in \mathcal{F}$ definiramo

$$p_{\mathcal{F}_K}(f) = \frac{1}{v^{t-1}}.$$

Da bi dokazali, da je $\mathcal{F}$ popolna shema za deljenje skrivnosti, moramo preveriti lastnosti (1) in (2). Prva lastnost sledi iz definicije pravokotne škatle in $\lambda = 1$. Vrednosti katerihkoli t delov določijo vrstico matrike M in s tem natanko določen ključ.

Za drugo lastnost moramo pokazati, da za vsak $K \in \mathcal{K}$ in $f_B \in \mathcal{S}(B)$, kjer je $|B| \leq t-1$.

$$\frac{p_{\mathcal{S}(B)}(f_B/K)p_{\mathcal{K}}(K)}{p_{\mathcal{S}(B)}(f_B)} = p_{\mathcal{K}}(K)$$

oziroma $p_{\mathcal{S}(B)}(f_B/K) = p_{\mathcal{S}(B)}(f_B)$.

Naj bo $|B| = i \leq t-1$. Za vsak $K \in \mathcal{K}$ imamo natanko v^{t-i-1} distribucijskih pravil $f \in \mathcal{F}_K$, za katera je $f|_B = f_B$ (saj je $i+1$ simbolov v določenih $i+1$ stolpcih v natanko v^{t-i-1} vrsticah matrike M). Ker je $|\mathcal{F}_K| = v^{t-1}$, velja

$$p_{\mathcal{S}(B)}(f_B/K) = \frac{1}{v^i} \quad \text{za vsak } f_B \text{ in vsak } K.$$

Sedaj ni več težko izračunati za vsak $K \in \mathcal{K}$

$$p_{\mathcal{S}(B)}(f_B) = \sum_{K \in \mathcal{K}} p_{\mathcal{S}(\mathcal{B})}(f_B/K)p_{\mathcal{K}}(K)$$

$$= v^{-i} \sum_{K \in \mathcal{K}} p_{\mathcal{K}}(K) = v^{-i} = p_{\mathcal{S}(B)}(f_B/K). \blacksquare$$

Shamirjeva shema je poseben primer te konstr

Naj bodo $x_0 = 0, x_1, \ldots, x_w$ različni elementi
končnega obsega $GF(q)$.

Če za poljubno t-terico $(a_0, \ldots, a_{t-1}) \in$ (
definiramo

$$M((a_0, \ldots, a_{t-1}), i) = \sum_{j=0}^{t-1} a_j (x_i)^j,$$

dobimo ravno Shamirjevo shemo.

Ekvivalenca stopenjske sheme in OA

Sedaj pa pokažimo še obrat (da lahko iz določene stopenjske sheme skonstruiramo pravokotno škatlo).

Izrek 2. *Naj bo M matrika, katere vrstice in stolpci so označeni zaporedoma z elementi iz $\mathcal{F}$ in elementi iz $\mathcal{P} \cup \{D\}$ ter za katero je $M(f, X) = f(X)$. Potem je M pravokotna škatla $OA_1(t, w+1, v)$ z $v = |\mathcal{S}|$.*

Dokaz tega izreka razbijemo na več korakov.

Iz lastnost (2) sledi naslednji rezultat.

Lema 3. *Naj bo $\mathcal{F}$ množica distribucijskih pravil (t, w)-stopenjske sheme in $B \subseteq \mathcal{P}$, $|B| = t - 1$. Za $f \in \mathcal{F}$ in za vsak ključ $K \in \mathcal{K}$ obstaja distribucijsko pravilo $g_B \in \mathcal{F}_K$, za katerega je $g_K|_B = f|_B$.* ■

Lema 4. *Za (t, w)-stopenjsko shemo je $|\mathcal{S}| \geq |\mathcal{K}$.*

Dokaz: Naj bo $P \in \mathcal{P} \backslash \{B\}$, kjer je $B \subseteq \mathcal{P}$ in $|B| = t - 1$. Iz lastnosti (1) sledi $g_K(P) = g_{K'}(P)$ za $K \neq K'$, kjer smo g definirali v prejšnji lemi.

Potem je funkcija

$$\theta : \mathcal{K} \longrightarrow \mathcal{S}, \quad \text{s pravilom} \quad \theta(K) = g_K(P)$$

injektivna in trditev sledi. ■

Odslej privzemimo $|\mathcal{S}| = |\mathcal{K}|$, se pravi, da je θ bijekcija (in lahko privzamemo kar $\mathcal{S} = \mathcal{K}$) sledi:

Lema 5. *Naj bo $\mathcal{F}$ množica distribucijski (t, w)-stopenjske sheme z $|\mathcal{S}| = |\mathcal{K}|$. Naj bo $B \subseteq \mathcal{P}$ in $|B| = t - 1$. Če je $f, g \in$ nek ključ K in je $f|_B = g|_B$, potem je $f =$*

Posledica 6. *V poljubnih t stolpcih matrike M se pojavi vsaka t-terica v največ eni vrstici.*

Dokaz: Naj bo $C \subseteq \mathcal{P} \cup \{D\}$, $|C| = t$.

Če je $D \in C$, potem rezultat sledi iz Leme 5.

Sedaj pa naj bo $C \subseteq \mathcal{P}$ in $f|_C = g|_C$.
Ker je $|C| = t$ iz lastnosti (1) sledi $f(D) = g(D)$.
Naj bo $C' = C \cup \{D\} \backslash \{X\}$ za nek $X \in C$.
Iz prvega primera sledi $f = g$. ■

Lema 7. *Če je $1 \leq i \leq t$, potem se v poljubnih i-tih stolpcih matrike M vsaka i-terica elementov pojavi vsaj v eni vrstici.*

Dokaz: Naj bo $C \subseteq \mathcal{P}$, $|C| = i$. Dokazovali bomo z indukcijo na i. Če je $i = 1$, vzemimo $C = \{P\}$. Naj bo $B \subseteq \mathcal{P}$, $|B| = t - 1$ in $B \cap C = \emptyset$. Potem uporabimo Lemo 4.

Sedaj pa naj bo $i \leq 2$. Ločimo dva primera glede na to ali je $D \in C$. Če je $C \subseteq \mathcal{P}$. Potem je $P \in C$ in $C' \subseteq \mathcal{P}$, kjer je $|C'| = t - i$ in $C \cap C' = \emptyset$.

Po indukcijski predpostavki je vsaka $(i-1)$-terica v stolpcih iz $C'' = C \backslash \{P\}$. Uporabimo Lemo 4 na $B = C' \cup C''$.

V drugem primeru, ko je $D \in C$ postopamo podobno: naj bo $C' \subset \mathcal{P}$, kjer je $|C'| = t - i$ in $C \cap C' = \emptyset$. Po indukcijski predpostavki se vsaka $(i-1)$-terica pojavi v stolpcih iz $C'' = C \backslash \{D\}$. Končno uporabimo Lemo 2 za $B = C' \cup C''$. ■

Izrek 2 sedaj sledi iz Posledice 6 in Leme 7.

Informacijska mera

Radi bi ocenili učinkovitost dobljenih shem.

Informacijska mera za osebo P_i je

$$\rho_i = \log_2 |\mathcal{K}| / \log_2 |\mathcal{S}(P_i)|,$$

kjer so $\mathcal{S}(P_i)$ možni deli za osebo P_i.

Informacijska mera sheme pa je

$$\rho = \max_{1 \leq i \leq n} \rho_i.$$

Izrek 8. *Naj bo* **C** *monotono vezje. Potem obstaja popolna shema za deljenje skivnosti, ki realizira strukturo dovoljenj* $\Gamma(\mathbf{C})$ *z informacijsko mero*

$$\rho = \max\{1/r_i \mid 1 \leq i \leq n\},$$

kjer r_i *označuje število vhodnih žic vezja* **C** *z delom* x_i*.*

Izrek 9. *Za vsako popolno shemo za deljenje skrivnosti, ki realizira strukturo dovoljenj* Γ*, je* $\rho \leq 1$*.*

Če velja enačaj, pravimo, da je shema **idealna**. Brickellova konstrukcija z vektorskim prostorom nam da idealno shemo (to in dokaze zgornjih izrekov izpustimo).