Capitolul 4

Sisteme de partajare a secretelor

Vom începe cu două exemple simple:

- Într-o bancă, seiful trebuie deschis în fiecare zi. Banca are trei directori, dar nu încredinţează combinaţia seifului nici unuia din ei. Ea doreşte să dispună de un sistem de acces prin care orice asociere de doi directori să poată deschide seiful, dar acest lucru să fie imposibil pentru unul singur.

- Conform revistei *Time Magazin* (4 mai 1992), în Rusia, accesul la arma nucleară utilizează un sistem *doi - din - trei* similar. Cele trei persoane sunt Preşedintele ţării, Preşedintele Parlamentului şi Ministrul Apărării.

Vom face o primă formalizare:
Fiind dat un secret S, se cere împărţirea lui la n participanţi ($n \geq 2$), astfel încât:

1. Cel puţin k din cei n participanţi pot regăsi S prin combinarea informaţiile lor;

2. Nici o asociere de mai puţin de k participanţi nu pot recompune S.

Acest lucru se poate realiza prin *partajarea* secretului S în n componente ("shares" în engleză) $S_1, S_2, \ldots, S_n$ şi distribuirea câte unei componente fiecărui participant.

Intuitiv, un sistem de partajare a secretelor este deci o metodă de spargere a unui secret în componente, astfel încât acesta să poată fi recompus numai de către *grupurile autorizate* (grupuri care au dreptul să refacă secretul).

În funcţie de "cantitatea" de informaţie secretă pe care o pot obţine grupurile neautorizate, sistemele de partajare a secretelor se clasifică în

- *Sisteme perfecte* de partajare: componentele deţinute de grupurile neautorizate nu oferă nici o informaţie (în sensul teooretic al termenului) despre secretul S;

- *Sisteme computaţional - sigure* de partajare: grupurile neautorizate au acces la o anumită cantitate de informaţie relativă la S, dar problema aflării secretului plecând de la această informaţie formează o problemă $\mathcal{NP}$ - completă.

Literatura de specialitate abundă în prezentarea de sisteme de partajare a secretelor. Acest capitol face o trecere în revistă a celor mai importante sisteme şi abordări legate de subiectul propus.

Vom începe cu o clasă de sisteme/scheme de partajare a secretelor, numite *sisteme majoritare*.[1]

4.1 Scheme de partajare majoritară

Definiţia 4.1. *Fie k, n $(2 \leq k \leq n)$ două numere întregi.*
O schemă de partajare (n, k) - majoritară este o metodă de partajare a unui secret S între membrii unei mulţimi $\mathcal{P}= \{P_1, \ldots, P_n\}$ de participanţi, astfel încât orice asociere de k participanţi să poată calcula S, lucru imposibil pentru asocieri de $k-1$ sau mai puţini participanţi.

Exemplele date la începutul acestui capitol sunt sistem $(3, 2)$ - majoritare.

Să formalizăm puţin aceste noţiuni:

Definiţia 4.2. *Se numeşte* **structură de acces** $\mathcal{A}\subseteq 2^{\mathcal{P}}$ *mulţimea*[2] *tuturor grupurilor "autorizate", care dispun de informaţia legală necesară construirii sistemului.*

Celelalte grupuri sunt numite "grupuri neautorizate".

Fie $B \in \mathcal{A}$ şi $B \subseteq C \subseteq \mathcal{P}$. Dacă mulţimea de participanţi C caută să determine secretul S, ea va reuşi lucrând numai cu participanţii din B şi ignorând participanţii din $C \setminus B$. Altfel spus, structura de acces $\mathcal{A}$ satisface condiţia de monotonie:

$$\text{Dacă } B \in \mathcal{A} \text{ şi } B \subseteq C \subseteq \mathcal{P}, \text{ atunci } C \in \mathcal{A}.$$

Vom presupune că orice structură de acces este *monotonă*.

Definiţia 4.3. *Fie $2 \leq k \leq n$. Structura*

$$\mathcal{A}= \{A \in 2^{\mathcal{P}} \mid card(A) \geq k\}$$

se numeşte structură de acces (n, k) **- majoritară***.*

Deci o schemă de partajare (n, k) - majoritară este o structură monotonă de acces (n, k) - majoritară.

Un element $B \in \mathcal{A}$ este *minimal* dacă

$$(\forall A \in \mathcal{P})[A \subset B \quad \Longrightarrow \quad A \notin \mathcal{A}]$$

Vom nota cu $\mathcal{A}_{min}$ mulţimea elementelor minimale autorizate din $\mathcal{A}$.

[1] *Threshold scheme* în engleză, *a seuil* în franceză.
[2] S-a notat cu $2^{\mathcal{P}}$ mulţimea tuturor submulţimilor lui $\mathcal{P}$.

Se observă că această mulţime – numită şi ”bază autorizată de acces” – caracterizează complet $\mathcal{A}$. Mai exact,

$$\mathcal{A} = \{C \subseteq \mathcal{P} \mid \exists B \in \mathcal{A}_{min},\ B \subseteq C\}.$$

Spunem că $\mathcal{A}$ este *închiderea* lui $\mathcal{A}_{min}$ şi notăm prin $\mathcal{A}= \overline{\mathcal{A}_{min}}$.

Exemplul 4.1. *Fie* $\mathcal{P}= \{P_1, P_2, P_3, P_4\}$ *şi* $\mathcal{A}_{min} = \{\{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3\}\}$. *Vom avea*

$\mathcal{A}= \{\{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3\}, \{P_1, P_2, P_3\}, \{P_2, P_3, P_4\}, \{P_1, P_2, P_3, P_4\}\}$.

Invers, fiind dat $\mathcal{A}$*, se vede imediat că* $\mathcal{A}_{min}$ *este mulţimea părţilor sale minimale.*

Referitor la grupurile neautorizate de participanţi, este evident că dacă o mulţime $B \subseteq \mathcal{P}$ este neautorizată, orice submulţime a sa va fi de asemenea neautorizată.
Deci se va lua ca bază de lucru mulţimea grupurilor maximale neautorizate.

Definiţia 4.4. *O mulţime* $B \in 2^{\mathcal{P}} \backslash \mathcal{A}$ *este maximal neautorizată dacă*

$$(\forall C \in 2^{\mathcal{P}})\ [B \subset C \quad \Longrightarrow \quad C \in \mathcal{A}].$$

Vom nota cu $\mathcal{NA}_{max}$ mulţimea mulţimilor maximale neautorizate. Atunci o structură de acces neautorizată $\mathcal{NA}= 2^{\mathcal{P}} \backslash \mathcal{A}$ va fi definită prin

$$\mathcal{NA} = \left\{A \in 2^{\mathcal{P}} \mid (\exists B \in \mathcal{NA}_{max})\ (A \subseteq B)\right\}$$

Exemplul 4.2. *Fie* $n = 4$ *şi structura de acces*
$\mathcal{A}= \{\{P_1, P_2\}, \{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_1, P_2, P_3, P_4\}, \{P_3, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3, P_4\}\}$.

Atunci:

$\mathcal{A}_{min} = \{\{P_1, P_2\}, \{P_3, P_4\}\}$,
$\mathcal{NA}_{max} = \{\{P_1, P_3\}, \{P_1, P_4\}, \{P_2, P_3\}, \{P_2, P_4\}\}$,
$\mathcal{NA}= \{\emptyset, \{P_1\}, \{P_2\}, \{P_3\}, \{P_4\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_2, P_3\}, \{P_2, P_4\}\}$.

Vom nota cu S_i componenta din secretul S, cunoscută de participantul P_i.

Valoarea lui S este aleasă de un *arbitru* $D \notin \mathcal{P}$. D va distribui – printr-un canal securizat – componentele $S_1, \ldots S_n$ (ale secretului) membrilor grupului $\mathcal{P}$, astfel încât nici un participant P_i să nu cunoască componentele celorlalţi şi nici să fie capabil ca din S_i să poată recompune secretul S.

Ulterior, participanţii unei submulţimi $B \subseteq \mathcal{P}$ pot pune în comun componentele cunoscute de ei (sau să le dea unei autorităţi în care au încredere) cu scopul de a determina S. Ei trebuie să poată reuşi în această tentativă dacă şi numai dacă $card(B) \geq k$.

Să notăm cu $\mathcal{K}$ spaţiul tuturor secretelor posibile S şi cu $\mathcal{S}$ spaţiul componentelor (toate componentele S_i posibile ale unui secret S).

4.1.1 Schema lui Blakely

Propusă în 1979 ([7]), aceasta este – istoric – prima schemă de partajare a secretelor.

Fie q un număr prim, k şi n numere întregi pozitive ($k \le n$) şi $\mathcal{K}= Z_q^k$, $\mathcal{S}= Z_q^{k+1}$. Dacă $S = (a_1, a_2, \ldots, a_k)$ este un secret, atunci schema lui Blakely este:

1. D alege $\alpha_{ij}, \beta_i \in Z_q$ $(1 \le i \le n,\ 1 \le j \le k)$ astfel ca

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1k} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2k} \\ & & \vdots & \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nk} \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} \quad (mod\ q)$$

iar matricea $\begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1k} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2k} \\ & & \vdots & \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nk} \end{pmatrix}$ să aibă rangul k.

2. Trimite fiecărui participant P_i componenta $S_i = (\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{ik}, \beta_i)$

Schema este o structură de acces (n, k) - majoritară deoarece:

- Fiecare participant P_i va construi – din componenta sa – ecuaţia diofantică

$$\alpha_{i1}x_1 + \ldots + \alpha_{ik}x_k = \beta_i \quad (mod\ q)$$

  care are printre soluţiile sale şi secretul $S = (a_1, \ldots, a_k)$.

- Orice grup de k parteneri va putea recompune secretul S rezolvând un sistem format din cele k ecuaţii liniare puse în comun.

Exemplul 4.3. *Fie $q = 31$ şi să considerăm o schemă $(3, 2)$ - majoritară, unde componentele participanţilor P_1, P_2, P_3 sunt:*

$$S_1 = (4, 29, 8),\ S_2 = (2, 1, 8),\ S_3 = (3, 27, 1)$$

Nici unul din participanţi nu poate afla singur secretul $S = (x, y) \in Z_{31} \times Z_{31}$.

Dacă se aliază însă P_1 cu P_3, ei au de rezolvat – în Z_{31} – sistemul liniar

$$\begin{cases} 4x + 29y = 8 \\ 3x + 27y = 1 \end{cases}$$

care are soluţia (unică) $S = (3, 2)$.

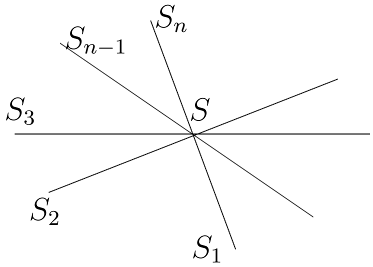
La acelaşi rezultat ajunge şi o alianţă P_1 cu P_2, P_2 cu P_3 sau P_1 cu P_2 şi P_3. Structura de acces este deci

$$\mathcal{A} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_2, P_3\}, \{P_1, P_2, P_3\}\},$$

o structură $(3, 2)$ *- majoritară.*

Schema lui Blakely are şi o interpretare geometrică. Fiecare participant deţine ecuaţia unui hiperplan $(k-1)$ - dimensional, cu proprietatea că printre cele n hiperplanuri nu sunt două paralele. Intersecţia oricăror k astfel de hiperplanuri este un singur punct – totdeauna acelaşi – care constituie secretul S.

Figura următoare descrie cazul $k = 2$.



Schema lui Blakely nu constituie un sistem perfect, deoarece orice grup neautorizat ştie că secretul se află undeva la intersecţia hiperplanelor deţinute de membrii săi; deci grupul posedă o anumită cantitate de informaţie suplimentară, ceea ce reduce dimensiunea acestor hiperplane.

O securitate perfectă se atinge atunci când secretul S este numai una din coordonatele $a \in Z_q$ ale soluţiei $(a_1, \ldots, a_k)$.

4.1.2 Schema lui Shamir

Fie q $(q \geq n+1)$ un număr prim şi $\mathcal{K} = Z_q$, $\mathcal{S} = Z_q$. Schema lui Shamir ([73]), definită în 1979, se bazează pe un polinom generat aleator $a(X)$ de grad cel mult $k-1$, în care termenul liber este S. Fiecare participant P_i cunoaşte un punct (x_i, y_i) de pe graficul acestui polinom.

1. D alege n elemente distincte $x_1, \ldots, x_n \in Z_q$ (x_i publice), fiecare x_i fiind comunicat lui P_i.
2. Dacă D intenţionează să repartizeze secretul $S \in Z_q$, el va genera $k-1$ elemente aleatoare $a_1, \ldots, a_{k-1} \in Z_q$ şi va construi polinomul
$$a(X) = S + \sum_{j=1}^{k-1} a_j X^j \quad (mod\ q).$$
3. D calculează $y_i = a(x_i)$ şi comunică această valoare lui P_i $(1 \leq i \leq n)$.

Fie acum o submulţime $\{P_{i_1}, \ldots, P_{i_k}\}$ de participanţi care doresc să reconstituie secretul. Ei ştiu valorile x_{i_j} şi $y_{i_j} = a(x_{i_j})$ pentru $1 \le j \le k$; $a(X) \in Z_q[X]$ este polinomul (secret) folosit de D. Cum gradul lui este cel mult $k-1$, putem scrie

$$a(X) = a_0 + a_1X + \ldots + a_{k-1}X^{k-1}$$

unde $a_0, \ldots, a_{k-1} \in Z_q$ sunt necunoscute. Ele se află rezolvând sistemul liniar de k ecuaţii $y_{i_j} = a(x_{i_j}),\ \ 1 \le j \le k$.
Dacă ecuaţiile sunt independente, soluţia este unică, iar valoarea lui a_0 este chiar secretul S.

Exemplul 4.4. *Să presupunem* $q = 17,\ k = 3,\ n = 5$ *şi* $x_i = i\ (1 \le i \le 5)$.
Dacă mulţimea $B = \{P_1, P_3, P_5\}$ *de participanţi vrea să afle secretul, fiecare participant aducând informaţiile* $8,\ 10$ *şi respectiv* 11, *ei vor scrie polinomul general* $a(X) = a_0 + a_1X + a_2X^2$ *şi vor reduce problema la rezolvarea în* Z_{17} *a sistemului liniar*

$$\left\{\begin{array}{rcrcl} a(1) & = & a_0 + a_1 + a_2 & = & 8 \\ a(3) & = & a_0 + 3a_1 + 9a_2 & = & 10 \\ a(5) & = & a_0 + 5a_1 + 8a_2 & = & 11 \end{array}\right.$$

Acesta admite soluţia unică în $Z_{17}:\quad a_0 = 13,\ a_1 = 10,\ a_2 = 2.$
Deci valoarea căutată este $S = 13$.

Teorema 4.1. *În schema de partajare Shamir, orice mulţime* B *de* k *participanţi poate reconstitui în mod unic secretul* S.

Demonstraţie. Fie $a(X) = a_0 + a_1X + \ldots + a_{k-1}X^{k-1}$ polinomul ales de D, unde $a_0 = S$. Afirmaţia se reduce la a arăta că sistemul de ecuaţii $y_{i_j} = a(x_{i_j})\quad (1 \le j \le k)$, de necunoscute $a_0, \ldots, a_{k-1}$, admite soluţie unică.
Determinantul acestui sistem este

$$\left|\begin{array}{ccccc} 1 & x_{i_1} & x_{i_1}^2 & \ldots & x_{i_1}^{k-1} \\ 1 & x_{i_2} & x_{2_1}^2 & \ldots & x_{i_2}^{k-1} \\ & & \ldots & & \\ 1 & x_{i_k} & x_{i_k}^2 & \ldots & x_{i_k}^{k-1} \end{array}\right| = \prod_{1 \le j < t \le k} (x_{i_t} - x_{i_j}) \quad (mod\ q)$$

Deoarece toate numerele x_i sunt distincte, iar Z_q este corp, rezultă că acest produs este nenul, deci sistemul are totdeauna soluţie unică, iar a_0 este chiar secretul căutat. $\square$

Ce se întâmplă dacă un grup de $k-1$ participanţi încearcă să calculeze secretul S ?

Dacă procedează conform algoritmului anterior, vor obţine un sistem de $k-1$ ecuaţii cu k necunoscute. Fie y_0 o valoare arbitrară a lui S. Vom avea $y_0 = a_0 = a(0)$, care formează încă o ecuaţie a sistemului (în total sunt acum k ecuaţii). Acesta va avea de asemenea o soluţie unică.

Deci, pentru orice valoare $S \in Z_q$ există un polinom unic $a_S(X) \in Z_q[X]$ care verifică toate condiţiile:

$$y_0 = a_S(0), \qquad y_{i_j} = a_S(x_{i_j}), \quad 1 \le j \le k-1.$$

Rezultă că orice valoare a lui S este consistentă cu componentele deţinute de cei $k-1$ participanţi; asocierea lor nu oferă nici o informaţie suplimentară pentru aflarea secretului. Avem deci o structură de acces (n, k) - majoritară.

Mai există o modalitate de abordare a sistemului Shamir: folosind polinoamele de interpolare Lagrance.

În această interpretare, construcţia schemei de partajare (n, k) - majoritară este:

1. Se alege un număr prim $q > max\{S, n\}$.
2. Se defineşte polinomul
$$a(X) = a_{k-1}X^{k-1} + \ldots + a_1X + a_0 \in Z_q[X]$$
cu $a_0 = S$ şi a_i $(1 \le i \le k-1)$ arbitrari în Z_q.
3. Se determină componentele
$$S_i = a(x_i), \quad 1 \le i \le n$$
unde $x_1, x_2, \ldots, x_n \in Z_q$ sunt valori publice arbitrare, distincte două câte două. Aceste componente se trimit celor n participanţi.

Având componentele S_{i_j} $(1 \le j \le k)$ ale unui grup de acces, secretul S se poate obţine folosind formula de interpolare Lagrance. Fie polinomul

$$P(X) = \sum_{j=1}^{k} S_{i_j} \prod_{\substack{1 \le t \le k \\ t \ne j}} \frac{X - x_{i_t}}{x_{i_j} - x_{i_t}}.$$

Evident, acesta este un polinom de grad cel mult $k-1$, cu proprietatea $S_{i_j} = P(x_{i_j}),\ j = 1, \ldots, k$.

Cum un astfel de polinom este unic, rezultă că el este chiar polinomul $a(X)$.

Un grup B de k participanţi poate calcula $a(X)$ pe baza acestei formule. De fapt, nici nu este nevoie se determine tot polinomul: este suficient să obţină $S = a(0)$.

Deci, înlocuind în formulă pe X cu 0, avem

$$S = \sum_{j=1}^{k} S_{i_j} \prod_{\substack{1 \le t \le k \\ t \neq j}} \frac{x_{i_t}}{x_{i_t} - x_{i_j}}.$$

Dacă definim

$$b_j = \prod_{\substack{1 \le t \le k \\ t \neq j}} \frac{x_{i_t}}{x_{i_t} - x_{i_j}}, \qquad 1 \le j \le k$$

aceste valori pot fi precalculate şi făcute publice de către arbitru.

Secretul este atunci o combinaţie liniară de k componente:

$$S = \sum_{j=1}^{k} b_j S_{i_j}.$$

Exemplul 4.5. *Să considerăm o schemă de partajare Shamir* $(3,2)$ *- majoritară.*

Fie $q = 31,\ x_1 = 20,\ x_2 = 6,\ x_3 = 11$ *componentele publice.*

Componentele secrete sunt $S_1 = 12,\ S_2 = 25$ *şi* $S_3 = 27$*.*

Să presupunem că mulţimea autorizată $\{P_2, P_3\}$ *doreşte să afle secretul* S*. Ea va calcula*

$$S = S_2 \cdot \frac{x_3}{x_3 - x_2} + S_3 \cdot \frac{x_2}{x_2 - x_3} = \frac{25 \cdot 11 - 27 \cdot 6}{5} = 20 \cdot 25 = 4 \quad (mod\, 31)$$

La acelaşi rezultat se ajunge dacă se rezolvă în $Z_{31} \times Z_{31}$ *sistemul de ecuaţii liniare*

$$\begin{cases} 6a_1 + a_0 = 25 \\ 11a_1 + a_0 = 27 \end{cases}$$

cu soluţia $a_1 = 19,\ a_0 = 4$*.*

În subsidiar, se observă că sistemul Shamir a lucrat cu polinomul de interpolare $a(X) = 19X + 4$*. Într-adevăr,*

$S_1 = a(x_1) = a(20) = 12\ (mod\, 31)$,

$S_2 = a(x_2) = a(6) = 25\ (mod\, 31)$,

$S_3 = a(x_3) = a(11) = 27\ (mod\, 31)$.

Exemplul 4.6. *Să considerăm* $q = 11,\ n = 5$ *şi* $k = 3$*.*

Fie polinomul $a(X) = 2X^2 + 7X + 10 \in Z_{11}[X]$*.*

Secretul este $S = 10$*, iar componentele se calculează imediat (în* Z_{11}*):*

$S_1 = a(1) = 8,\ S_2 = a(2) = 10,\ S_3 = a(3) = 5,\ S_4 = a(4) = 4,\ S_5 = a(5) = 7.$

Pentru o mulţime autorizată $\{P_1, P_2, P_4\}$*, secretul poate fi reconstruit cu*

$$8 \cdot \frac{2}{2-1} \cdot \frac{4}{4-1} + 10 \cdot \frac{1}{1-2} \cdot \frac{4}{4-2} + 4 \cdot \frac{1}{1-4} \cdot \frac{2}{2-4}$$

Teorema 4.2. *Schema de partajare Shamir este perfectă.*

Demonstraţie. Dacă avem numai $k-1$ componente, sistemul de $k-1$ ecuaţii

$$\begin{cases} a_{k-1}x_{i_1}^{k-1} + \ldots + a_1 x_{i_1} & = & S_{i_1} - a_0 \\ a_{k-1}x_{i_2}^{k-1} + \ldots + a_1 x_{i_2} & = & S_{i_2} - a_0 \\ & \vdots & \\ a_{k-1}x_{i_{k-1}}^{k-1} + \ldots + a_1 x_{i_{k-1}} & = & S_{i_{k-1}} - a_0 \end{cases}$$

având necunoscutele $(a_{k-1}, \ldots, a_1)$ are soluţie unică pentru fiecare a_0. Deci este posibilă orice valoare a secretului S. □

Lema 4.1. *Dacă informaţia grad*$(a(X)) = k-1 > 0$ *este publică, atunci schema lui Shamir nu este perfectă.*

Demonstraţie. În acest caz, orice grup de $k-1$ utilizatori poate determina un element b_0, care în mod cert nu este a_0 (deci domeniul de valori $\mathcal{K}$ al secretului se micşorează).
Mai exact, folosind formula de interpolare Lagrance, se poate determina un polinom

$$Q(X) = b_{k-2}X^{k-2} + \ldots + b_1 X + b_0$$

cu proprietatea $Q(x_{i_j}) = S_{i_j} = a(x_{i_j})$ $(1 \le j \le k-1)$, care conduce la sistemul

$$\begin{cases} a_{k-1}x_{i_1}^{k-1} + (a_{k-2} - b_{k-2})x_{i_1}^{k-2} + \ldots + (a_1 - b_1)x_1 + (a_0 - b_0) & = & 0 \\ & \vdots & \\ a_{k-1}x_{i_{k-1}}^{k-1} + (a_{k-2} - b_{k-2})x_{i_{k-1}}^{k-2} + \ldots + (a_1 - b_1)x_{k-1} + (a_0 - b_0) & = & 0 \end{cases}$$

Dacă presupunem $a_0 = b_0$, acest sistem de $k-1$ ecuaţii cu $k-1$ necunoscute $(a_{k-1}, \ldots, a_1)$ va avea soluţie unică:

$$a_{k-1} = 0, \quad a_{k-2} = b_{k-2}, \quad \ldots, \quad a_1 = b_1,$$

ceea ce contrazice presupunerea $a_{k-1} \neq 0$.

În concluzie, orice grup de $k-1$ participanţi poate determina un element b_0 care nu este secret; deci gradul lor de incertitudine nu va coincide cu cel de incertitudine al unui atacator extern. □

Observaţia 4.1.

1. *Mărimea fiecărei componente S_i nu depăşeşte mărimea secretului S (schema este "ideală").*

2. *Pentru o valoare fixată a lui k se pot adăuga sau elimina dinamic componente S_i (de exemplu, prin venirea sau ieşirea din sistem a noi participanţi) fără a afecta celelalte componente.*

3. *Componentele S_i pot fi modificate fără a schimba secretul S: singura schimbare constă în alegerea unui nou polinom $a(X)$ având S ca termen liber. Acest lucru se recomandă a se efectua periodic, pentru a păstra nivelul de securitate al sistemului.*

4. *McElliece şi Sarwate ([56]) au remarcat că schema Shamir are multe similitudini cu codurile Reed - Solomon; deci algoritmii de decodificare construiţi pentru aceste coduri pot fi utilizaţi pentru generalizarea schemei de partajare Shamir.*

Pentru cazul $n = k$ se poate construi o variantă simplificată a algoritmului Shamir. Ea funcţionează pentru $\mathcal{K}= Z_m$, $\mathcal{S}= Z_m$ (m nu este obligatoriu număr prim şi – chiar mai mult – este posibil ca $m \le n$). Noul algoritm este:

1. D alege aleator $n-1$ elemente $y_1, \ldots, y_{n-1} \in Z_m$;
2. D calculează $y_n = S - \sum_{i=1}^{n-1} y_i \pmod{m}$;
3. Fiecare element y_i este transmis (prin canal securizat) lui P_i, $i = 1, \ldots, n$.

Cei n participanţi pot determina secretul S pe baza formulei

$$S = \sum_{i=1}^{n} y_i \pmod{m}.$$

Evident, $n-1$ participanţi nu-l pot obţine pe S. Chiar dacă pun în comun componentele lor, ei pot determina valoarea $S - y$, unde y este componenta celui care lipseşte. Cum y este o valoare aleatoare din Z_m, nu se va obţine nici o informaţie suplimentară referitoare la secret. Acesta este deci o structură de acces (n, n) - majoritară.

4.1.3 Schema Mignotte

Schema de partajare (n, k) - majoritară a lui Mignotte ([59]) se bazează pe secvenţe de numere întregi numite *şiruri Mignotte.*

Definiţia 4.5. *Fie n ($n \ge 2$) un număr întreg şi $2 \le k \le n$. Un şir (n, k) - Mignotte este o secvenţă de numere întregi pozitive $p_1 < p_2 < \ldots < p_n$ prime două câte două, cu proprietatea*

$$\prod_{i=0}^{k-2} p_{n-i} < \prod_{i=1}^{k} p_i.$$

Această relaţie este echivalentă cu

$$\max_{1 \le i_1 < \ldots < i_{k-1} \le n} (p_{i_1} \ldots p_{i_{k-1}}) < \min_{1 \le i_1 < \ldots < i_k \le n} (p_{i_1} \ldots p_{i_k})$$

Exemplul 4.7. *Şirul*

$$5, 7, 9, 11, 13$$

formează o secvenţă $(5, 3)$ *- Mignotte. Cele cinci numere sunt prime (deci şi prime între ele), iar inegalitatea din Definiţia 4.5 este* $p_4 \cdot p_5 < p_1 \cdot p_2 \cdot p_3$*, verificată evident.*

Schema de partajare (n, k) - majoritară Mignote se defineşte astfel:

1. D alege un şir (n, k) - Mignotte şi calculează
$$\alpha = \prod_{i=1}^{k} p_i, \qquad \beta = \prod_{i=0}^{k-2} p_{n-i}.$$
2. D alege $S \in (\beta, \alpha)$ (în general, S este generat aleator).
3. D calculează $S_i = S \ (mod\ p_i)$ şi trimite fiecărui utilizator P_i perechea $(p_i, S_i), \quad i = 1, \ldots, n$.

Fiind cunoscute k componente distincte $S_{i_1}, \ldots, S_{i_k}$, secretul S poate fi aflat pe baza Teoremei Chineze a Restului (TCR), fiind soluţia unică modulo $p_{i_1} p_{i_2} \ldots p_{i_k}$ a sistemului de congruenţe

$$\begin{cases} x \equiv S_{i_1} \quad (mod\ p_{i_1}) \\ \quad \vdots \\ x \equiv S_{i_k} \quad (mod\ p_{i_k}) \end{cases}$$

Pentru a asigura un ordin de securitate acceptabil, trebuie folosit un şir (n, k) - Mignotte cu o valoare $(\alpha - \beta)/\beta$ mare (o metodă de generare a unor astfel de şiruri este prezentată în [48], pagina 9).

Exemplul 4.8. *Folosind şirul Mignotte din Exemplul 4.7 se determină*

$$\alpha = 5 \cdot 7 \cdot 9 = 315, \qquad \beta = 11 \cdot 13 = 143.$$

Să considerăm secretul $285 \in (143, 315)$.

Cele cinci componente sunt

$$\begin{array}{lll} S_1 = S\ (mod\ 5) = 0, & S_2 = S\ (mod\ 7) = 5, & S_3 = S\ (mod\ 9) = 6, \\ S_4 = S\ (mod\ 11) = 10, & S_5 = S\ (mod\ 13) = 12 & \end{array}.$$

Pentru grupul autorizat $\{P_1, P_3, P_4\}$ *trebuie rezolvat sistemul*

$$\begin{cases} x \equiv 0\ (mod\ 5) \\ x \equiv 6\ (mod\ 9) \\ x \equiv 10\ (mod\ 11) \end{cases}$$

a cărui soluţie unică este 285.

De remarcat că – deoarece $\dfrac{\beta - \alpha}{\beta} = 1.2$ *– în intervalul* (β, α) *există puţine numere care pot fi luate drept secret* S *accesibil oricărui grup autorizat.*

De exemplu, pentru $S = 300$*, participanţii* P_3 *şi* P_4 *posedă aceeaşi componentă:* $S_3 = S_4 = 3$*; deci nu există nici un grup autorizat de forma* $\{P_3, P_4, x\}$ *care să aibă acces la secretul* S.

Evident, schema Mignotte nu este perfectă; avantajul ei este însă acela că oferă componente mici, şi deci poate fi utilizată în aplicaţii în care un factor important de lucru constă în compactificarea componentelor.

Sorin Iftene ([41]) extinde schema de partajare majoritară Mignotte, folosind şirurile Mignotte generalizate (elementele sale nu mai sunt obligatoriu prime două câte două).

Schema Asmuth-Bloom

Schema propusă de Asmuth and Bloom ([1]) este foarte asemănătoare cu schema Mignotte. Ea foloseşte un şir de numere întregi pozitive prime două câte două

$$p_0,\ p_1 < \ldots < p_n$$

cu proprietatea

$$p_0 \cdot \prod_{i=0}^{k-2} p_{n-i} < \prod_{i=1}^{k} p_i.$$

Fiind dat un şir Asmuth-Bloom, schema de partajare (n, k) - majoritară este definită astfel:

1. D stabileşte secretul $S \in Z_{p_0}$.
2. Componentele S_i $(1 \le i \le n)$ sunt definite $S_i = (S + r \cdot p_0)\ (mod\ p_i)$, unde r este un întreg arbitrar cu proprietatea $S + r \cdot p_0 \in Z_{p_1 \ldots p_k}$.
3. D trimite componentele S_i $(1 \le i \le n)$ celor n participanţi.

Fiind date k componente distincte $S_{i_1}, \ldots, S_{i_k}$, secretul S se obţine prin $S = x_0\ (mod\ p_0)$, unde x_0 este soluţia modulo $p_{i_1} \ldots p_{i_k}$ (obţinută cu TCR) a sistemului

$$\begin{cases} x \equiv S_{i_1} \quad (mod\ p_{i_1}), \\ \quad \vdots \\ x \equiv S_{i_k} \quad (mod\ p_{i_k}) \end{cases}$$

Exemplul 4.9. *Să considerăm şirul Asmuth - Bloom*

$$p_0 = 5,\ p_1 = 11,\ p_2 = 13,\ p_3 = 17,\ p_4 = 19,\ p_5 = 23$$

Evident, inegalitatea $p_0 \cdot p_4 \cdot p_5 < p_1 \cdot p_2 \cdot p_3$ este verificată (revine la $2185 < 2431$).
Pe baza acestui şir definim schema de partajare $(5,3)$ - majoritară Asmuth-Bloom:
Fie $S = 2 \in Z_5$. Alegem $r = 317$ şi avem $S + r \cdot p_0 = 1587$.
Cele cinci componente sunt:

$$\begin{array}{lll} S_1 = 1587\ (mod\ 11) = 3, & S_2 = 1587\ (mod\ 13) = 1, & S_3 = 1587\ (mod\ 17) = 6 \\ S_4 = 1587\ (mod\ 19) = 10, & S_5 = 1587\ (mod\ 23) = 0. & \end{array}$$

Să considerăm mulţimea autorizată $\{P_2, P_3, P_4\}$.
Cei trei patricipanţi vor avea de rezolvat sistemul de congruenţe

$$x \equiv 1\ (mod\ 13), \qquad x \equiv 6\ (mod\ 17), \qquad x \equiv 10\ (mod\ 19)$$

care are soluţia (unică în Z_{4199})

$$x_0 = 313 \cdot 6 \cdot 1 + 247 \cdot 2 \cdot 6 + 221 \cdot 8 \cdot 10 = 22582\ (mod\ 4199) = 1587$$

Se poate determina acum secretul $S = 1587\ (mod\ 5) = 2$.

Şirul Asmuth-Bloom poate fi generalizat eliminând condiţia de numere prime între ele. Practic, se poate utiliza orice şir $p_0, p_1, \ldots, p_n$ care verifică inegalitatea[3]

$$p_0 \cdot \max_{1 \le i_1 < i_2 < \ldots < i_{k-1} \le n} \Big([p_{i_1}, \ldots, p_{i_{k-1}}]\Big) < \min_{1 \le i_1 < i_2 < \ldots < i_k \le n} ([p_{i_1}, \ldots, p_{i_k}])$$

Este uşor de remarcat că dacă se înmulţesc elementele p_i $(i > 0)$ ale unui şir Asmuth-Bloom $p_0, p_1, \ldots, p_n$ cu o valoare fixată $r \in \mathcal{Z}$, $(r, p_0 \ldots p_n) = 1$, se obţine un şir Asmuth-Bloom generalizat.

4.1.4 Scheme de partajare majoritar ponderate

Într-o schemă de partajare *majoritar ponderată*, fiecărui utilizator i se asociază un număr pozitiv (numit "pondere"); secretul poate fi reconstruit dacă şi numai dacă suma ponderilor participanţilor este cel puţin egală cu o valoare limită fixată.

Shamir ([73]) este primul care defineşte astfel de scheme, prezentând scenariul unei companii, în care secretul poate fi acoperit de 3 directori, de doi directori şi un vice-preşedinte, sau de către preşedinte. Ideea de bază este de a acorda mai multe componente utilizatorilor mai importanţi (aici preşedintele primeşte 3 componente, fiecare vice-preşedinte are câte două componente, iar un director deţine numai o componentă a secretului).

Structurile de acces majoritar ponderate se definesc astfel:

[3] Notaţia $[x, y]$ semnifică cel mai mic multiplu comun al numerelor întregi pozitive x şi y.

Definiţia 4.6. *Fie* $n \geq 2$, $x = (x_1, \ldots, x_n)$ *un vector de numere întregi pozitive şi numărul întreg* $w \in \left(2, \sum_{i=1}^{n} x_i\right)$. *Structura de acces*

$$\mathcal{A} = \left\{ A \in 2^{\mathcal{P}} \mid \sum_{P_i \in A} x_i \geq w \right\}$$

se numeşte structură (x, w, n) *- majoritar ponderată.*

Într-o astfel de schemă, un grup $\{P_{i_1}, \ldots, P_{i_t}\}$ este autorizat dacă şi numai dacă $\{i_1, \ldots, i_t\}$ este o mulţime de acces într-o structură (x, w, n) - majoritar ponderată: $\sum_{j=1}^{t} x_{i_j} \geq w$.

Parametrii $x_1, \ldots, x_n$ se numesc *ponderi* iar w este *limita* schemei de partajare. Dacă $\mathcal{A}$ este o structură de acces (x, w, n) - majoritar ponderată, orice sistem de partajare construit pe baza ei se numeşte *schemă de partajare a secretelor* (x, w, n) *- majoritar ponderată.*

Observaţia 4.2. *O schemă de partajare a secretelor* (n, k) *- majoritară este un caz particular de schemă* (x, w, n) *- majoritar ponderată cu* $x_1 = \ldots = x_n = 1$ *şi* $w = k$.

Benaloh şi Leichter ([5]) au demonstrat că există structuri de acces care nu sunt majoritar ponderate.

Exemplul 4.10. *Fie* $n = 4$ *şi* $\mathcal{A}_{min} = \{\{P_1, P_2\}, \{P_3, P_4\}\}$ *(a se vedea şi Exemplul 4.2). Să presupunem că lucrăm cu o structură de acces majoritar ponderată, cu ponderile* x_1, x_2, x_3, x_4 *şi limita* w. *Deci*

$$x_1 + x_2 \geq w, \quad x_3 + x_4 \geq w.$$

Adunând aceste inegalităţi, obţinem $x_1 + x_2 + x_3 + x_4 \geq 2w$, *deci*

$$2 \cdot max(x_1, x_2) + 2 \cdot max(x_3, x_4) \geq 2w$$

sau $max(x_1, x_2) + max(x_3, x_4) \geq w$.

În concluzie, una din mulţimile $\{P_1, P_3\}, \{P_1, P_4\}, \{P_2, P_3\}, \{P_2, P_4\}$ *este o mulţime autorizată de acces, dar nu este generată de baza* $\mathcal{A}_{min}$.

Cea mai simplă metodă de construcţie a unei scheme (x, w, n) - majoritar ponderate constă în utilizarea unei scheme de partajare (N, w) - majoritare, în care $N = \sum_{i=1}^{n} x_i$.

Detaliind, fie $s_1, \ldots, s_N$ componentele corespunzătoare unui secret S în raport cu o schemă arbitrară de partajare a secretelor (N, w) - majoritară. Considerăm o partiţie oarecare $\{X_1, \ldots, X_n\}$ a mulţimii $\{1, 2, \ldots, N\}$, cu $card(X_i) = x_i, (1 \leq i \leq n)$.

Definim atunci componentele structurii de acces majoritar ponderate prin

$$S_i = \{s_j \mid j \in X_i\}, \quad i = 1 \ldots n$$

Scheme majoritar ponderate bazate pe TCR

O extensie (naturală) a şirului Mignotte generalizat este:

Definiţia 4.7. *Fie $x = (x_1, \ldots, x_n)$ $(n \geq 2)$ un şir de ponderi şi w o limită. Un şir (x, w, n) - Mignotte este un şir $p_1, \ldots, p_n$ de numere întregi pozitive cu proprietatea*

$$\max_{\substack{A \in 2^{\mathcal{P}} \\ \sum_{P_i \in A} x_i \leq w-1}} ([\{p_i \mid P_i \in A\}]) < \min_{\substack{A \in 2^{\mathcal{P}} \\ \sum_{P_i \in A} x_i \geq w}} ([\{p_i \mid P_i \in A\}])$$

Observaţia 4.3. *Pentru $x_1 = \ldots = x_n = 1$ şi $w = k$, un şir $p_1, \ldots, p_n$ este şir (x, w, n) - Mignotte dacă şi numai dacă $p_1, \ldots, p_n$ este un şir (n, k) - Mignotte generalizat.*

În aceleaşi ipoteze, un şir $p_1, \ldots, p_n$ cu elemente prime între ele, este un şir $(x, , w, n)$ - Mignotte dacă şi numai dacă $p_1, \ldots, p_n$ este un şir (n, k) - Mignotte (conform Definiţiei 4.5).

O modalitate de construcţie a şirurilor (x, w, n) - Mignotte este:

Fie $p'_1, \ldots, p'_N$ un şir (N, w) - Mignotte generalizat, unde $N = \sum_{i=1}^{n} x_i$.

Definim $p_i = \left[\{p'_j \mid j \in X_i\}\right]$, $(1 \leq i \leq n)$, unde $\{X_1, \ldots, X_n\}$ este o partiţie arbitrară a mulţimii $\{1, 2, \ldots, N\}$ astfel încât $card(X_i) = x_i$ $(1 \leq i \leq n)$.

Se obţine

$$\max_{A \in T} ([\{p_i \mid P_i \in A\}]) = \max_{A \in T} \left([\{[\{p'_j \mid j \in X_i\}] \mid P_i \in A\}]\right) = \max_{A \in T} \left([\{p'_j \mid j \in \bigcup_{P_i \in A} X_i\}]\right)$$

unde am notat $T = \{A \in 2^{\mathcal{P}} \mid \sum_{P_i \in A} x_i \leq w - 1\}$.

În plus, pentru orice mulţime $A \in 2^{\mathcal{P}}$ cu $\sum_{P_i \in A} x_i \leq w - 1$ se obţine

$card\left(\{p'_j \mid j \in \bigcup_{P_i \in A} X_i\}\right) = \sum_{P_i \in A} card(X_i) = \sum_{P_i \in A} x_i \leq w - 1$, şi deci

$$\max_{A \in T} ([\{p_i \mid P_i \in A\}]) \leq \max_{1 \leq i_1 < \ldots < i_{w-1} \leq N} \left([\{p'_{i_1}, \ldots, p'_{i_{w-1}}\}]\right).$$

Printr-un raţionament similar se arată şi relaţia

$$\min_{1 \leq i_1 < \ldots < i_w \leq N} \left([\{p'_{i_1}, \ldots, p'_{i_w}\}]\right) \leq \min_{A \in U} ([\{p_i \mid P_i \in A\}])$$

unde s-a notat $U = \{A \in 2^{\mathcal{P}} \mid \sum_{P_i \in A} x_i \geq w\}$.

Cu aceste două relaţii, din faptul că $p'_1, \ldots, p'_N$ este un şir (N, w) - Mignotte generalizat şi din Definiţia 4.7, rezultă că $p_1, \ldots, p_n$ este un şir (x, w, n) - Mignotte.

Exemplul 4.11. *Fie* $n = 4$*, ponderile* $x_1 = x_2 = 1,\ x_3 = x_4 = 2$ *şi limita* $w = 3$*.*
Se obţine imediat $N = 6$*.*

Folosim şirul $7, 11, 13, 17, 19, 23$ *(care este un şir* $(3, 6)$ *- Mignotte generalizat).*
Considerând partiţia $\{\{6\}, \{5\}, \{1, 4\}, \{2, 3\}\}$ *a mulţimii* $\{1, 2, 3, 4, 5, 6\}$*, va rezulta şirul*

$$23, 19, 119, 143 \qquad \textit{unde} \quad 119 = [7, 17],\ 143 = [11, 13]$$

ca un şir $((1, 1, 2, 2), 3, 4)$ *- Mignotte.*

Pe baza unui şir (x, w, n) - Mignotte $p_1, \ldots, p_n$, se poate construi o schemă de partajare (x, w, n) - majoritar ponderată, în felul următor:

1. D calculează U şi
$$\alpha = \min_{A \in U} ([\{p_i \mid P_i \in A\}]), \qquad \beta = \max_{A \in T} ([\{p_i \mid P_i \in A\}]);$$
2. D generează (aleator) secretul $S \in [\beta + 1, \alpha - 1]$.
3. Componentele sunt $S_i = S \ (mod\ p_i)$, $\quad (1 \le i \le n)$.
4. Fiecare participant P_i $(1 \le i \le n)$ primeşte de la D perechea (S_i, p_i).

Pentru o mulţime de componente $\{S_i \mid P_i \in A\}$, unde mulţimea $A \in \mathcal{A}$ verifică inegalitatea $\sum_{i \in A} x_i \ge w$, secretul S poate fi obţinut ca soluţie (unică) modulo $[\{p_i \mid P_i \in A\}]$ a sistemului

$$\{\ x \equiv S_i \ (mod\ p_i), \quad P_i \in A\ .$$

Securitatea schemei (x, w, n) **- majoritar ponderată**: Pentru un set de componente $\{S_i \mid P_i \in A\}$, unde A verifică inegalitatea $\sum_{P_i \in A} x_i \le w - 1$, singura informaţie care se poate obţine prin aflarea soluţiei $x_0 \in Z_{[\{p_i \mid P_i \in A\}]}$ a sistemului

$$\{\ x \equiv S_i \ (mod\ p_i), \quad P_i \in A$$

este $S \equiv x_0 \ \ (mod\ [\{p_i \mid P_i \in A\}])$.

Într-adevăr, prin alegerea secretului S $(S > \beta)$, vom avea $S \notin Z_{[\{p_i \mid P_i \in A\}]}$, deci acesta nu va fi soluţia unică modulo $[\{p_i \mid P_i \in A\}]$ a sistemului de mai sus.

Alegând şiruri (x, w, n) - Mignotte cu valori mari pentru $\dfrac{\alpha - \beta}{\beta}$, problema găsirii secretului S, ştiind că este în intervalul $[\beta + 1, \alpha - 1]$ şi $S \equiv x_0 \ \ (mod\ [\{p_i \mid P_i \in A\}])$, pentru o mulţime neautorizată A, este $\mathcal{NP}$ - completă.

Exemplul 4.12. *Fie $n = 4$, ponderile $x_1 = x_2 = 1$, $x_3 = x_4 = 2$ şi limita $w = 3$. Structura de acces majoritar ponderată este generată de* $\mathcal{A}_{min} = \{\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$, *iar* $\mathcal{A}_{max} = \{\{1,2\},\{3\},\{4\}\}$.

Conform Exemplului 4.11, şirul $23, 19, 119, 143$ *este un şir* $((1,1,2,2),3,4)$ *- Mignotte. Calculăm*

$\alpha = min([23,119],[23,143],[19,119],[19,143],[119,143]) = 2261$ *respectiv*

$\beta = max([23,19],119,143) = 437$.

O schemă de partajare a secretelor $((1,1,2,2),3,4)$ *- ponderat majoritară este:*

- $S \in [438, 2260]$ *este generat aleator; de exemplu, fie* $S = 601$.
- *Componentele sunt*

$$\begin{aligned} S_1 &= 601\ (mod\ 23) = 3,\\ S_2 &= 601\ (mod\ 19) = 12,\\ S_3 &= 601\ (mod\ 119) = 6,\\ S_4 &= 601\ (mod\ 143) = 29. \end{aligned}$$

Considerând de exemplu componentele $S_1 = 3$ *şi* $S_3 = 6$ *(puse în comun de mulţimea autorizată de acces* $\{P_1, P_3\}$*), secretul* S *poate fi obţinut ca soluţie în* Z_{2737} *a sistemului*

$$\begin{cases} x \equiv 3 & (mod\ 23) \\ x \equiv 6 & (mod\ 119) \end{cases}$$

care este 601.

În schimb $A = \{P_1, P_2\}$ *nu corespunde unei mulţimi autorizate de acces. Într-adevăr, din componentele* $S_1 = 3$, $S_2 = 12$, *secretul* S *nu poate fi obţinut din soluţia în* Z_{437} *a sistemului*

$$\begin{cases} x \equiv 3 & (mod\ 23) \\ x \equiv 12 & (mod\ 119) \end{cases}$$

Se verifică imediat că acest sistem are soluţia unică 164.

4.1.5 Schemă majoritară bazată pe dispersia informaţiei

Ideea de schemă majoritară de dispersie a informaţiei a fost introdusă de Rabin ([67]).

Definiţia 4.8. *Se dau numerele întregi* n, k $(2 \leq k \leq n)$. *O schemă de dispersie a informaţiei* (n, k) *- majoritară este o metodă de generare* $(S, (F_1, \ldots, F_n))$ *cu proprietatea că pentru orice mulţime* $A \in 2^{\mathcal{P}}$ *cu* $card(A) = k$, *problema aflării elementului* S *din mulţimea* $\{F_i \mid P_i \in A\}$, *este "uşoară".*

Elementul S este numit "informaţia" iar $F_1, \ldots, F_n$ sunt numite "fragmentele lui S".

Singura diferenţă dintre noţiunea de dispersie a informaţiei şi cea de partajare a secretelor constă în faptul că în primul caz nu există nici o restricţie referitoare la grupurile neautorizate.

Krawczyk ([49]) a definit o schemă de dispersie a informaţiei (n, k) - majoritară, foarte apropiată de schema de partajare a lui Shamir:

- Fie informaţia $S = (a_0, \ldots, a_{k-1})$ cu elemente dintr-un corp finit. Se defineşte polinomul $a(X) = a_0 + a_1X + \ldots + a_{k-1}X^{k-1}$.
- Se construiesc fragmentele $F_1, \ldots, F_n$ prin $F_i = a(x_i)\ \ (1 \le i \le n)$, unde $x_1, \ldots, x_n$ sunt valori publice distincte, generate aleator.
- Fiind dat un grup $A \in 2^{\mathcal{P}}$ cu $card(A) = k$ şi fragmentele $\{F_i \mid P_i \in A\}$, polinomul $a(X)$ (şi deci informaţia S) se poate obţine cu formula de interpolare Lagrange:

$$\sum_{P_i \in A} \left(F_i \cdot \prod_{P_j \in A \setminus \{P_i\}} \frac{X - x_j}{x_i - x_j} \right).$$

Diferenţa între această schemă şi schema de partajare majoritară a lui Shamir constă în faptul că aici informaţia este reprezentată printr-un polinom complet, pe când la Shamir ea era conţinută doar în termenul liber al unui polinom.

Pe baza acestei scheme, Krawczyk a definit un protocol majoritar de partajare a secretelor, computaţional sigur. O formă a sa este:

1. D face public un algoritm de criptare e.
2. D alege aleator o cheie K şi calculează $\overline{S} = e_K(S)$.
3. D foloseşte o schemă de dispersie a informaţiei (n, k) - majoritară pentru a ”sparge” secretul $\overline{S}$ în n fragmente $F_1, \ldots, F_n$.
4. D foloseşte o schemă perfectă de partajare a secretelor (n, k) - majoritară pentru a construi componentele $K_1, \ldots, K_n$ corespunzătoare cheii secrete K.
5. Se definesc componentele $S_i = (F_i, K_i)\ \ i = 1 \ldots n$, care se distribuie utilizatorilor prin canale securizate.

Fiind date k componente distincte $S_{i_1} = (F_{i_1}, K_{i_1}), \ldots, S_{i_k} = (F_{i_k}, K_{i_k})$, secretul S poate fi recompus astfel:

1. Se determină $\overline{S}$ folosind algoritmul de reconstrucţie aplicat lui $F_{i_1}, \ldots, F_{i_k}$.
2. Se determină cheia K folosind algoritmul de reconstrucţie pentru $K_{i_1}, \ldots, K_{i_k}$.
3. Se calculează secretul $S = d_K(\overline{S})$.

Observaţia 4.4. *Referitor la cantitatea de informaţie deţinută de un participant:*
Lungimea celei de a i-a componente este $|F_i| + |K_i|$; deci ea depinde atât de schema de dispersie a informaţiei cât şi de schema de partajare folosită.
Dacă se foloseşte un sistem de criptare care păstrează lungimea ($\forall K \forall x,\ |e_K(x)| = |x|$), o schemă ideală de dispersie majoritară a informaţiei $\left(|F_i| = \dfrac{|S|}{k},\ \forall i = 1, \ldots, n\right)$ şi o schemă ideală de partajare a secretelor, atunci fiecare componentă S_i va avea lungimea $\dfrac{|S|}{k} + |K|$.

4.2 Scheme de partajare unanime

În cazul $\mathcal{A} = \mathcal{A}_{min} = \{P_1, P_2, \ldots, P_n\}$, o $\mathcal{A}$ - schemă de partajare a secretelor se numeşte *unanimă*[4] de ordin n.
Pentru astfel de scheme, secretul este aflat numai prin participarea tuturor utilizatorilor implicaţi.

Evident, o schemă de partajare unanimă de ordin n este echivalentă cu o schemă de partajare (n, n) - majoritară şi – reciproc – orice schemă de partajare a secretelor (n, n) - majoritară poate fi utilizată în realizarea unei scheme de partajare unanime.

O schemă de partajare unanimă foarte simplă este propusă de Karnin, Greene şi Hellman ([44]):

1. Secretul S este un număr aleator din Z_q ($q > 2$ număr arbitrar fixat).
2. D generează aleator componentele $S_i \in Z_q,\ (1 \le i \le n-1)$.
   După aceea determină $S_n = S - \sum_{i=1}^{n-1} S_i \ (mod\ q)$.
3. D trimite fiecărui participant P_i componenta $S_i \quad i = 1, \ldots, n$

Secretul S poate fi reconstruit cu relaţia $S = \sum_{i=1}^{n} S_i \ (mod\ q)$.

Exemplul 4.13. *Să considerăm $n = 20,\ q = 15$, şi fie secretul $S = 4 \in Z_{15}$.*
Dacă se definesc componentele $S_i = i\ (1 \le i \le 19)$, ultima componentă va fi

$$S_{20} = 4 - \sum_{i=1}^{19} i = 4 - 190 = -186 = 9\ (mod\ 15)$$

[4]în engleză "unanimous consent secret sharing scheme".

Secretul S poate fi recompus numai prin însumarea celor 20 componente:

$$S = \sum_{i=1}^{20} S_i = 1 + 2 + \ldots + 19 + 9 = 199 = 4 \ (mod\ 15)$$

4.3 Scheme bazate pe grafuri pentru structuri de acces

O structură de acces în care orice mulţime minimală de acces are două elemente se numeşte *structură de acces* 2 - *omogenă* sau *structură de acces bazată pe grafuri* (deoarece grupurile minimale de acces pot fi specificate în acest caz prin arcele unui graf).

Definiţia 4.9. *Un graf $G = (V, E)$ este multipartit complet dacă V se poate partiţiona în submulţimile $V_1, \ldots, V_s$ astfel încât $\{x, y\} \in E$ dacă şi numai dacă $x \in V_i,\ y \in V_j$ cu $i \neq j$. Mulţimile V_i se numesc componente.*
Dacă $card(V_i) = n_i$ $(1 \leq i \leq s)$, graful este notat $K_{n_1,\ldots,n_s}$.
Graful multipartit complet $K_{1,\ldots,1}$ cu s componente este de fapt un graf complet şi se notează K_s.

Teorema 4.3. *Fie G un graf conex. Există o schemă ideală de partajare a secretelor pentru structura de acces specificată de G dacă şi numai dacă G este un graf multipartit complet.*

Stinson ([77]) construieşte o schemă ideală de partajare a secretelor, bazată pe structura de acces specificată de graful $K_{n_1,n_2,\ldots,n_s} = (V, E)$:

1. Fie $q > m = card(V)$ un număr prim şi $V_1, \ldots, V_s$ componentele grafului $K_{n_1,n_2,\ldots,n_s}$ (având nodurile numerotate $1, 2, 3, \ldots, m$).
2. D generează s numere aleatoare distincte $x_1, \ldots, x_s \in Z_q$.
3. Dacă $S \in Z_q$ este un secret, componentele sale se definesc prin

   $$S_i = x_j \cdot S + r \ (mod\ q)$$

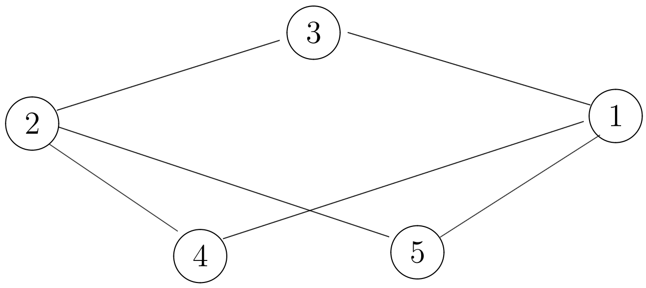
   pentru $i \in V_j$ $(1 \leq j \leq s)$ şi $r \in Z_q$ arbitrar fixat.
4. D trimite fiecărui participant $u_i \in V_j$ componenta (S_i, x_j), $1 \leq j \leq s$.

Deci $\mathcal{K} = Z_q$, $\mathcal{S} = Z_q \times Z_q$.
Oricare doi utilizatori $(u_1, u_2) \in V_{j_1}, \times V_{j_2}$ $(j_1 \neq j_2)$ pot recompune secretul S după

formula

$$S = \frac{S_{u_1} - S_{u_2}}{x_{j_1} - x_{j_2}} \quad (mod\ q).$$

Exemplul 4.14. *Să considerăm graful multipartit complet* $K_{2,3}$*:*



Avem $s = 2$ *şi* $V_1 = \{P_1, P_2\},\ V_2 = \{P_3, P_4, P_5\}$.

Fie $q = 11$ *şi să alegem aleator valorile* $x_1 = 7,\ x_2 = 4,\ r = 8$.

Pentru secretul $S = 10$*, componentele sale sunt:*

$$S_1 = S_2 = x_1 \cdot S + r = 7 \cdot 10 + 8\ (mod\ 11) = 1,$$

$$S_3 = S_4 = S_5 = x_2 \cdot S + r = 4 \cdot 10 + 8\ (mod\ 11) = 4.$$

Dacă participanţii P_2 *şi* P_3 *vor să recompună secretul, ei vor calcula*

$$S = \frac{S_1 - S_4}{x_1 - x_2} = \frac{1-4}{7-4} = (-3) \cdot 3^{-1} = -1 = 10\ (mod\ 11)$$

4.4 Construcţia circuitelor monotone

Ideea ([5]) constă în construirea unui circuit combinaţional care ”recunoaşte” structura de acces şi generează un sistem de partajare a secretului. Un astfel de circuit este numit de autori (Benaloh şi Leichter) *circuit monoton*.

Fie **C** un circuit combinaţional[5] cu n intrări notate prin variabilele booleene $x_1, \ldots, x_n$ (corespunzătoare celor n participanţi $P_1, \ldots, P_n$) şi o ieşire booleană $y = \mathbf{C}(x_1, \ldots, x_n)$. Presupunem că la construcţia circuitului sunt folosite numai porţi AND şi OR (fără porţi NOT). Un astfel de circuit este numit ”monoton” dacă modificarea valorii unei intrări din 0 în 1 nu va implica niciodată transformarea ieşirii y din 1 în 0.

Vom nota

$$B(x_1, \ldots, x_n) = \{P_i \mid x_i = 1\}$$

mulţimea participanţilor asociaţi în mulţimea B. Presupunând că circuitul **C** este monoton, vom avea

$$\Gamma(\mathbf{C}) = \{B(x_1, \ldots, x_n) \mid \mathbf{C}(x_1, \ldots, x_n) = 1\}.$$

[5]Pentru detalii a se consulta *A. Atanasiu - Arhitectura Calculatoarelor*, editura InfoData Cluj, 2007.

Circuitul **C** fiind monoton, $\Gamma(\mathbf{C})$ este o mulţime monotonă de părţi ale lui $\mathcal{P}$.

Fiind dată o mulţime monotonă $\mathcal{A} \subseteq \mathcal{P}$, se poate construi uşor un circuit monoton **C** cu $\Gamma(\mathbf{C})= \mathcal{A}$. Un exemplu de construcţie este următorul:

Fie $\mathcal{A}_{min}$ o bază a lui $\mathcal{A}$. Vom construi formula booleană (în forma normal disjunctivă)

$$\bigvee_{B\in\mathcal{A}_{min}} \left(\bigwedge_{P_i\in B} P_i \right)$$

Fiecare clauză din această formă normală este legată printr-o poartă AND, iar disjuncţia finală corespunde unei porţi OR.
Numărul total de porţi folosite este $1 + card(\mathcal{A}_{min})$.

Fie acum **C** un circuit monoton care recunoaşte $\mathcal{A}$. Vom construi un algoritm care permite arbitrului D să construiască un sistem perfect de partajare a secretului cu structura de acces $\mathcal{A}$, similar schemei de partajare (n, n) - majoritară definită în secţiunea 4.2. Mulţimea secretelor este deci $\mathcal{K}= Z_q$ (q număr prim).

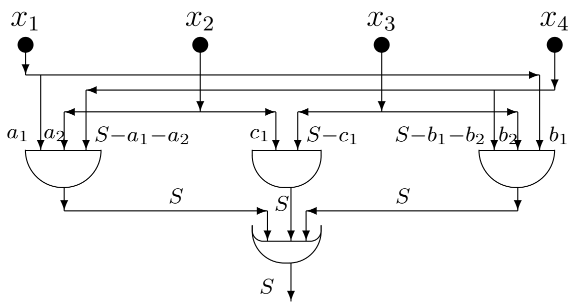
Algoritmul parcurge circuitul de la ieşire spre intrare, marcând recursiv cu $x_V \in \mathcal{K}$, fiecare arc V parcurs (în sens invers).
Iniţial, arcului care marchează ieşirea y i se atribuie valoarea $x_{out} = S$.
Formal, algoritmul este:

1. $x_{out} \leftarrow S$;
2. pentru orice poartă G din care iese un arc marcat x, iar arcele care intră sunt nemarcate, execută:
   (a) Dacă G este o poartă OR, atunci $x_V \leftarrow x$ pentru orice arc V care intră în G;
   (b) Dacă G este o poartă AND şi $V_1, \ldots, V_n$ sunt arcele care intră în G, atunci
      i. Alege aleator $x_{V,1}, \ldots, x_{V,n-1} \in Z_q$;
      ii. Calculează $x_{V,n} = x - \sum_{i=1}^{n-1} x_{V,i} \pmod q$;
      iii. Marchează arcul V_i cu $x_{V,i}$ $(1 \le i \le n)$.
      iv. D distribuie fiecărui participant P_i componenta S_i definită
      $S_i = \{x_{V,i} \mid V \text{ arc ce intră într-o poartă } AND\}$.

Exemplul 4.15. *Pentru mulţimea din Exemplul 4.1, avem*
$\mathcal{A}_{min} = \{\{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3\}\}$, *deci se poate asocia expresia booleană*

$$(P_1 \wedge P_2 \wedge P_4) \vee (P_1 \wedge P_3 \wedge P_4) \vee (P_2 \wedge P_3).$$

Circuitul monoton asociat este desenat mai jos; în paralel au fost marcate şi arcele, conform algoritmului descris:



Aici $a_1, a_2, b_1, b_2, c_1, c_2$ sunt numere alese aleator în Z_q. Fiecare participant primeşte drept componentă două numere: 1. a_1 *şi* b_1 *pentru* P_1,

2. a_2 *şi* c_1 *pentru* P_2,
3. b_2 *şi* $S - c_1$ *pentru* P_3,
4. $S - a_1 - a_2$ *şi* $S - b_1 - b_2$ *pentru* P_4.

Fiecare submulţime autorizată poate calcula valoarea lui S (modulo q). Astfel, $\{P_1, P_2, P_4\}$ determină $S = a_1 + a_2 + (S - a_1 - a_2)$, submulţimea $\{P_1, P_3, P_4\}$ calculează $S = b_1 + b_2 + (S - b_1 - b_2)$, iar $\{P_2, P_3\}$ va calcula $S = c_1 + (S - c_1)$.

Să vedem acum ce se întâmplă cu mulţimile neautorizate.
Deoarece orice submulţime a unei mulţimi neautorizate sa va fi de asemenea neautorizată, este suficient să demonstrăm că mulţimile maximale neautorizate nu pot determina secretul, folosind informaţiile pe care le deţin.

Exemplul 4.16. *Revenind la exemplul anterior, mulţimile maximale neautorizate sunt $\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_2, P_4\}, \{P_3, P_4\}$. În fiecare caz, pentru determinarea secretului S lipseşte o informaţie definită aleator.*

De exemplu, grupul $\{P_1, P_2\}$ deţine informaţiile a_1, a_2, b_1 şi c_1. Pentru a reconstitui S ar avea nevoie cel puţin de numărul $S - a_1 - a_2$, sau de $S - c_1$.

Sisteme cu aceeaşi structură de acces pot fi obţinute folosind şi alte circuite.

Exemplul 4.17. *Să reluăm Exemplul 4.1 şi să rescriem expresia booleană sub formă normal conjunctivă:*

$$(P_1 \vee P_2) \wedge (P_1 \vee P_3) \wedge (P_2 \vee P_3) \wedge (P_2 \vee P_4) \wedge (P_3 \vee P_4)$$

Construind schema de partajare corespunzătoare acestei expresii, vom avea următoarea distribuţie a componentelor (omitem detaliile):

1. P_1 *primeşte* $S_1 = \{a_1,\ a_2\}$;
2. P_2 *primeşte* $S_2 = \{a_1,\ a_3,\ a_4\}$;
3. P_3 *primeşte* $S_3 = \{a_2,\ a_3,\ S - a_1 - a_2 - a_3 - a_4\}$;
4. P_4 *primeşte* $S_4 = \{a_4,\ S - a_1 - a_2 - a_3 - a_4\}$.

Teorema 4.4. *Fie* $\mathbf{C}$ *un circuit combinaţional monoton. El defineşte o schemă perfectă de partajare a secretului, a cărui structură de acces este* $\mathcal{A} = \Gamma(\mathbf{C})$.

Demonstraţie. Vom folosi o inducţie după numărul de porţi din circuitul $\mathbf{C}$.

i. Cazul când $\mathbf{C}$ are o singură poartă este banal: dacă poarta este OR, fiecare participant deţine secretul S şi structura de acces este $\mathcal{A} = 2^{\mathcal{P}} \setminus \{\emptyset\}$; dacă poarta este AND şi are n intrări, se obţine sistemul (n, n)-majoritar definit anterior.

ii. Să presupunem că pentru $j > 1$, orice circuit $\mathbf{C}$ cu mai puţin de j porţi verifică teorema, şi fie $\mathbf{C}$ un circuit cu j porţi. Vom considera ultima poartă G a acestui circuit (din care iese rezultatul y). Ea nu poate fi decât OR sau AND. Dacă G este o poartă OR, să trasăm cele n arce $V_1, V_2, \ldots, V_n$ care intră în G. Acestea sunt arcele de ieşire din n circuite $\mathbf{C_i}$; conform ipotezei de inducţie, fiecare astfel de circuit defineşte un subsistem de partajare a secretului, cu structura de acces $\mathcal{A}_i = \Gamma(\mathbf{C_i})$. Vom avea – evident

$$\Gamma(\mathbf{C}) = \bigcup_{i=1}^{n} \mathcal{A}_i.$$

Cum valoarea S a secretului se atribuie fiecărui arc V_i, sistemul va avea structura de acces $\Gamma(\mathbf{C})$.

Procedeul este similar dacă G este o poartă AND. În acest caz,

$$\Gamma(\mathbf{C}) = \bigcap_{i=1}^{n} \mathcal{A}_i.$$

Deoarece secretul S este repartizat peste toate arcele V_i conform unui sistem (n, n) - majoritar, sistemul total va admite $\Gamma(\mathbf{C})$ drept structură de acces. □

Când un grup autorizată B doreşte aflarea secretului S, el trebuie să ştie circuitul utilizat de D pentru construirea schemei şi să deducă de aici ce componente sunt necesare pentru parcurgerea arcelor respective.
Această informaţie trebuie să fie publică. Numai valorile componentelor S_i trebuie să fie secrete.

4.5 Rata de informaţie

Fie $\mathcal{P}$ o mulţime de participanţi şi $\mathcal{S}$ spaţiul tuturor componentelor posibile ale cheii. O distribuţie de componente este o funcţie

$$f : \mathcal{P} \longrightarrow \mathcal{S}$$

Ea codifică matematic modalitatea de repartizare a informaţiilor între participanţi. $f(P_i)$ va fi componenta distribuită participantului P_i $(1 \le i \le n)$.

Pentru fiecare $S \in \mathcal{K}$, fie $\mathcal{F}_S$ mulţimea tuturor distribuţiilor posibile ale secretului K. În general, informaţia $\mathcal{F}_S$ este publică. Definim

$$\mathcal{F} = \bigcup_{S \in \mathcal{K}} \mathcal{F}_S.$$

$\mathcal{F}$ este ansamblul complet al tuturor distribuţiilor posibile de secrete. Rolul arbitrului va fi de a selecta aleator un element $f \in \mathcal{F}_S$ şi de a distribui componentele în conformitate cu această alegere.

Pentru o submulţime $B \subseteq \mathcal{P}$ (autorizată sau nu) de participanţi, se defineşte

$$S(B) = \{f^B \mid f \in \mathcal{F}\},$$

unde funcţia $f^B : B \longrightarrow \mathcal{S}$ este restricţia distribuţiei de componente f la submulţimea B; ea este deci definită prin $f^B(P_i) = f(P_i), \quad \forall P_i \in B$.

Deci $S(B)$ este mulţimea tuturor distribuţiilor posibile ale componentelor la participanţii din submulţimea B.

Să facem o evaluare a performanţelor sistemelor perfecte de partajare a secretelor construite până acum (pe baza structurilor de acces monotone).

În cazul unei scheme de partajare (n, k) - majoritare, circuitul boolean construit pe baza expresiei scrise în forma normal disjunctivă (a se vedea secţiunea 4.4) are $1 + C_n^k$ porţi. Fiecare participant primeşte o componentă formată din C_{n-1}^{k-1} numere din Z_p. Această partajare este foarte slabă comparativ cu schema Shamir (n, k) - majoritară, care oferă acelaşi rezultat folosind componente formate dintr-un singur număr.

Pentru măsurarea performanţelor sistemelor perfecte de partajare a secretelor, vom folosi un instrument numit *rată de informaţie.*

Definiţia 4.10. *Considerăm un sistem perfect de partajare a secretelor cu structura de acces $\mathcal{A}$. Rata de informaţie a unui participant P_i este prin definiţie*

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

unde $S(P_i) \subseteq \mathcal{S}$ este mulţimea componentelor posibile pe care le poate primi participantul P_i.

Rata de informaţie a sistemului este

$$\rho = min\{\rho_i \mid 1 \leq i \leq n\}$$

Exemplul 4.18. *Să comparăm cele două scheme folosite în exemplele din secţiunea anterioară. Schema din Exemplul 4.15 are rata de informaţie $\rho = \frac{log_2 q}{log_2 q^2} = \frac{1}{2}$.*

Pentru schema din Exemplul 4.17, avem $\rho = \frac{log_2 q}{log_2 q^3} = \frac{1}{3}$.

Deci prima schemă are o rată de informaţie mai bună.

În general, dacă se construieşte un sistem de partajare a secretelor plecând de la un circuit monoton $\mathbf{C}$, rata sa de informaţie se obţine folosind următoarea teoremă:

Teorema 4.5. *Fie* $\mathbf{C}$ *un circuit combinaţional monoton. Există atunci o schemă perfectă de partajare a secretelor, cu structura de acces* $\mathcal{A} = \Gamma(\mathbf{C})$*, care admite ca rată de informaţie*

$$\rho = \max_{1\le i\le n}\left\{\frac{1}{r_i}\right\}$$

unde r_i *este numărul arcelor de intrare din circuit (pentru valorile* x_i*).*

Evident, este preferabilă o rată de informaţie cât mai mare. Valoarea ei este însă limitată superior, conform teoremei următoare:

Teorema 4.6. *Pentru orice schemă perfectă de partajare a secretelor cu structura de acces* $\mathcal{A}$*, rata de informaţie verifică inegalitatea* $\rho \le 1$*.*

Demonstraţie. Să considerăm un sistem perfect de partajare a secretelor având structura de acces $\mathcal{A}$. Fie $B \in \mathcal{A}_{min}$ şi $P_j \in B$ un participant arbitrar. Definim $B' = B \setminus \{P_j\}$. Fie $g \in S(B)$. Cum $B' \in \mathcal{NA}$, distribuţia componentelor $g_{B'}$ nu dă nici o informaţie despre secretul S.
Deci, pentru orice $S \in \mathcal{K}$ există o distribuţie a componentelor $g^S \in \mathcal{F}$ astfel ca $g^S_{B'} = g_{B'}$.
Cum $B \in \mathcal{A}$, vom avea $g^S(P_j) \ne g^{S'}(P_j)$ pentru $S \ne S'$.
Deci $card(S(P_j)) \ge card(\mathcal{K})$, adică $\rho \le 1$. □

O schemă de partajare cu $\rho = 1$ va fi numită ”ideală”. Ca un exemplu, schema de partajare majoritară Shamir are $\rho = 1$, deci este o schemă ideală.
În schimb, rata de informaţie pentru o schemă de partajare (n, k) - majoritară bazată pe circuite monotone construite cu forma normal disjunctivă este $\dfrac{1}{C_{n-1}^{k-1}}$, extrem de ineficientă când $1 < k < n$.

4.6 Schema de partajare a lui Brickell

Sistemul construit în această secţiune este cunoscut sub numele de *construcţia vectorială a lui Brickell.*

Fie $\mathcal{A}$ o structură de acces, q un număr prim, iar $d \ge 2$ un număr întreg. Fie

$$\phi : \mathcal{P} \longrightarrow Z_q^d$$

o funcţie cu proprietatea[6]

$$(1, 0, \ldots, 0) \in \langle \phi(P_i) \mid P_i \in B\rangle \iff B \in \mathcal{A}. \tag{1}$$

Altfel spus, vectorul $(1, 0, \ldots, 0)$ este o combinaţie liniară de vectori din mulţimea $\{\phi(P_i) \mid P_i \in B\}$ dacă şi numai dacă B este o mulţime autorizată.

[6] S-a notat cu $\langle X\rangle$ spaţiul generat de mulţimea de vectori X.

Plecând de la această funcţie, vom construi o schemă de partajare a secretelor cu $\mathcal{K}= S(P_i) = Z_q$ $(1 \le i \le n)$.
Pentru orice $\mathbf{a} = (a_1, \ldots, a_d) \in Z_p^d$. vom defini o funcţie de distribuţie a componentelor $f_{\mathbf{a}} : \mathcal{P} \longrightarrow \mathcal{S}$ prin

$$f_{\mathbf{a}}(x) = \mathbf{a} \cdot \phi(x)$$

Schema Brickell de partajare a secretelor este :

1. Pentru $1 \le i \le n$, D atribuie lui P_i vectorul $\phi(P_i) \in Z_q^d$.
   Aceşti vectori sunt publici.
2. Pentru partajarea secretului $S \in Z_q$, D alege $d - 1$ elemente aleatoare $a_2, \ldots, a_d \in Z_q$.
3. Folosind vectorul $\mathbf{a} = (S, a_2, \ldots, a_d)$, arbitrul calculează componentele

$$S_i = \mathbf{a} \cdot \phi(P_i) \quad (1 \le i \le n)$$

4. Pentru $i = 1, 2, \ldots, n$ arbitrul D trimite componenta S_i participantului P_i.

Vom avea rezultatul următor:

Teorema 4.7. *Dacă ϕ verifică proprietatea* (1)*, mulţimea distribuţiilor de componente $\mathcal{F}_S$, $S \in \mathcal{K}$ formează o schemă perfectă de partajare a secretelor, cu structura de acces $\mathcal{A}$.*

Demonstraţie. Să arătăm întâi că dacă B este o mulţime autorizată, participanţii lui B pot calcula secretul S. Deoarece $(1, 0, \ldots, 0) \in \langle \phi(P_i) \mid P_i \in B \rangle$, putem scrie

$$(1, 0, \ldots, 0) = \sum_{\{i|P_i \in B\}} c_i \phi(P_i)$$

unde $c_i \in Z_q$.
Fie S_i componenta lui P_i. Vom avea $S_i = \mathbf{a} \cdot \phi(P_i)$, unde $\mathbf{a}$ este vectorul necunoscut ales de D, iar $S = a_1 = \mathbf{a} \cdot (1, 0, \ldots, 0)$. Atunci

$$S = \sum_{\{i|P_i \in B\}} c_i \, \mathbf{a} \cdot \phi(P_i)$$

Membrii grupului B pot reconstitui deci secretul

$$S = \sum_{\{i|P_i \in B\}} c_i S_i$$

Ce se întâmplă dacă B nu este un grup autorizat ?
Fie e dimensiunea spaţiului vectorial $\langle \phi(P_i) \mid P_i \in B \rangle$ (evident, $e \leq card(B)$).
Fie $S \in \mathcal{K}$ şi să considerăm sistemul liniar

$$\begin{aligned} \phi(P_i) \cdot \mathbf{a} &= S_i \quad \forall P_i \in B \\ (1, 0, \dots, 0) \cdot \mathbf{a} &= S \end{aligned}$$

cu necunoscutele $a_1, \dots, a_d$.

Matricea sistemului are rangul $e + 1$ deoarece $(1, 0, \dots, 0) \notin \langle \phi(P_i) \mid P_i \in B \rangle$. Deci, independent de valoarea lui S, spaţiul soluţiilor are gradul $d - e - 1$, adică există q^{d-e-1} distribuţii de componente în fiecare $\mathcal{F}_S$, consistente cu componentele participanţilor din B. □

Schema de partajare (n, k) - majoritară a lui Shamir este un caz particular al acestei construcţii.
Într-adevăr, fie $d = k$ şi $\phi(P_i) = (1, x_i, x_i^2, \dots x_i^{k-1})$, pentru $1 \leq i \leq n$, unde x_i este coordonata x dată de P_i. Sistemul obţinut este echivalent cu sistemul din schema lui Shamir.

Un alt rezultat general se referă la structurile de acces care admit ca bază un ansamblu de perechi care definesc un graf multipartit complet.

Teorema 4.8. *Fie $G = (V, E)$ un graf multipartit complet. Atunci există un sistem perfect de partajare a secretelor, ideal, cu structura de acces $\overline{E}$ peste mulţimea V de participanţi.*

Demonstraţie. Fie $V_1, \dots, V_s$ componentele lui G şi $x_1, \dots, x_s \in Z_q$ distincte ($q \geq s$).
Să considerăm $d = 2$.
Pentru fiecare participant $v \in V_i$ se defineşte $\phi(v) = (x_i, 1)$. Proprietatea (1) se verifică imediat, deci – conform Teoremei 4.7 – afirmaţia este demonstrată. □

Vom aplica acest rezultat considerând toate structurile de acces posibile pentru $n = 4$ participanţi.

Va fi suficient să luăm în calcul numai structurile a căror bază nu se poate partiţiona în două mulţimi nevide. De exemplu, $\mathcal{A}_{min} = \{\{P_1, P_2\}, \{P_3, P_4\}\}$ poate fi partiţionată în $\{\{P_1, P_2\}\} \cup \{\{P_3, P_4\}\}$, fiecare cu dezvoltarea sa independentă, deci nu o vom lua în considerare.

O listă completă a structurilor de acces neizomorfe pentru 2, 3 sau 4 participanţi este dată în Tabelul 4.1 (s-a notat cu ρ^* valoarea maximă a ratei de informaţie pentru structura respectivă). Se pot construi scheme de partajare ideale pentru 10 din aceste 18 structuri de acces. Acestea sunt structuri majoritare sau structuri a căror bază este un graf multipartit, pentru care se aplică Teorema 4.8.

Exemplul 4.19. *Să considerăm structura de acces cu numărul 9 din Tabelul 4.1; deci $d = 2$ şi $q \geq 3$. Definim aplicaţia ϕ în felul următor*

$$\phi(P_1) = (0, 1), \quad \phi(P_2) = (0, 1), \quad \phi(P_3) = (1, 1), \quad \phi(P_4) = (1, 2)$$

Tabelul 4.1: Structuri de acces cu maxim 4 participanţi

Nr.crt	n	$\mathcal{A}_{min}$	ρ^*	Rezultate
1.	2	$\{P_1, P_2\}$	1	$(2, 2)$- majoritar
2.	3	$\{P_1, P_2\}, \{P_2, P_3\}$	1	$\mathcal{A}_{min} \simeq K_{1,2}$
3.	3	$\{P_1, P_2\}, \{P_2, P_3\}, \{P_1, P_3\}$	1	$(3, 2)$ - majoritar
4.	3	$\{P_1, P_2, P3\}$	1	$(3, 3)$- majoritar
5.	4	$\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}$	2/3	
6.	4	$\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}$	1	$\mathcal{A}_{min} \simeq K_{1,3}$
7.	4	$\{P_1, P_2\}, \{P_1, P_4\}, \{P_2, P_3\}, \{P_3, P_4\}$	1	$\mathcal{A}_{min} \simeq K_{2,2}$
8.	4	$\{P_1, P_2\}, \{P_2, P_3\}, \{P_2, P_4\}, \{P_3, P_4\}$	2/3	
9.	4	$\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_2, P_3\}, \{P_2, P_4\}$	1	$\mathcal{A}_{min} \simeq K_{1,1,2}$
10.	4	$\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}, \{P_2, P_3\}, \{P_2, P_4\}, \{P_3, P_4\}$	1	$(4, 2)$ - majoritar
11.	4	$\{P_1, P_2, P_3\}, \{P_1, P_4\}$	1	
12.	4	$\{P_1, P_3, P_4\}, \{P_1, P_2\}, \{P_2, P_3\}$	2/3	
13.	4	$\{P_1, P_3, P_4\}, \{P_1, P_2\}, \{P_2, P_3\}, \{P_2, P_4\}$	2/3	
14.	4	$\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}$	1	
15.	4	$\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_3, P_4\}$	1	
16.	4	$\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}$	1	
17.	4	$\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3, P_4\}$	1	$(4, 3)$- majoritar
18.	4	$\{P_1, P_2, P_3, P_4\}$	1	$(4, 4)$- majoritar

Aplicând Teorema 4.8 se obţine o structură perfectă de partajare a secretelor, ideală pentru acest tip de acces.

În Tabelul 4.1 rămân de analizat 8 structuri de acces. Pentru 4 din ele (structurile 11, 14, 15 şi 16) se poate utiliza schema lui Brickell.

Exemplul 4.20. *Pentru structura de acces* 11 *vom considera* $d = 3$ *şi* $q \geq 3$. *Definiţia lui* ϕ *este*

$$\phi(P_1) = (0, 1, 0), \quad \phi(P_2) = (1, 0, 1), \quad \phi(P_3) = (0, 1, -1), \quad \phi(P_4) = (1, 1, 0)$$

Calculând, se obţine
$\phi(P_4) - \phi(P_1) = (1, 1, 0) - (0, 1, 0) = (1, 0, 0)$ *şi*
$\phi(P_2) + \phi(P_3) - \phi(P_1) = (1, 0, 1) + (0, 1, -1) - (0, 1, 0) = (1, 0, 0)$.

Deci $(1, 0, 0) \in \langle \phi(P_1), \phi(P_2), \phi(P_3) \rangle$ *şi* $(1, 0, 0) \in \langle \phi(P_1), \phi(P_4) \rangle$.

Mai rămâne de arătat că $(1, 0, 0) \notin \langle \phi(P_i) \mid P_i \in B \rangle$ *pentru orice mulţime maximală neautorizată* B.

Există numai trei astfel de mulţimi: $\{P_1, P_2\}$, $\{P_1, P_3\}$, $\{P_2, P_3, P_4\}$. *Pentru fiecare caz se arată că sistemul liniar asociat nu are soluţie.*

De exemplu, să considerăm sistemul

$$(1,0,0) = a_2\phi(P_2) + a_3\phi(P_3) + a_4\phi(P_4)$$

cu $a_2, a_3, a_4 \in Z_p$. El este echivalent cu sistemul

$$\begin{array}{rcl} a_2 + a_4 & = & 1 \\ a_3 + a_4 & = & 0 \\ a_2 - a_3 & = & 0 \end{array}$$

care nu are soluţie.

Exemplul 4.21. *Pentru structura de acces 14 vom defini $d = 3$, $q \geq 2$, iar ϕ va fi definită:*

$$\phi(P_1) = (0,1,0), \quad \phi(P_2) = (1,0,1), \quad \phi(P_3) = (0,1,1), \quad \phi(P_4) = (0,1,1)$$

Proprietatea (1) se verifică imediat; deci se poate aplica Teorema 4.8.

În mod similar se pot construi sisteme perfecte de partajare a secretelor ideale pentru structurile 15 şi 16.

Cele patru sisteme rămase nu admit construcţia unor astfel de sisteme.

4.7 Construcţia prin descompunere

Prezentăm aici o altă modalitate de construire a schemelor de partajare a secretelor, remarcabilă prin performanţele rezultatelor, care maximizează rata de informaţie.

Definiţia 4.11. *Fie $\mathcal{A}$ o structură de acces cu baza $\mathcal{A}_{min}$ şi $\mathcal{K}$ o mulţime de secrete. O $\mathcal{K}$ - descompunere ideală a lui $\mathcal{A}_{min}$ este un set $\{\Gamma_1, \ldots, \Gamma_w\}$ cu proprietăţile*

1. $\Gamma_i \subseteq \mathcal{A}_{min} \quad (1 \leq i \leq w)$;
2. $\bigcup_{i=1}^{w} \Gamma_i = \mathcal{A}_{min}$;
3. $\forall\, i\ (1 \leq i \leq w)$ *există un sistem perfect de partajare a secretelor, ideal, cu mulţimea de secrete $\mathcal{K}$, peste mulţimea de participanţi $\mathcal{P}_i = \bigcup_{B\in\Gamma_i} B$.*

Pentru o $\mathcal{K}$ - descompunere ideală a structurii de acces $\mathcal{A}$ se poate construi uşor o schemă perfectă de partajare a secretelor.

Teorema 4.9. *Fie $\mathcal{A}$ o structură de acces cu baza $\mathcal{A}_{min}$, $\mathcal{K}$ o mulţime de secrete şi o $\mathcal{K}$ - descompunere ideală $\{\Gamma_1, \ldots, \Gamma_w\}$ a lui $\mathcal{A}$.*
Pentru fiecare participant P_i, fie $R_i = card\{s|\ P_i \in \mathcal{P}_s\}$.

Există atunci un sistem perfect de partajare a secretelor cu structură de acces $\mathcal{A}$ şi rată de informaţie $\rho = 1/R$, unde $R = \max\limits_{1 \le i \le w} \{R_i\}$.

Demonstraţie. Pentru $1 \le i \le w$ există un sistem ideal de structură de acces de bază Γ_i peste mulţimea secretelor $\mathcal{K}$. Notăm $\mathcal{F}_i$ mulţimea distribuţiilor componentelor sale.

Vom construi un sistem cu structură de acces $\mathcal{A}$ peste mulţimea $\mathcal{K}$.
Mulţimea distribuţiilor componentelor sale este generată după regula: dacă arbitrul D doreşte să împartă secretul S (în cazul $1 \le i \le w$), el va genera aleator o distribuţie de componente $f_i \in \mathcal{F}^i_S$ şi va distribui efectiv aceste componente participanţilor din $\mathcal{P}_i$.

Se verifică uşor că acest sistem este perfect. Să determinăm rata sa de informaţie. Vom avea $card(S(P_i)) = [card(\mathcal{K})]^{R_i}$ pentru orice i $(1 \le i \le n)$. Deci $\rho_i = 1/R_i$ şi

$$\rho = \frac{1}{max\{R_i \mid 1 \le i \le n\}},$$

ceea ce încheie demonstraţia. □

O generalizare a acestui rezultat – pentru s $\mathcal{K}$ - descompuneri ideale – se bazează pe teorema

Teorema 4.10. *(Construcţia prin descompunere): Fie $\mathcal{A}$ o structură de acces de bază $\mathcal{A}_{min}$, $s \ge 1$ un număr întreg, şi $\mathcal{K}$ un set de secrete. Presupunem că s-a construit o $\mathcal{K}$ - descompunere ideală $\mathcal{D}_j = \{\Gamma_{j,1}, \ldots, \Gamma_{j,w_j}\}$ a lui $\mathcal{A}_{min}$, şi fie $\mathcal{P}_{j,k}$ mulţimea participanţilor la structura de acces $\Gamma_{j,k}$. Pentru fiecare participant P_i definim*

$$R_i = \sum_{j=1}^{s} card\{k \mid P_i \in \mathcal{P}_{j,k}\}.$$

Există atunci o schemă perfectă de partajare a secretelor, cu structura de acces $\mathcal{A}$, a cărei rată de informaţie este $\rho = s/R$, unde $R = \max\limits_{1 \le i \le n}(R_i)$.

Demonstraţie. Pentru $1 \le j \le s$ şi $1 \le k \le w$ se poate construi o schemă de partajare ideală, cu baza $\Gamma_{j,k}$ şi mulţimea de secrete $\mathcal{K}$. Vom nota $\mathcal{F}_{j,k}$ mulţimea corespunzătoare de distribuţii a componentelor.

Vom construi un sistem cu structura de acces $\mathcal{A}$ şi mulţimea de secrete $\mathcal{K}^s$. Mulţimea sa de distribuţii de componente $\mathcal{F}$ se generează astfel: dacă arbitrul D doreşte să partiţioneze secretul $S = (S_1, \ldots, S_s)$ atunci – pentru fiecare k $(1 \le k \le w)$ – el va genera aleator o distribuţie de componente $f^{j,k} \in \mathcal{F}^{j,k}_{S_j}$, pe care le distribuie efectiv participanţilor din $\mathcal{P}_{j,k}$.

În continuare se repetă demonstraţia Teoremei 4.9. □

Exemplul 4.22. *Să considerăm structura de acces* 5 *din Tabelul 4.1, a cărei bază nu este un graf multipartit complet.*

Fie q un număr prim şi să considerăm două Z_q - descompuneri:

$$\mathcal{D}_1 = \{\Gamma_{1,1}, \Gamma_{1,2}\} \; cu \; \begin{array}{lcl} \Gamma_{1,1} & = & \{\{P_1, P_2\}\} \\ \Gamma_{1,2} & = & \{\{P_2, P_3\}, \{P_3, P_4\}\} \end{array}$$

şi

$$\mathcal{D}_2 = \{\Gamma_{2,1}, \Gamma_{2,2}\} \; cu \; \begin{array}{lcl} \Gamma_{2,1} & = & \{\{P_1, P_2\}, \{P_2, P_3\}\} \\ \Gamma_{2,2} & = & \{\{P_3, P_4\}\} \end{array}$$

Aceste descompuneri corespund lui K_2 şi $K_{1,2}$, deci sunt descompuneri ideale. Ambele oferă o rată de informaţie $\rho = 1/2$. Dacă le vom combina conform Teoremei 4.10 cu $s = 2$, vom obţine o rată de informaţie maximă $\rho = 2/3$.

Luând ca bază Teorema 4.8, putem obţine efectiv un astfel de sistem. D alege aleator patru elemente $b_{1,1}, b_{1,2}, b_{2,1}, b_{2,2} \in Z_q$. Pentru o cheie $S = (S_1, S_2) \in Z_q \times Z_q$, arbitrul va distribui componentele astfel:

1. *P_1 primeşte $\{b_{1,1},\ b_{2,1}\}$;*
2. *P_2 primeşte $\{b_{1,1} + S_1,\ b_{1,2},\ b_{2,1} + S_2\}$;*
3. *P_3 primeşte $\{b_{1,2} + S_1,\ b_{2,1},\ b_{2,2}\}$;*
4. *P_4 primeşte $\{b_{1,2},\ b_{2,2} + S_2\}$.*

(toate calculele sunt efectuate în Z_q).

Exemplul 4.23. *Fie structura de acces 8 din Tabelul 4.1. Vom considera $\mathcal{K} = Z_q$ pentru un număr prim $q \geq 3$. Vom utiliza două $\mathcal{K}$ - descompuneri ideale*

$$\mathcal{D}_1 = \{\Gamma_{1,1}, \Gamma_{1,2}\} \; cu \; \begin{array}{lcl} \Gamma_{1,1} & = & \{\{P_1, P_2\}\} \\ \Gamma_{1,2} & = & \{\{P_2, P_3\}, \{P_2, P_4\}, \{P_3, P_4\}\} \end{array}$$

şi

$$\mathcal{D}_2 = \{\Gamma_{2,1}, \Gamma_{2,2}\} \; cu \; \begin{array}{lcl} \Gamma_{2,1} & = & \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_2, P_4\}\} \\ \Gamma_{2,2} & = & \{\{P_3, P_4\}\} \end{array}$$

$\mathcal{D}_1$ corespunde lui K_2 şi K_3, iar $\mathcal{D}_2$ – lui K_2 şi $K_{1,3}$; deci ambele sunt $\mathcal{K}$ - descompuneri. Aplicând Teorema 4.10 cu $s = 2$ se va obţine $\rho = 2/3$.
Similar exemplului precedent, o construcţie efectivă se realizează astfel:

D alege aleator patru elemente $b_{1,1}, b_{1,2}, b_{2,1}, b_{2,2} \in Z_q$.
Pentru o cheie $S = (S_1, S_2) \in Z_p^2$, el va distribui componentele astfel:

1. *P_1 primeşte $\{b_{1,1} + S_1,\ b_{2,1} + S_2\}$;*
2. *P_2 primeşte $\{b_{1,1},\ b_{1,2},\ b_{2,1}\}$;*
3. *P_3 primeşte $\{b_{1,2} + S_1,\ b_{2,1} + S_2,\ b_{2,2}\}$;*
4. *P_4 primeşte $\{b_{1,2} + 2S_1,\ b_{2,1} + S_2,\ b_{2,2} + S_2\}$.*

(toate calculele sunt efectuate în Z_q).

4.8 Scheme de partajare fără arbitru

Există posibilitatea ca un anumit secret să fie partiţionat fără a face apel la arbitru. Este o situaţie care apare frecvent în protocoale de partajare de chei. Evident, în acest caz, secretul va fi considerat implicit şi va fi aflat doar atunci când este reconstituit de o mulţime autorizată de acces.

Ideea construirii unei astfel de partajări de secrete apare prima oară în lucrarea lui C. Meadows ([55]), dar o schemă funcţională este propusă de Ingermarsson şi Simmons în [42]. Aici, utilizatorul P_i alege un număr S_i care va fi una din cele n componente ale unui secret S, pe care îl partajează pentru ceilalţi utilizatori. Se obţine astfel o schemă de partajare $(n, n-1)$ - majoritară.

1. Fiecare participant P_i alege un număr aleator $S_i \in Z_q$ (q număr prim fixat şi public);
2. P_i generează aleator componentele $S_{i,j}$ astfel ca
$$S_i = \sum_{(j=1)\&(j\neq i)}^{n} S_{i,j} \quad (mod\ q)$$
3. P_i trimite fiecărui participant P_j $(1 \leq j \leq n, \ \ j \neq i)$ componenta $S_{i,j}$.

Deci, fiecare participant P_i va dispune de componenta

$$(S_i, S_{1,i}, \ldots, S_{i-1,i}, S_{i+1,i}, \ldots, S_{n,i})$$

Să presupunem că primii $n-1$ participanţi vor să recompună secretul. Ei vor calcula

$$S = \sum_{i=1}^{n-1} S_i + \sum_{i=1}^{n-1} S_{n,i} = \sum_{i=1}^{n-1} S_i + S_n = \sum_{i=1}^{n} S_i = S \quad (mod\ q)$$

Jackson, Martin şi O′ Keefe generalizează această schemă ([43]) la o mulţime de acces arbitrară $\mathcal{A}$.

1. Se foloseşte o schemă unanimă de ordin k pentru a construi componentele $S_1, \ldots, S_k$ ale unui secret S;
2. Utilizatorul P_i $(1 \leq i \leq k)$ împarte S_i (considerat ca un secret al cărui arbitru este) în componente, pentru o mulţime de acces $\mathcal{A}_i$, apoi împarte aceste componente utilizatorilor din $\mathcal{A}_i$.

Pentru construcţia mulţimilor de acces $\mathcal{A}_i$ se procedează în modul următor:

- Se ia mulţimea $\mathcal{A} \cup \{\{P_1\}\}$ şi se consideră baza ei; fie $\mathcal{A}_{1,min}$ această bază;
- $\mathcal{A}_1$ este mulţimea de acces generată de $\mathcal{A}_{1,min}$;

- Pentru $i = 2, \ldots, k$:
  - Se elimină utilizatorii $P_1, \ldots, P_{i-1}$ din $\mathcal{P}$; fie $\mathcal{A}'$ noua mulţime de acces;
  - Se construieşte $\mathcal{A}' \cup \{\{P_i\}\}$ şi se determină baza ei: $\mathcal{A}_{i,min}$;
  - $\mathcal{A}_i$ este mulţimea de acces generată de $\mathcal{A}_{i,min}$.

Exemplul 4.24. *Să construim o schemă de partajare* $(4, 3)$ *- majoritară, fără arbitru, pentru mulţimea de acces având baza*

$$\mathcal{A}_{min} = \{\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3, P_4\}\}$$

Cele trei baze sunt:

$$\mathcal{A}_{1,min} = \{\{P_1\}, \{P_2, P_3, P_4\}\}, \quad \mathcal{A}_{2,min} = \{\{P_2\}, \{P_3, P_4\}\}, \quad \mathcal{A}_{3,min} = \{\{P_3\}, \{P_4\}\}$$

Utilizatorul P_1*:*

1. *Generează aleator* S_1*;*
2. *Construieşte – cu un algoritm de partajare majoritară – componentele* $S_{1,2}, S_{1,3}, S_{1,4}$ *ale secretului* S_1*;*
3. *Distribuie* $S_{1,j}$ *participantului* P_j $(j = 2, 3, 4)$.

Utilizatorul P_2*:*

1. *Generează aleator* S_2*;*
2. *Construieşte – cu un algoritm de partajare majoritară – componentele* $S_{2,3}, S_{2,4}$ *ale secretului* S_2*;*
3. *Distribuie* $S_{2,j}$ *participantului* P_j $(j = 3, 4)$.

Utilizatorul P_3*:*

1. *Generează aleator* S_3*;*
2. *Trimite* $S_{3,4} = S_3$ *participantului* P_4.

Deci,secretul este $S = S_1 + S_2 + S_3$ *cu* $S_1 = S_{1,2} + S_{1,3} + S_{1,4}$, $S_2 = S_{2,3} + S_{2,4}$, $S_3 = S_{3,4}$ *şi*
P_1 *deţine* $\{S_1\}$,
P_2 *deţine* $\{S_2, S_{1,2}\}$
P_3 *deţine* $\{S_3, S_{1,3}, S_{2,3}\}$,
P_4 *deţine* $\{S_{1,4}, S_{2,4}, S_{3,4}\}$.

Dacă – de exemplu – mulţimea autorizată de acces $\{P_1, P_3, P_4\}$ *vrea să găsească secretul, va calcula*

$$S = S_1 + S_3 + S_{2,3} + S_{2,4}$$

4.9 Scheme de partajare verificabile

În toate schemele prezentate până acum s-a presupus că părţile implicate (arbitrul şi participanţii) se comportă onest. Cazul când arbitrul D trişează este studiat prima oară de Chor, Goldwasser, Micali şi Awerbuch ([20]); ei introduc şi noţiunea de *schemă de partajare verificabilă*, unde fiecare participant poate verifica dacă primit o componentă validă.

4.9.1 Schema de partajare a lui Feldman

P. Feldman propune în [31] o schemă de verificare a sistemului de partajare Shamir. Aceasta este:

1. Se generează numerele prime p, q astfel ca $q|(p-1)$; fie $\alpha \in Z_p^*$ un element de ordin q. Toate aceste valori sunt publice;
2. D generează polinomul
$$a(X) = a_0 + a_1X + \ldots + a_{k-1}X^{k-1} \in Z_q[X]$$
cu $a_0 = S$; face publice elementele $\alpha_i = \alpha^{a_i}\ (mod\ p), \quad (0 \le i \le k-1)$;
3. D distribuie (prin canal securizat) către fiecare participant P_i componenta $S_i = a(i) \quad (i = 1, \ldots, n)$;

Fiecare participant verifică corectitudinea componentei primite S_i testând dacă are loc egalitatea
$$\alpha^{S_i}\ (mod\ p)\ =\ \prod_{j=0}^{k-1} \alpha_j^{i^j}\ (mod\ p)$$

Observaţia 4.5. *Schema lui Feldman poate fi construită pe un caz general, utilizând o funcţie homomorfă*[7] f. *Elementele* $f(a_0), f(a_1), \ldots, f(a_{k-1})$ *sunt publice, iar consistenţa componentei* S_i *se verifică pe baza egalităţii*
$$f(S_i) = f(a_0) \cdot f(a_1)^{i^1} \ldots f(a_{k-1})^{i^{k-1}}$$
Sistemul prezentat mai sus a folosit funcţia $f : Z_q \longrightarrow Z_p, \quad f(x) = \alpha^x\ (mod\ p)$, *cu* p, q *numere prime,* $q|(p-1)$ *şi* $\alpha \in Z_p^*$ *de ordin* q.

[7] O funcţie homomorfă are proprietatea $(\forall x, y)\ \ f(x+y) = f(x) \cdot f(y)$.

4.9.2 Schema lui Pedersen

Schema lui Feldman are dezavantajul că valoarea α^S este publică, şi deci confidenţialitatea secretului depinde direct de problema logaritmului discret. Pentru a elimina această (posibilă) falie, Pedersen propune următoarea variantă, relativă tot la sistemul de partajare Shamir:

1. Se generează numerele prime p, q cu $q|(p-1)$ şi elementele $g, h \in Z_p^*$ de ordin q. Toate aceste numere sunt publice;
2. Arbitrul D calculează $E_0 = g^S h^t \ (mod\ p)$ unde $t \in Z_q$ este ales arbitrar;
3. D generează polinoamele

$$\begin{array}{l} a(X) = S + a_1X + \ldots + a_{k-1}X^{k-1} \in Z_[X], \\ b(X) = t + b_1X + \ldots + b_{k-1}X^{k-1} \in Z_q[X], \end{array}$$

   calculează valorile $E_i = g^{a_i} h^{b_i} \ (mod\ p)$ şi face public vectorul $(E_0, E_1, \ldots, E_n)$;
4. D distribuie (prin canal securizat) către fiecare participant componenta

$$S_i = (a(i), b(i)), \quad i = 1, \ldots, n$$

Fiecare utilizator P_i poate testa corectitudinea componentei $S_i = (s_i, t_i)$ primite, verificând egalitatea

$$g^{s_i} h^{t_i} = \prod_{j=0}^{k-1} E_j^{i^j} \ \ (mod\ p)$$

Schema Pedersen are proprietăţi de liniaritate: astfel, dacă secretele A_1, A_2 sunt definite prin componentele $(s_{i,j}, t_{i,j})$, $i = 1, \ldots, n$, $j = 1, 2$, atunci, pentru orice valori $a_1, a_2 \in Z_p$ secretul $a_1A_1 + a_2A_2$ este definit de componentele

$$(a_1 \cdot s_{i,1} + a_2 \cdot s_{i,2}), \quad i = 1, 2, \ldots, n$$

toate calculele fiind efectuate în Z_q.

Această facilitate permite unele aplicaţii interesante în domenii adiacente, cum sunt gestiunea cheilor sau protocoale de vot electronic.

4.9.3 Scheme de partajare verificabile public

Schemele verificabile prezentate până acum permiteau doar participanţilor să îşi verifice corectitudinea propriilor componente primite. Este însă posibil să se solicite ca această

verificare să fie publică, putând fi efectuată de orice persoană interesată.
Prezentăm o astfel de schemă ([76]), propusă de Stadler în 1996 sub o formă generală:

1. Componentele corespunzătoare unui secret S sunt criptate de arbitrul D folosind cheile publice ale participanţilor, Aceste elemente
$$ES_i = e_{K_i}(S_i), \quad (1 \le i \le n)$$
sunt publice.
2. Se foloseşte un algoritm public $PubVerify$ pentru a testa validitatea componentelor criptate. Astfel, dacă pentru o mulţime de acces $A \in \mathcal{A}_{min}$ avem $PubVerify(\{ES_i \mid P_i \in A\}) = 1$, atunci participanţii din A pot – după ce decriptează componentele – să recompună secretul S.

Sunt diverse protocoale propuse pentru construirea algoritmilor $PubVerify$; majoritatea lor sunt de tipul *(Provocare, Răspuns)* şi vor fi studiate în Capitolul 7.

4.10 Exerciţii

4.1. *Construiţi o* $(5,3)$ *- schemă de partajare Shamir peste* Z_{29}*, folosind polinomul de interpolare* $a(X) = 11X^2 + X + 18$ *şi cheile secrete* $x_i = 3^i \pmod{29}, \ \ i = 1, \ldots, 5$.

Recompuneţi secretul pentru mulţimea $\{P_2, P_3, P_5\}$.

4.2. *Se dă secvenţa* $7, 9, 11, 12, 13, 15, 17, 19$.

1. *Pentru ce valori ale lui* k *ea este un şir* $(7, k)$ *- Mignotte ?*
2. *Pentru fiecare astfel de* k*, să se construiască o schemă Mignotte de partajare a secretului* $S = \lfloor(\beta - \alpha)/2\rfloor$.

4.3. *Folosind graful multipartit complet* $K_{2,3,3}$ *şi valorile* $q = 13, \ r = 5, \ x_1 = 1, \ x_2 = 2, \ x_3 = 3$*, să se construască o schemă de partajare pentru secretul* $S = 8$.

4.4. *Construiţi o schemă perfectă de partajare pentru structura de acces:*
$$\mathcal{A} = \{\{P_1\}, \{P_2, P_3\}, \{P_2, P_4, P_5\}, \{P_3, P_4, P_5\}\}$$

4.5. *Să se construiască circuite monotone pentru structurile de acces din exerciţiul anterior.*

4.6. *Construiţi sisteme de partajare perfecte cu rata de informaţie* $\rho = 1/2$*, folosind metoda circuitelor monotone, pentru structurile de acces ale căror baze sunt;*

1. $\mathcal{A}_{min} = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_2, P_4\}, \{P_3, P_4\}\}$.

2. $\mathcal{A}_{min} = \{\{P_1, P_3, P_4\}, \{P_1, P_2\}, \{P_2, P_3\}, \{P_2, P_4\}\}$.

3. $\mathcal{A}_{min} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_2, P_3, P_4\}, \{P_2, P_4, P_5\}, \{P_3, P_4, P_5\}\}$.

4.7. *Construiţi sisteme de partajare perfecte folosind schema Brickell, pentru structurile de acces ale căror baze sunt:*

1. $\mathcal{A}_{min} = \{\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_3, P_4\}\}$.

2. $\mathcal{A}_{min} = \{\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}\}$.

3. $\mathcal{A}_{min} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_3\}, \{P_1, P_4, P_5\}, \{P_2, P_4, P_5\}\}$.

4.8. *Construiţi sisteme perfecte de partajare a secretelor pentru structurile de acces* 15 *şi* 16 *din Tabelul 4.1.*

4.9. *Folosind metoda descompunerilor, construiţi sisteme perfecte de partajare cu rata de informaţie specificată, pentru structurile de acces având bazele:*

1. $\mathcal{A}_{min} = \{\{P_1, P_3, P_4\}, \{P_1, P_2\}, \{P_2, P_3\}\}, \ \rho = 3/5$.

2. $\mathcal{A}_{min} = \{\{P_1, P_3, P_4\}, \{P_1, P_2\}, \{P_2, P_3\}, \{P_2, P_4\}\}, \ \rho = 4/7$.

Bibliografie

[1] C. A. Asmuth, J. Bloom – *A modular approach to key safeguarding*, IEEE Trans on IT 29 (1983), pp. 208-210.

[2] Atanasiu, A. – *Securitatea Informaţiei, vol. 1, Criptografie*, ed. InfoData, Cluj, 2008.

[3] D. Bayer, S.Haber, W.Stornetta – *Improving the efficiency and reliability of digital time-stamping. Sequences II*, Methods in Communication, Security and Computer Science, Springer Verlag (1993), 329-334.

[4] J. Benaloh – *Verifiable sectret-ballot elections*, Ph.D thesis, Yale University, Technical report 561, 1987.

[5] J. Benaloh, J. Leichter – *Generalized secret sharing and monotone functions*, în "Advances in Cryptology – CRYPTO 8", S. Goldwasser, ed., LNCS 403 (1989), pp. 27-35.

[6] S. Blake - Wilson, A. Menezes – *Authenticated Diffie - Hellman Key Agreement Protocols*, Proc. of the 5-th Intern. Workshop on Security Protocols, LNCS 1361, 1997, pp. 137-158.

[7] G. R. Blakley – *Safeguarding cryptographic keys*, în "Proc. of the National Computer Conference, 1979", American Federation of Information Processing Societies Proc. 48 (1979), pp. 313-317.

[8] Boneh, D., Franklin, M. – *Identity Based Encryption from the Weil Pairing*, SIAM Journal of Computing, vol. 32, no. 3, pp. 586-615.

[9] Boneh, D., Boyen, X. – *Efficient Selective - ID Secure Identity Based Encryption Without Random Oracles*, Proc. of EUROCRYPT 2004, Interlaken, Elveţia, 2-6 May 2004, pp. 223-238.

[10] J. N. Bos, D. Chaum - *Provably unforgable signatures*, LNCS, 740 (1993), pp. 1-14.

[11] S. Brands – *An Efficient Off-Line Electronic Cash System Based On The Representation Problem*, Technical Report CS-R9323, 1993, CWI, Amsterdam, Netherlands.

[12] D. Chaum – *Untraceable electronic mail, return addresses, and digital pseudonyms*, Commun. ACM, 24 (2), 1981, pp. 8490.

[13] D. Chaum, H. van Antwerpen – *Undeniable signatures*, LNCS, 435 (1990), pp. 212-216.

[14] D. Chaum, A. Fiat, M. Naor – *Untraceable Electronic Cash*, Advances in Cryptology, CRYPTO 8, S. Goldwasser (Ed.), Springer-Verlag, pp. 319-327.

[15] D. Chaum, E. van Heyst – *Group signatures*, Advances in Cryptology, EUROCRYPT 91, LNCS, vol. 547, Springer-Verlag (1991), pp. 257-265.

[16] D. Chaum, E. van Heijst, B. Pfitzmann – *Cryptographically strong undeniable signatures, unconditionally secure for the signer*, LNCS, 576 (1992), pp. 470-484.

[17] Chen, L. ş.a – *An Efficient ID-KEM Based on the Sakai-Kasahara Key Construction*, IEEE Proc. Information Theory, vol. 153, no. 1, (2006), pp. 19-26.

[18] T-S Chen, K-H Huang, Y-F Chung – *Digital Multi - Signature Scheme based on the Elliptic Curve Cryptosystem*, J. Comp. Sci & Technol. vol. 19 (2004), no. 4, pp. 570-573.

[19] X. Chen, F. Zang, K. Kim – *A new ID - based group signature scheme from bilinear pairings*, $http://eprint.iacr.org/2003/100.pdf$, 2003.

[20] B. Chor, S. Goldwasser, S. Micali, B. Awerbuch – *Verifiable secret sharing and achieving simultaneity in the presence of faults*, Proc. of the 26th IEEE Symposium on the Foundations of Computer Science, (1985), pp. 383-395

[21] Cocks, C. – *an Identity Based Encryption Scheme Based on Quadratic Residues*, Proc. of the Eighth IMA Intern. Conf. on Cryptography and Coding, Cirencester, 17-19 Dec. 2001, pp. 360-363.

[22] J.S. Coron, D. Naccache, J. Stern – *On the security of RSA Padding*, In Advances of Cryptology CRYPTO 99, LNCS 1666, Springer - Verlag, 1999, pp. 1-18.

[23] R. Cramer, R. Gennaro, B. Schoenmakers – *A secure and optimally efficient multi-authority election scheme*, în EUROCRYPT 1997, pp. 103 118.

[24] I.B. Damgard –*A design principle for hash functions*, LNCS, 435 (1990), pp. 516-427.

[25] H. Delfs, H. Knebl – *Introduction to Cryptography, Second edition*, Springer Verlag, 2007.

[26] W. Diffie, M.E. Hellman – *Multiuser cryptographic techniques*, AFIPS Conference Proceedings, $45(1976), 109 - 112$

[27] W. Diffie, M.E. Hellman – *New Directions in Cryptography*, IEEE Trans. on Information Theory, vol. IT-22 (1976), pp 644-654

[28] H. Dobbertin – *Cryptanalysis of MD4*, Journal of Cryptology, 11 (1998), pp. 253-271.

[29] T. ElGamal – *A public key cryptosystem and a signature scheme based on discrete algorithms*, IEEE Trans. on Information Theory, 31 (1985), pp. 469-472.

[30] M. J. Farsi – *Digital Cash*, Masters Thesis in Computer Science, Dpt of Mathematics and Computing Science, Goteborg University 1997.

[31] P. Feldman – *A practical scheme for non-interactive verifiable secret sharing*, Proc. of the 28th IEEE Symposium on the Foundations of Computer Science, (1987), pp. 427-437.

[32] N. Ferguson – *Single Term Off-Line Coins*, Advances in Cryptology - EUROCRYPT 93, Springer-Verlag, pp. 318-328.

[33] A. Fujioka, T. Okamoto, K. Ohta – *A practical secret voting scheme for large scale elections*, în J. Seberry şi Y. Zheng, (eds), ASIACRYPT, LNCS 718 (1992), pp. 244251.

[34] E. Fujisaki, T. Okamoto – *Secure Integration of Assymetric and Simmetric Encryption Schemes*, Proc. of Crypto 99, Santa Barbara, CA, August 20-24, 1999, pp. 537-554.

[35] S. Galbraith – *Pairings*, în "Advances in Elliptic Curve Cryptography" ed. T. Blake, G. Seroussi şi N. Smart; London Math. Society, Lecture Notes Series 317 (2005), pp. 183-214.

[36] T. El Gamal – *A public key cryptosystem and a signature scheme based on discrete algorithms*, IEEE Trans on Inf. Theory, 31 (1985), pp. 469-472.

[37] J. Gibson – *Discrete logarithm hash function that is collision free and one way*, IEEE Proceedings-E, 138 (1991), 407-410.

[38] H. Ghodosi, J. Pieprzyk, Safavi-Naini – *Remarks on the multiple assignment secret sharing scheme*, LNCS 1334 (1997), 72-82.

[39] S. Haber, W. Stornetta; How to timestamp a digital document. Journal of Cryptology, 3(1991), 99-111.

[40] E. van Heyst, T.P.Petersen – *How to make efficient fail-stop signatures*, LNCS, 658 (1993), 366-377.

[41] S. Iftene – *A generalisation of Mignottes secret sharing scheme*, în Proc. of the 6th Intern. Symposium on Symbolic and Numeric Algorithms for scientific computing, Timişoara, T. Jebelean, V. Negru, D. Petcu, D. Zaharia (eds), Sept. 2004, pp. 196-201, Mirton Publ. House (2004).

[42] I. Ingermarsson, G. D. Simmons – *A protocol to set up shared secret schemes without assistance of mutually trusted party*, EUROCRYPT 90, LNCS vol. 473, Springer - verlag 1991, pp. 266-282

[43] W. Jackson, K.M. Martin, C. M. O′ Keefe – *Muttualy trusted authority - free secret sharing schemes*, Journal of Cryptology, 10 (4), 1997, pp. 261-289.

[44] E. D. Karnin, J. W. Greene, M. E. Hellman – *On secret sharing systems*, IEEE Trans. on Information Theory 29 (1983), pp. 35-41.

[45] V. Klima – *Tunnels in Hash Functions: $MD5$ Collisions within a Minute*, Cryptology ePrint Archive, http://eprint.iacr.org, Report 105 (2006).

[46] Klitz, E. – *On the Limitations of the Spread of an IBE-to-PKE Transformation*, Proc of PKC 2006, LNCS 3958, Springer, 2006, pp. 274-289.

[47] H. Krawczyk, M. Bellare, R. Canetti – *HMAC: Keyed - Hashing for Message Authentication*, RFC 2104, 1997.

[48] E. Kranakis – *Primality and Cryptography*, Wiley-Teubner Series in Computer Science (1986).

[49] H. Krawczyk – *Secret sharing made short*, în Advances in Cryptology – CRYPTO 93, D. R. Stinson, ed., LNCS 773 (1994), pp. 136-146.

[50] L. Law, S. Sabett, J. Solinas – *How to make a mint: The Cryptography of Anonymous Electronic Cash*, http://jya.com/nsamint.htm

[51] C.I. Lei, C.I. Fan – *A universal single-authority election system*, IEICE Transactions on Fundamentals E81-A (10) (1998), 2186-2193

[52] Mambo, Masahiro, Keisyke, Usuda, Okamoto – *Proxy signatures: Delegation of the power to sign mesages*, IEICE Trans. Fundamentals, ET9-A (1996), pp. 1338 - 1354.

[53] Martin, L – *Introduction to Identity – Based Encryption*, Artech House, Information Security and Privacy Series, 2008.

[54] T. Matsumoto, Y. Takashima, H. Imai – *On seeking smart public-key distribution systems*, The Trans. of the IECE of Japan, E69 (1986), pp. 99-106.

[55] C. Meadows – *Some threshold schemes without central key distributors*, Congressus Numerantium, 46 (1985), pp. 187-199.

[56] R. J. McEliece, D. Sarwate – *On sharing secrets and Reed-Solomon codes*, Comm. of the ACM 24 (1981), pp. 583-584.

[57] A. Menezes, P. van Oorschot, S. Vanstome – *Handbook of Applied Cryptography*, CRC Press Inc (1997)

[58] R.C. Merkle – *A fast software one-way functions and DES*, LNCS, 435 (1990), pp. 428-446.

[59] M. Mignotte – *How to share a secret*, în Cryptography Proc., Burg Feuerstein 1982, T. Beth, ed., LNCS 149 (1983), pp. 371-375.

[60] C. J. Mitchell, F. Piper, P. Wild – *Digital signatures*, Contemporary Cryptology, The Science of Information Integrity, IEEE Press, (1992), pp. 325-378.

[61] Y.Mu, V. Varadharajan – *Anonymous e-voting over a network*, Proc. of the 14th Annual Computer Security Applications Conference, ASAC8 (1998) 293-299

[62] R. Needham, M. Schroeder – *Using encryption for authentication in large networks of computers.*, Comm. of the ACM 21, 12 (1978), pp. 993 999.

[63] A. M. Odlyzco – *Cryptanalytic attacks on the multiplicative knapsack cryptosystems and on Shamirs fast signature scheme*, IEEE Trans. on Information Theory, IT30 (1984), pp. 594-601.

[64] T. Okamoto – *Receipt - free electronic voting scheme for large scale elction*, Proc. of Workshop on Security Protocols, LNCS 1361 (1997).

[65] T. Okamoto, K. Ohta – *Universal electronic cash*, J. Feigenbaum (Ed.), Advances in cryptology CRYPTO91, LNCS 576, Springer-Verlag (1992).

[66] B. Preneel, R. Govaerts, J. Vandewalle – *Hash functions based on block ciphers: a syntetic approach*, LNCS, 773 (1994), pp. 368-378.

[67] M.O. Rabin – *Efficient dispersal of information for security, load balancing, and fault tolerance*, Journal of ACM, 36(2), 1989, pp. 335-348.

[68] R.L. Rivest – *The $MD4$ message digest algorithm*, LNCS, 537, (1991), pp. 303-311.

[69] R. L. Rivest – *The $MD5$ Message Digest Algorithm*, RFC 1321 (1992).

[70] A. Salomaa – *Criptografie cu chei publice*, Ed. Militară, 1994.

[71] B. Schoenmakers – *A simple publicly verifiable secret sharing scheme and its application to electronic voting*, Advanced in Cryptology, LNCS 1666 (1999), pp. 148-164.

[72] A. Shamir – *Identity-Based Cryptosystems and Signature Schemes*, Proc. of CRYPTO 84, Santa Barbara, CA. August 19-22, 1984, pp. 47-53.

[73] A. Shamir – *How to share a secret*, Comm of the ACM 22 (1979), 612-613.

[74] G.J. Simmons – *The prisoners problem and the subliminal channel*, Advances in Cryptology - Crypto, 83 (1984), pp. 51-67.

[75] M. E. Smid, D. K. Branstad – *Response to comments on the NIST proposed digital signature standard*, LNCS, 740 (1993), pp. 76-88.

[76] M. Stadler – *Publicly verifiable secret sharing*, Advances in Cryptology - EUROCRYPT 96, LNCS vol. 1070, Springer verlag (1996), pp. 190-199.

[77] D. R. Stinson – *Decomposition constructions for secret sharing schemes*, IEEE Trans. on Information Theory 40 (1994), pp. 118-125.

[78] D. Stinton – *Cryptographie, theorie et pratique*, Intern. Thompson Publ. France, 1995.

[79] Z. Tan, Z. Liu, C. Tan – *Digital proxy Blind Signature Schemes based on DLP and ECDLP*, MM Research Preprints, 212-217, Academia Sinica, Beijing, no. 21, Dec. 2002.

[80] S. Vaudenay – *A Classical Introduction to Cryptography*, Springer Verlag 2006.

[81] H.C.Williams – *Some public-key criptofunctions as intractable as factorisation*, Cryptologia, 9 (1985), pp. 224-237.

[82] *ISO/IEC* 9796; Information technology – Security Techniques – Digital Signature Scheme Giving message recovery, Intern. Organisation for Standardisation, Geneva, 1991.

[83] *Secure Hash Standard*, National Bureau of Standards, FIPS Publications 180, 1993.

[84] *SKIPJACK and KEA Algorithm Specifications*, versiunea 2.0, http://csrc.nist.gov/groups/ST/toolkit/documents/skipjack/skipjack.pdf

[85] *Digital signature standard*, National Bureau of Standards, FIPS Publications 186, 1994

Index