Prelegerea 5

Sisteme de partajare a secretelor

5.1 Sistemul confidenţial al lui Shamir

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.

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

Să prezentăm întâi un sistem de partajare a secretului numit *sistem confidenţial*.[1]

Definiţia 5.1 *Fie t, w două numere întregi pozitive, $t \leq w$. Un sistem confidenţial (t, w) este o metodă de partajare a unei chei K între membrii unei mulţimi $\mathcal{P}$ de w participanţi, astfel ıncât orice asociere de t participanţi să poată calcula K, lucru imposibil pentru asocieri de $t-1$ sau mai puţini participanţi.*

Exemplul precedent este deci un sistem confidenţial $(2, 3)$.

Valoarea lui K este aleasă de un *arbitru*[2] D. Vom presupune că $D \notin \mathcal{P}$. D va distribui în secret componente ale cheii membrilor grupului $\mathcal{P}$, astfel încât nici un participant să nu cunoască componentele celorlalţi şi nici să fie capabil ca din componenta sa să poată recompune cheia K.

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

Să notăm

$$\mathcal{P} = \{P_i \mid 1 \leq i \leq w\}$$

mulţimea celor w participanţi. $\mathcal{K}$ este spaţiul tuturor cheilor posibile, iar $\mathcal{S}$ este spaţiul componentelor (toate componentele posibile ale cheii).

Sistemul prezentat în această secţiune este datorat lui Shamir şi a fost creat în 1979. Fie p $(p \geq w + 1)$ un număr prim şi $\mathcal{K} = Z_p$, $\mathcal{S} = Z_p$. Deci cheile şi componentele sunt numere din Z_p. Sistemul confidenţial al lui Shamir, prezentat mai jos, se bazează pe un polinom aleator

[1] *Threshold scheme* în engleză, *a seuil* în franceză.

[2] *Dealer* în engleză, *initiateur* în franceză.

$a(X)$ de grad cel mult $t-1$, în care termenul liber este K. Fiecare participant P_i află un punct (x_i, y_i) de pe graficul acestui polinom.

1. (Iniţializare): D alege w elemente distincte $x_1, \ldots, x_w \in Z_p$ (x_i publice), fiecare x_i fiind comunicat lui P_i.
2. Să presupunem că D doreşte să repartizeze cheia $K \in Z_p$. D va selecta aleator $t-1$ elemente $a_1, \ldots, a_{t-1} \in Z_p$ şi construieşte polinomul
$$a(X) = K \sum_{j=1}^{t-1} a_j X^j \quad (mod\ p).$$
3. D calculează $y_i = a(x_i)$ şi comunică această valoare lui P_i $(1 \leq i \leq w)$.

Fie acum o submulţime $\{P_{i_1}, \ldots, P_{i_t}\}$ de participanţi care doresc să reconstituie cheia. Ei ştiu valorile x_{i_j} şi $y_{i_j} = a(x_{i_j})$ pentru $1 \leq j \leq t$; $a(X) \in Z_q[X]$ este polinomul (secret) folosit de D. Cum gradul lui este cel mult $t-1$, putem scrie
$$a(X) = a_0 + a_1 X + \ldots + a_{t-1} X^{t-1}$$
unde $a_0 = K$ iar $a_0, \ldots, a_{t-1} \in Z_q$ sunt necunoscute. Ele se află rezolvând sistemul liniar de t ecuaţii $y_{i_j} = a(x_{i_j})$. Dacă ecuaţiile sunt independente, soluţia este unică, iar valoarea lui a_0 este chiar cheia K.

Exemplul 5.1 *Să presupunem $p = 17$, $t = 3$, $w = 5$, iar $x_i = i$, $(1 \leq i \leq 5)$. Dacă $B = \{P_1, P_3, P_5\}$ vor să afle cheia aducând fiecare informaţiile 8, 10 şi respectiv 11, ei vor scrie polinomul general $a(X) = a_0 + a_1 X + a_2 X^2$ şi vor reduce problema la rezolvarea în Z_{17} a sistemului liniar*

$$\begin{cases} a(1) &=& a_0 + a_1 + a_2 &=& 8 \\ a(3) &=& a_0 + 3a_1 + 9a_2 &=& 10 \\ a(5) &=& a_0 + 5a_1 + 8a_2 &=& 11 \end{cases}$$

Acesta admite soluţia unică în Z_{17} : $a_0 = 13,\ a_1 = 10,\ a_2 = 2$.

Deci valoarea căutată este $K = 13$.

Teorema 5.1 *Într sistemul confidenţial al lui Shamir, orice mulţime B de t participanţi poate reconstitui în mod unic cheia K.*

Demonstraţie: Fie $a(X) = a_0 + a_1 X + \ldots + a_{t-1} X^{t-1}$ polinomul ales de D, unde $a_0 = K$. Afirmaţia se reduce la a arăta că sistemul de ecuaţii $y_{i_j} = a(x_{i_j})$ $(1 \leq j \leq t)$, de necunoscute $a_0, \ldots, a_{t-1}$, admite soluţie unică. Determinantul acestui sistem este

$$\begin{vmatrix} 1 & x_{i_1} & x_{i_1}^2 & \ldots & x_{i_1}^{t-1} \\ 1 & x_{i_2} & x_{2_1}^2 & \ldots & x_{i_2}^{t-1} \\ & & \ldots & & \\ 1 & x_{i_t} & x_{i_t}^2 & \ldots & x_{i_t}^{t-1} \end{vmatrix} = \prod_{1 \leq j < k \leq t} (x_{i_k} - x_{i_j}) \quad (mod\ p)$$

Deoarece toate numerele x_i sunt distincte, iar Z_p este corp, rezultă că acest produs este nenul, deci sistemul are totdeauna soluţie unică, iar a_0 este chiar cheia căutată. □

Ce se întâmplă dacă un grup de $t-1$ participanţi încearcă să calculeze cheia K ?

Dacă procedează conform algoritmului anterior, vor obţine un sistem de $t-1$ ecuaţii cu t necunoscute. Fie y_0 o valoare arbitrară a cheii K. Vom avea $y_0 = a_0 = a(0)$, care formează a t - a ecuaţie a sistemului. Acesta oferă de asemenea soluţie unică. Deci, pentru orice valoare $K \in Z_p$ există un polinom unic $a_K(X) \in Z_p[X]$ care verifică toate condiţiile:

$$y_{i_j} = a_K(x_{i_j}) \quad (1 \leq j \leq t-1), \qquad y_0 = a_K(0).$$

Rezultă că orice valoare a lui K este consistentă cu componentele deţinute de cei $t-1$ participanţi; asocierea lor nu oferă nici o informaţie suplimentară pentru aflarea cheii.

Mai există o modalitate de abordare a sistemului confidenţial al lui Shamir: folosind polinoamele de interpolare Lagrance. Acestea oferă o exprimare explicită a polinomului $a(X)$, sub forma

$$a(X) = \sum_{j=1}^{t} y_{i_j} \prod_{\substack{1 \leq k \leq t \\ k \neq j}} \frac{x - x_{i_k}}{x_{i_j} - x_{i_k}}.$$

Evident, acesta este un polinom de grad cel mult $t-1$, cu proprietatea $y_{i_j} = a(x_{i_j})$, $\forall j = 1, \ldots, t$. Cum un astfel de polinom este unic, rezultă că el este chiar polinomul căutat.

Un grup B de t participanţi poate calcula $a(X)$ pe baza acestei formule. De fapt, nici nu este nevoie se determine tot polinomul: este suficient să obţină $K = a(0)$. Deci, înlocuind în formulă pe X cu 0, avem

$$K = \sum_{j=1}^{t} y_{i_j} \prod_{\substack{1 \leq k \leq t \\ k \neq j}} \frac{x_{i_k}}{x_{i_k} - x_{i_j}}.$$

Dacă definim

$$b_j = \prod_{\substack{1 \leq k \leq t \\ k \neq j}} \frac{x_{i_k}}{x_{i_k} - x_{i_j}} \quad (1 \leq j \leq t),$$

aceste valori pot fi precalculate şi făcute publice de către arbitru. Cheia este atunci o combinaţie liniară de t componente:

$$K = \sum_{j=1}^{t} b_j y_{i_j}.$$

Exemplul 5.2 *Să revenim la Exemplul 5.1. Participanţii* $\{P_1, P_3, P_5\}$ *pot calcula* b_1, b_2, b_3*; se obţine (calculele sunt făcute modulo* 17*):*

$$b_1 = \frac{x_3 x_5}{(x_3 - x_1)(x_5 - x_1)} = 3 * 5 * (-2)^{-1} * (-4)^{-1} = 4.$$

Similar, $b_2 = 3$, $b_5 = 11$*. Cu componentele* 8, 10 *şi* 11*, cheia se determină imediat:*

$$K = 4 * 8 + 3 * 10 + 11 * 11 = 13 \pmod{17}$$

Această variantă oferă o simplificare a algoritmului Shamir pentru cazul $w = t$. Ea funcţionează pentru $\mathcal{K} = Z_m$, $\mathcal{S} = Z_m$ (m nu este obligatoriu număr prim şi – chiar mai mult – este posibil ca $m \leq w$). Noul algoritm este:

1. D alege aleator $t-1$ elemente $y_1, \ldots, y_{t-1} \in Z_m$;
2. D calculează $y_t = K - \sum_{i=1}^{t-1} y_i \pmod m$;
3. Fiecare element y_i este transmis în secret lui P_i $(1 \leq i \leq t)$.

Cei t participanţi pot determina cheia K pe baza formulei

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

Evident, $t-1$ participanţi nu pot obţine cheia K. Chiar dacă pun în comun componentele lor, ei pot determina valoarea $K-y$, 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 cheie. Acesta este deci un sistem confidenţial (t,t).

5.2 Structura de acces şi partaj a secretului general

În paragraful precedent am studiat situaţia când orice asociere de t participanţi din totalul de w poate calcula cheia. Vom restrânge aici această condiţie, specificând ce submulţimi de participanţi pot avea acces la cheie şi pentru ce submulţimi acest acces este interzis. Fie Γ o mulţime de submulţimi ale lui $\mathcal{P}$, fiecare din ele reprezentând o asociaţie autorizată să calculeze cheia K. Γ se numeşte *structură de acces*, iar submulţimile ei se numesc *submulţimi autorizate*.

Fie $\mathcal{K}$ o mulţime de chei şi $\mathcal{S}$ o mulţime de componente. Când arbitrul D doreşte să repartizeze o cheie $K \in \mathcal{K}$, el va distribui câte o componentă fiecărui participant, urmând ca ulterior, o submulţime de participanţi să încerce să determine K punând în comun componentele cunoscute de ei.

Definiţia 5.2 *Un sistem perfect de partajare a secretelor cu structura de acces Γ este un procedeu de partajare a secretului unei chei K peste o mulţime $\mathcal{P}$ de participanţi, astfel încât:*

1. *Orice submulţime autorizată $B \subseteq \mathcal{P}$ de participanţi poate reconstitui cheia din componentele cunoscute de ei;*
2. *Orice submulţime neautorizată $B \subseteq \mathcal{P}$ de participanţi nu posedă nici o informaţie despre valoarea lui K.*

Un sistem confidenţial (t,w) realizează structura de acces $\Gamma = \{B \subseteq \mathcal{P} \mid card(B) \geq t\}$. O asemenea structură de numeşte *structură confidenţială*. Conform paragrafului precedent, sistemul confidenţial al lui Shamir este perfect şi realizează o structură confidenţială.

Să studiem securitatea sistemelor de partajare a secretelor. Ca de obicei, nu se impune nici o restricţie asupra puterii de calcul a submulţimilor neautorizate.

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

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

În continuare vom presupune că orice structură de acces este monotonă.

Un element $B \in \Gamma$ este *minimal* dacă $\forall A \subset B \Longrightarrow A \notin \Gamma$. Vom nota cu Γ_0 mulţimea elementelor minimale din Γ. Se observă că această mulţime caracterizează complet Γ. Mai exact,

$$\Gamma = \{C \subseteq \mathcal{P} \mid \exists B \in \Gamma_0,\ B \subseteq C\}.$$

Spunem că Γ este *închiderea* lui Γ_0 şi notăm prin $\Gamma = \overline{\Gamma}_0$.

Exemplul 5.3 *Fie* $\mathcal{P} = \{P_1, P_2, P_3, P_4\}$ *şi* $\Gamma_0 = \{\{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3\}\}$. *Vom avea* $\Gamma = \{\{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3\}, \{P_1, P_2, P_3\}, \{P_2, P_3, P_4\}, \{P_1, P_2, P_3, P_4\}\}$.
Invers, fiind dat Γ*, se vede imediat că* Γ_0 *este mulţimea părţilor sale minimale.*

În cazul structurilor confidenţiale de acces, baza este mulţimea submulţimilor formate cu t participanţi.

5.3 Construcţia circuitelor monotone

Ideea din această secţiune aparţine lui Benaloh şi Leichter; ea 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 *circuit monoton*.

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

Vom nota

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

mulţimea participanţilor asociaţi în mulţimea B. Presupunând că circuitul $\mathbf{C}$ este monoton, vom avea

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

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

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

Fie Γ_0 o bază a lui Γ. Vom construi formula booleană (în forma normal disjunctivă)

$$\bigvee_{B \in \Gamma_0} \left(\bigwedge_{P_i \in B} P_i \right)$$

Fiecare clauză din această formă normală este legată printr-o poartă AND, iar disjunc-ţia finală corespunde unei porţi OR. Numărul total de porţi folosite este $card(\Gamma_0) + 1$.

Fie acum $\mathbf{C}$ un circuit monoton care recunoaşte Γ. Vom prezenta un algoritm care permite arbitrului D să construiască un sistem perfect de partajare a secretului cu structura de acces Γ. Vom folosi sistemul confidenţial (t, t) din paragraful anterior. Mulţimea cheilor este deci $\mathcal{K} = Z_m$.

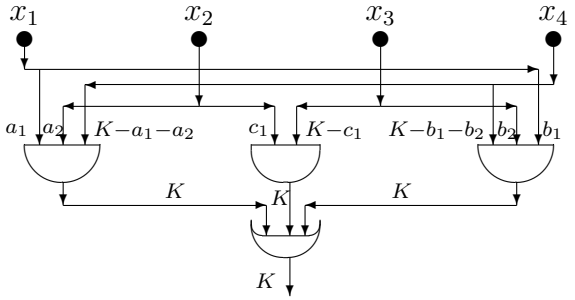
Algoritmul parcurge circuitul de la ieşire spre intrare, marcând recursiv cu $x_V \in \mathcal{K}$, fiecare arc V parcurs (în sens invers). Iniţial, arcului care marchează ieşirea y i se atribuie valoarea $x_{out} = K$ a cheii. Formal, algoritmul este:

1. $x_{out} \leftarrow K$;
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 $V_1, \ldots, V_t$ sunt arcele care intră în G, atunci
      i. Alege aleator $x_{V,1}, \ldots, x_{V,t-1} \in Z_m$;
      ii. Calculează $x_{V,t} = x - \sum_{i=1}^{t-1} x_{V,i} \pmod m$;
      iii. Marchează arcul V_i cu $x_{V,i}$, $(1 \leq i \leq t)$.

Exemplul 5.4 *Pentru mulţimea din Exemplul 5.3, avem* $\Gamma_0 = \{\{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3\}\}$*, 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, conforma algoritmului descris:



Aici $a_1, a_2, b_1, b_2, c_1, c_2$ *sunt numere alese aleator în* Z_m*. 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* $K - c_1$ *pentru* P_3*,*
4. $K - a_1 - a_2$ *şi* $K - b_1 - b_2$ *pentru* P_1*.*

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

Să vedem acum ce se întâmplă cu mulţimile neautorizate.

Ca o remarcă, dacă o mulţime B este neautorizată, orice submulţime a sa va fi de asemenea neautorizată.

Definiţia 5.3 *O mulţime* $B \subseteq \mathcal{P}$ *este maximal neautorizată dacă*

$$\forall B_1 \subset B \quad \Longrightarrow \quad B_1 \in \Gamma.$$

Este suficient deci de demonstrat că mulţimile maximal neautorizate nu pot afla cheia din informaţiile pe care le deţin.

Exemplul 5.5 *Revenind la exemplul anterior, mulţimile maximal 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 cheii* K *lipseşte o informaţie definită aleator. De exemplu,* $\{P_1, P_2\}$ *deţin informaţiile* a_1, a_2, b_1 *şi* c_1. *Pentru a reconstitui cheia* K *ar avea nevoie cel puţin de numărul* $K - a_1 - a_2$, *sau de* $K - c_1$.

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

Exemplul 5.6 *Să reluăm Exemplul 5.3 şi să rscriem 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 sistemul confidenţial corespunzător acestei expresii, vom avea următoarea distribuţie a componentelor (omitem detaliile):

1. P_1 *primeşte* a_1 *şi* a_2;
1. P_2 *primeşte* a_1, a_3 *şi* a_4;
1. P_3 *primeşte* a_2, a_3 *şi* $K - a_1 - a_2 - a_3 - a_4$;
1. P_4 *primeşte* a_4 *şi* $K - a_1 - a_2 - a_3 - a_4$;

Teorema 5.2 *Fie* $\mathbf{C}$ *un circuit boolean monoton. Construcţia sa generează un sistem perfect de partajare a secretului, a cărui structură de acces este* $\Gamma(\mathbf{C})$.

Demonstraţie: Vom folosi o recurenţă asupra numărului de porţi din circuitul $\mathbf{C}$. Cazul când $\mathbf{C}$ are o singură poartă este banal: dacă poarta este OR, fiecare participant conţine cheia K şi structura de acces este mulţimea tuturor părţilor nevide ale lui $\mathcal{P}$; dacă poarta este AND şi are t intrări, se obţine sistemul confidenţial (t, t) definit anterior.

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 considerăm cele t arce care intră în G : V_i $(1 \leq i \leq t)$. Acestea sunt arcele de ieşire din t circuite $\mathbf{C_i}$; conform ipotezei de inducţie, fiecare astfel de circuit defineşte un sub-sistem de partajare a secretului, cu structura de acces $\Gamma(\mathbf{C_i})$. Vom avea – evident

$$\Gamma(\mathbf{C}) = \bigcup_{i=1}^{t} \Gamma(\mathbf{C_i}).$$

Cum valoarea cheii 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,

$$\Gamma(\mathbf{C}) = \bigcap_{i=1}^{t} \Gamma(\mathbf{C_i}).$$

Deoarece K este repartizată peste toate arcele V_i conform unui sistem confidenţial (t, t), sistemul total va admite $\Gamma(\mathbf{C})$ drept structură de acces. □

Când o mulţime autorizată B doreşte aflarea cheii, ea trebuie să ştie circuitul utilizat de arbitru pentru construirea sistemului şi să deducă de aici ce componente sunt necesare pentru parcurgerea arcelor respective. Această informaţie trebuie să fie publică. Numai valoarea componentelor trebuie să fie secretă.

5.4 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 $(1 \leq i \leq w)$.

Pentru fiecare $K \in \mathcal{K}$, fie $\mathcal{F}_K$ mulţimea tuturor distribuţiilor posibile ale cheii K. În general, $\mathcal{F}_K$ este publică. Definim

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

$\mathcal{F}$ este ansamblul complet al tuturor distribuţiilor posibile de chei. Rolul arbitrului va fi de a selecta aleator un element $f \in \mathcal{F}_K$ 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 părţi 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 elementele submulţimii B.

Ne punem acum problema evaluării performanţelor sistemelor perfecte de partajare a secretelor construite anterior, pe baza structurilor de acces monotone.

În cazul unui sistem confidenţial (t, w), circuitul boolean construit pe baza expresiei în forma normal disjunctivă are $1 + C_w^t$ porţi. Fiecare participant primeşte o componentă formată din C_{w-1}^{t-1} numere din Z_m. Această partajare este foarte slabă comparativ cu sistemul confidenţial al lui Shamir (t, w), 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 5.4 *Considerăm un sistem perfect de partajare a secretelor cu structura de acces* Γ. *Rata de informaţie a unui participant* P_i *este prin definiţie*

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

$S(P_i) \subseteq \mathcal{S}$ *este mulţimea componentelor posibile pe care le poate primi participantul* P_i. *S-a notat cu* $X = \mathcal{K}$ *mulţimea cheilor posibile.*

Rata de informaţie a sistemului este

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

Exemplul 5.7 *Să comparăm cele două sisteme date ca exemplu în paragraful anterior. Sistemul din Exemplul 5.4 are rata de informaţie* $\rho = \dfrac{log_2 m}{log_2 m^2} = \dfrac{1}{2}$.

Pentru sistemul din Exemplul 5.6, avem $\rho = \dfrac{log_2 m}{log_2 m^3} = \dfrac{1}{3}$.

Primul sistem este deci mai bun.

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 5.3 *Fie* $\mathbf{C}$ *un circuit boolean monoton. Există atunci un sistem perfect de partajare a secretelor, cu structura de acces* $\Gamma(\mathbf{C})$, *care admite ca rată de informaţie*

$$\rho = \max_{1 \leq i \leq w} \left\{ \frac{1}{r_i} \right\}$$

unde r_i *este numărul de arce de intrare în 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 5.4 *Pentru orice sistem perfect de partajare a secretelor cu structura de acces* Γ*, rata de informaţie verifică inegalitatea* $\rho \leq 1$*.*

Demonstraţie: Să considerăm un sistem perfect de partajare a secretelor având structura de acces Γ. Fie $B \in \Gamma_0$ şi $P_j \in B$ un participant. Definim $B' = B \setminus \{P_j\}$. Fie $g \in S(B)$. Cum $B' \notin \Gamma$, distribuţia componentelor $g|_{B'}$ nu dă nici o informaţie asupa cheii. Deci, pentru orice $K \in \mathcal{K}$ există o distribuţie a componentelor $g_K \in \mathcal{F}$ astfel ca $g_K|_{B'} = g|_{B'}$. Cum $B \in \Gamma$, vom avea $g_K(P_j) \neq gK'(P_j)$ pentru $K \neq K'$. Deci $card(S(P_j)) \geq card(\mathcal{K})$, adică $\rho \leq 1$. □

Un sistem cu $\rho = 1$ va fi numit ideal. Ca un exemplu, sistemul confidenţial al Shamir are $\rho = 1$, deci este un sistem ideal. În schimb, rata de informaţie pentru un sistem confidenţial (t, w) bazat pe circuite monotone construite cu forma normal disjunctivă este $\frac{1}{C_{w-1}^{t-1}}$, extrem de ineficientă dacă $1 < t < w$.

5.5 Sistemul de partajare al lui Brickell

Sistemul construit în acest paragraf este cunoscut sub numele de *construcţia vectorială a lui Brickell*.

Fie Γ o structură de acces, p un număr prim, iar $d \geq 2$ un număr întreg. Fie

$$\| : \mathcal{P} \longrightarrow Z_p^d$$

o funcţie cu proprietatea

$$(1, 0, \ldots, 0) \in \langle \| (P_i) \mid P_i \in B \rangle \iff B \in \Gamma. \qquad (A)$$

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

Plecând de la această funcţie, vom construi un sistem de partajare a secretelor cu $\mathcal{K}=S(P_i) = Z_p$ $(1 \leq i \leq w)$. 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 $f_{\mathbf{a}}(x) = \mathbf{a} \cdot \| (x)$.

S-a notat cu $\cdot$ produsul scalar a doi vectori. Algoritmul de partajare a secretelor Brickell este următorul:

1. (Iniţializare) Pentru $1 \leq i \leq w$, D atribuie lui P_i vectorul $\| (P_i) \in Z_p^d$. Aceşti vectori sunt publici.
2. Pentru repartizarea cheii $K \in Z_p$, arbitrul D alege aleator $d - 1$ elemente $a_2, \ldots, a_d \in Z_p$.
3. Folosind vectorul $\mathbf{a} = (K, a_2, \ldots, a_d)$, arbitrul calculează componenta $y_i = \mathbf{a} \cdot \| (P_i)$ $(1 \leq i \leq w)$, pe care o dă lui P_i.

Vom avea rezultatul următor:

Teorema 5.5 *Dacă $\|$ verifică proprietatea (A), mulţimea distribuţiilor de componente $\mathcal{F}_K$, $K \in \mathcal{K}$ formează un sistem perfect de partajare a secretelor, cu structura de acces Γ.*

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

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

unde $c_i \in Z_p$. Fie s_i componenta lui P_i. Vom avea $s_i = \mathbf{a} \cdot \| (P_i)$, unde $\mathbf{a}$ este vectorul necunoscut ales de D, iar $K = a_1 = \mathbf{a} \cdot (1, 0, \ldots, 0)$. Vom avea deci

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

Componenţii grupului B pot reconstitui deci cheia $K = \sum_{\{i|P_i \in B\}} c_i s_i$.

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

$$\begin{aligned} \| (P_i) \cdot \mathbf{a} &= s_i \quad \forall P_i \in B \\ (1, 0, \ldots, 0) \cdot \mathbf{a} &= K \end{aligned}$$

cu necunoscutele $a_1, \ldots, a_d$. Matricea sistemului are rangul $e + 1$ deoarece $(1, 0, \ldots, 0) \notin \langle \| (P_i) \mid P_i \in B \rangle$. Deci, independent de valoarea lui K, spaţiul soluţiilor este $d - e - 1$, adică există p^{d-e-1} distribuţii de componente în fiecare $\mathcal{F}_K$, consistente cu componentele participanţilor din B. □

Sistemul confidenţial (t, w) al lui Shamir este un caz particular al acestei construcţii. Într-adevăr, fie $d = t$ şi $\| (P_i) = (1, x_i, x_i^2, \ldots x_i^{t-1})$, pentru $1 \leq i \leq w$, unde x_i este coordonata x dată de P_i. Sistemul obţinut este echivalent cu cel al 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. Reamintim, 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 5.6 *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 $V_1, \ldots, V_s$ componentele lui G, şi $x_1, \ldots, x_s \in Z_p$ distincte $(p \geq s)$. Fie şi $d = 2$. Pentru fiecare participant $v \in V_i$ se defineşte $\| (v) = (x_i, 1)$. Proprietatea (A) se verifică imediat, deci – conform Teoremei 5.5 – afirmaţia este demonstrată. □

Vom aplica acest rezultat considerând structurile de acces posibile pentru patru participanţi. Va fi suficient să luăm în calcul numai structurile a căror bază nu se poate partiţiona în două mulţimi nevide. De exemplu, $\Gamma_0 = \{\{P_1, P_2\}, \{P_3, P_4\}\}$ 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 5.1 (s-a notat cu ρ^* valoarea maximă a ratei de informaţie pentru structura respectivă).

Se pot construi sisteme ideale pentru 10 din aceste 18 structuri de acces. Acestea sunt structuri confidenţiale sau structuri a căror bază este un graf multipartit, pentru care se aplică Teorema 5.6.

Tabelul 5.1: Structuri de acces cu maxim 4 participanţi

Nr.crt	w	Submulţimile lui G_0	ρ^*	Rezultate
1.	2	P_1P_2	1	Confidenţial $(2,2)$
2.	3	$P_1P_2,\ P_2P_3$	1	$\Gamma_0 \simeq K_{1,2}$
3.	3	$P_1P_2,\ P_2P_3,\ P_1P_3$	1	Confidenţial $(2,3)$
4.	3	P_1P_2P3	1	Confidenţial $(3,3)$
5.	4	$P_1P_2,\ P_2P_3,\ P_3P_4$	2/3	
6.	4	$P_1P_2,\ P_1P_3,\ P_1P_4$	1	$\Gamma_0 \simeq K_{1,3}$
7.	4	$P_1P_2,\ P_1P_4,\ P_2P_3,\ P_3P_4$	1	$\Gamma_0 \simeq K_{2,2}$
8.	4	$P_1P_2,\ P_2P_3,;P_2P_4,\ P_3P_4$	2/3	
9.	4	$P_1P_2,\ P_1P_3,\ P_1P_4,\ P_2P_3,\ P_2P_4$	1	$\Gamma_0 \simeq K_{1,1,2}$
10.	4	$P_1P_2,\ P_1P_3,\ P_1P_4,\ P_2P_3,\ P_2P_4,\ P_3P_4$	1	Confidenţial $(2,4)$
11.	4	$P_1P_2P_3,\ P_1P_4$	1	
12.	4	$P_1P_3P_4,\ P_1P_2,\ P_2P_3$	2/3	
13.	4	$P_1P_3P_4,\ P_1P_2,\ P_2P_3,\ P_2P_4$	2/3	
14.	4	$P_1P_2P_3,\ P_1P_2P_4$	1	
15.	4	$P_1P_2P_3,\ P_1P_2P_4,\ P_3P_4$	1	
16.	4	$P_1P_2P_3,\ P_1P_2P_4,\ P_1P_3P_4$	1	
17.	4	$P_1P_2P_3,\ P_1P_2P_4,\ P_1P_3P_4,\ P_2P_3P_4$	1	Confidenţial $(3,4)$
18.	4	$P_1P_2P_3P_4$	1	Confidenţial $(4,4)$

Exemplul 5.8 *Să considerăm structura de acces cu numărul* 9 *din Tabelul 5.1; deci* $d = 2$ *şi* $p \geq 3$. *Definim* $\|$ *prin*

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

Aplicând Teorema 5.6 se obţine o structură perfectă de partajare a secretelor, ideală pentru acest tip de acces.

Rămân de studiat opt structuri de acces. Se poate utiliza construcţia lui Brickell pentru patru din ele: structurile 11, 14, 15 şi 16.

Exemplul 5.9 *Pentru structura de acces* 11 *vom considera* $d = 3$ *şi* $p \geq 3$. *Definiţia lui* $\|$ *este*

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

Calculând, se obţine $\| (P_4) - \| (P_1) = (1,1,0) - (0,1,0) = (1,0,0)$ *şi*

$\| (P_2) + \| (P_3) - \| (P_1) = (1,0,1) + (0,1,-1) - (0,1,0) = (1,0,0)$.

Deci $(1,0,0) \in \langle \| (P_1), \| (P_2), \mathcal{P}(\mathcal{P}_\ni) \rangle$ *şi* $(1,0,0) \in \langle \| (P_1), \| (P_4) \rangle$.

Mai rămâne de arătat că $(1,0,0) \notin \langle \| (P_i) \mid P_i \in B \rangle$ *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*

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

cu $a_2, a_3, a_4 \in Z_p$. *Se obţine sistemul echivalent*

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

care nu are soluţie.

Exemplul 5.10 *Pentru structura de acces* 14 *vom defini* $d = 3$, $p \geq 2$, *iar* $\|$ *va fi:*

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

Proprietatea (A) *se verifică imediat; deci se poate aplica Teorema 5.6.*

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.

5.6 Construcţia prin descompunere

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

Definiţia 5.5 *Fie* Γ *o structură de acces cu baza* Γ_0 *şi* $\mathcal{K}$ *un set de chei. O* $\mathcal{K}$ *- descompunere ideală a lui* Γ_0 *este un set* $\{\Gamma_1, \ldots, \Gamma_n\}$ *cu proprietăt ile*

1. $\Gamma_k \subseteq \Gamma_0 \quad (1 \leq k \leq n)$;
2. $\bigcup_{k=1}^{n} \Gamma_k = \Gamma_0$;
3. $\forall\, k\ (1 \leq k \leq n)$ *există un sistem perfect de partajare a secretelor, ideal, cu mulţimea de chei* $\mathcal{K}$, *peste mulţimea de participanţi* $\mathcal{P}_k = \bigcup_{B \in \Gamma_k} B$.

Pentru o $\mathcal{K}$ - descompunere ideală a structurii de acces Γ se poate construi uşor un sistem perfect de partajare a secretelor.

Teorema 5.7 *Fie* Γ *o structură de acces cu baza* Γ_0, $\mathcal{K}$ *un set de chei şi o* $\mathcal{K}$ *- descompunere ideală* $\{\Gamma_1, \ldots, \Gamma_n\}$ *a lui* Γ. *Pentru fiecare participant* P_i, *fie* $R_i = card\{k \mid P_i \in \mathcal{P}_k\}$.

Există atunci un sistem perfect de partajare a secretelor cu structură de acces Γ *şi rată de informaţie* $\rho = 1/R$, *unde* $R = \max_{1 \leq i \leq w} \{R_i\}$.

Demonstraţie: Pentru $1 \leq k \leq n$ există un sistem ideal de structură de acces de bază Γ_k peste mulţimea $\mathcal{K}$. Notăm $\mathcal{F}_k$ mulţimea distribuţiilor componentelor sale. Vom construi un sistem cu structură de acces Γ peste mulţimea $\mathcal{K}$. Mulţimea distribuţiilor componentelor sale este generată după regula: dacă arbitrul D doreşte să împartă cheia K (în cazul $1 \leq k \leq n$), el va genera aleator o distribuţie de componente $f_k \in \mathcal{F}_K^k$ şi va distribui efectiv aceste componente participanţilor din $\mathcal{P}_k$.

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 $(1 \leq i \leq w)$. Deci $\rho_i = 1/R_i$ şi

$$\rho = \frac{1}{max\{R_i \mid 1 \leq i \leq w\}},$$

ceea ce incheie demonstraţia. □

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

Teorema 5.8 *(Construcţia prin descompunere): Fie Γ o structură de acces de bază Γ_0, $s \geq 1$ un număr întreg, şi $\mathcal{K}$ un set de chei. Presupunem că s-a construit o $\mathcal{K}$ - descompunere ideală $\mathcal{D}_j = \{\Gamma_{j,1}, \ldots, \Gamma_{j,n_j}\}$ a lui Γ_0, 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 un sistem perfect de partajare a secretelor, cu structura de acces Γ, a cărui rată de informaţie este $\rho = s/R$, unde $R = \max_{1 \leq i \leq w}(R_i)$.

Demonstraţie: Pentru $1 \leq j \leq s$ şi $1 \leq k \leq n$ se poate construi un sistem ideal cu baza $\Gamma_{j,k}$ şi mulţimea de chei $\mathcal{K}$. Vom nota $\mathcal{F}_{j,k}$ mulţimea corespunzătoare de distribuţii a componentelor. Vom construi un sistem cu structura de acces Γ şi mulţimea de chei $\mathcal{K}^s$. Mulţimea sa de distribuţii de componente $\mathcal{F}$ se generează astfel: dacă arbitrul D doreşte să împartă cheia $K = (K_1, \ldots, K_s)$ (pentru $1 \leq k \leq n$), el va genera aleator o distribuţie de componente $f^{j,k} \in \mathcal{F}_{K_j}^{j,k}$, pe care le distribuie efectiv participanţilor din $\mathcal{P}_{j,k}$.

În continuare se repetă demonstraţia Teoremei 5.7. □

Exemplul 5.11 *Să considerăm structura de acces 5 din Tabelul 5.1, a cărei bază nu este un graf multipartit complet.*

Fie p un număr prim şi să considerăm două Z_p - descompuneri:

$\mathcal{D}_1 = \{\Gamma_{1,1}, \Gamma_{1,2}\}$ *cu* $\Gamma_{1,1} = \{\{P_1, P_2\}\}$, $\Gamma_{1,2} = \{\{P_2, P_3\}, \{P_3, P_4\}\}$

şi

$\mathcal{D}_2 = \{\Gamma_{2,1}, \Gamma_{2,2}\}$ *cu* $\Gamma_{2,1} = \{\{P_1, P_2\}, \{P_2, P_3\}\}$, $\Gamma_{2,2} = \{\{P_3, P_4\}\}$

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 5.8 cu $s = 2$, vom obţine o rată de informaţie maximă $\rho = 2/3$.

Luând ca bază Teorema 5.6, putem obţine efectiv un astfel de sistem. D alege aleator patru elemente $b_{1,1}, b_{1,2}, b_{2,1}, b_{2,2} \in Z_p$. Pentru o cheie $(K_1, K_2) \in Z_p^2$, arbitrul va distribui componentele astfel:

1. *P_1 primeşte $b_{1,1}$ şi $b_{2,1}$;*
2. *P_2 primeşte $b_{1,1} + K_1$, $b_{1,2}$ şi $b_{2,1} + K_2$;*
3. *P_3 primeşte $b_{1,2} + K_1$, $b_{2,1}$ şi $b_{2,2}$;*
4. *P_4 primeşte $b_{1,2}$ şi $b_{2,2} + K_2$.*

(toate calculele sunt efectuate în Z_p).

Exemplul 5.12 *Fie structura de acces 8 din Tabelul 5.1. Vom considera $\mathcal{K} = Z_p$ pentru un număr prim $p \geq 3$. Vom utiliza două $\mathcal{K}$ - descompuneri ideale*

$\mathcal{D}_1 = \{\Gamma_{1,1}, \Gamma_{1,2}\}$ *cu* $\Gamma_{1,1} = \{\{P_1, P_2\}\}$, $\Gamma_{1,2} = \{\{P_2, P_3\}, \{P_2, P_4\}, \{P_3, P_4\}\}$

şi

$\mathcal{D}_2 = \{\Gamma_{2,1}, \Gamma_{2,2}\}$ *cu* $\Gamma_{2,1} = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_2, P_4\}\}$, $\Gamma_{2,2} = \{\{P_3, P_4\}\}$

$\mathcal{D}_1$ 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 5.8 cu $s = 2$ se va obţine $\rho = 2/3$. Similar exemplului precedent, o construcţie efectivă se realizează astfel:

D alege aleator (şi independent) patru elemente $b_{1,1}, b_{1,2}, b_{2,1}, b_{2,2} \in Z_p$. *Pentru o cheie* $(K_1, K_2) \in Z_p^2$, *arbitrul va distribui componentele astfel:*

1. P_1 *primeşte* $b_{1,1} + K_1$ *şi* $b_{2,1} + K_2$*;*
2. P_2 *primeşte* $b_{1,1}$, $b_{1,2}$ *şi* $b_{2,1}$*;*
3. P_3 *primeşte* $b_{1,2} + K_1$, $b_{2,1} + K_2$ *şi* $b_{2,2}$*;*
4. P_4 *primeşte* $b_{1,2} + 2K_1$, $b_{21} + K_2$ *şi* $b_{2,2} + K_2$.

(toate calculele sunt efectuate în Z_p*).*