UNIERSITATEA "ALEXANDRU IOAN CUZA"

Secret sharing folosind interpolare Birkhoff

de

Miron Radu

Teză în vederea susținerii
Licenței în Informatică

în
Universitatea "Alexandru Ioan Cuza", Iasi
Facultatea de Informatică

27 iunie 2018

Avizat, Îndrumător Lucrare de Licență :
Titlul, Numele și Prenumele

_____

Declarație privind originalitatea conținutului lucrării de licență

Data _____ semnatură Profesor: _____

Dată azi, _____ semnatură student: _____

Subsemnatul(a) .....
domiciliul în .....
născut(ă) la data de ......, identificat prin CNP .....
....., absolvent(a) al(a) Universității „Alexandru Ioan Cuza" din Iași, Facultatea de ..... specializarea ....., promoția ....., declar pe propria răspundere, cunoscând consecințele falsului în declarații în sensul art. 326 din Noul Cod Penal și dispozițiile Legii Educației Naționale nr. 1/2011 art.143 al. 4 si 5 referitoare la plagiat, că lucrarea de licență cu titlul .....: elaborată sub îndrumarea dl. / d-na ....., pe care urmează să o susțină în fața comisiei este originală, îmi aparține și îmi asum conținutul său în întregime. De asemenea, declar că sunt de acord ca lucrarea mea de licență să fie verificată prin orice modalitate legală pentru confirmarea originalității, consimțind inclusiv la introducerea conținutului său într-o bază de date în acest scop. Am luat la cunoștință despre faptul că este interzisă comercializarea de lucrări științifice in vederea facilitării fasificării de către cumpărător a calității de autor al unei lucrări de licență, de diploma sau de disertație și în acest sens, declar pe proprie răspundere că lucrarea de față nu a fost copiată ci reprezintă rodul cercetării pe care am întreprins-o.

Declarație de consimțământ

Prin prezenta declar că sunt de acord ca Lucrarea de licență cu titlul „Secret sharing folosind interpolare Birkhoff", codul sursă al programelor și celelalte conținuturi (grafice, multimedia, date de test etc.) care însoțesc această lucrare să fie utilizate în cadrul Facultății de Informatică. De asemenea, sunt de acord ca Facultatea de Informatică de la Universitatea „Alexandru Ioan Cuza" din Iași, să utilizeze, modifice, reproducă și să distribuie în scopuri necomerciale programele-calculator, format executabil și sursă, realizate de mine în cadrul prezentei lucrări de licență.

Iași, data:

_____

Absolvent Miron Radu,

_____

UNIERSITATEA "ALEXANDRU IOAN CUZA"

Abstract

Universitatea "Alexandru Ioan Cuza", Iasi
Facultatea de Informatică

Student Informatician

Miron Radu

Prin lucrarea de față se dorește găsirea unor asemănări între schemele de partajare a secretelor bazate pe interpolarea Lagrange și schemele de partajare ierarhice bazate pe interpolare Birkhoff. Ambele scheme se bucură de propritatea de liniaritate, deci de aici se pot deduce multe scheme precum cele deler-free sau cele de reducere a pragului. Deși schemele bazate pe Lagrange se bucura de o formă liniară a polinomului in funcție de subsecretele primite de utilizatori, iar cele bazate pe Birkhoff nu, în cele din urmă vom rescrie polinomul pentru a ne fi de folos în intenția noastră.

Cuprins

Symbols

F_p	corp de dimensiune p, unde p prim
$det(A)$	determinantul unei matrici A
$deg(P)$	gradul polinomului P
Γ	Structura de acces

Capitolul 1

Introducere

Partajarea de secrete reprezintă o metodă de a distribui un secret unui grup de participanți, în care fiecare participant are o parte din secret. Secretul va fi recompus numai de către o submulțime de utilizatori suficient de numeroasă, iar numărul de participanți necesari se numește prag.

Există un dealer care are un rol important în faza de setup, în care se crează secretul și se distribuie. Astfel, o schemă cu n utilizatori și cu prag t se numește (t, n) schema de partajare, unde n, t sunt numere naturale.

Această tema este una foarte interesantă deoarece are o mulțime de aplicții în viața cotidiană. Transferurile bancare sau securitatea în cloud sunt puține dintre aplicațiile partajării de secrete.

În secret sharing, este important ca orice mulțime de utilizatori care nu atinge pragul să nu poată să extragă absolut nicio informație asupra secretului. De exemplu, sa presupunem ca avem parola par = "brumă", formată din exact 5 litere. Presupunem ca ea se partajeaza la 4 utilizatori astfel : primul share este "br- - -", al doilea share este "–u–", al treilea este "—m-" si al patrulea este "—-ă". Dacă un utlizator nu are nimic de la dealer, atunci el trebuie să încerce s^5 posibilități, pe când dacă ar ști primul share, atunci ar avea de încercat doar s^3, deoarece ar ști deja 2 litere. Un așa scenariu este interzis în secret sharing.

Această partajare cu prag poate fi generalizată în mai multe moduri, dar una din generalizările cele mai interesante este cea în care fiecare utilizator dobândește o anumită importanță, deci vom avea mai multe praguri. Acest tip de partajare se numește partajare ierarhică. În cazul transferurilor bancare, un scenariu de utilizare a unei astfel de scheme este acela când, pentru a afla cheia de transfer avem nevoie de cel puțin 2 directori și cel puțin 3 brokeri.

Proprietățile schemelor de partajare ierarhice au fost studiate intens abia spre anul 2017, ceea ce înseamnă că este o temă recentă și interesantă.

Capitolul 2

Contribuții

Tema de licență a fost aleasă de comun acord împreună cu profesorul de licență. Discuțiile au pornit în urma unei scheme propuse de doi japonezi care era gresită. Deși făcusem progrese spre rezolvarea problemei, peste puțin timp deja începuseră sa apară articole despre schema respectivă. Am continuat cercetarea și am încercat sa schimb direcția în care se îndrepta corectura schemei. Problema era ca informația publică din schemă parea să lase loc de scurgeri de informație.
Astfel, am încercat să găsesc o structura ierarhica fară a pune la dispoziție informație publică. O astfel de schemă exista deja, și anume schema lui Tassa. Contribuția mea constă în cercetarea proprietăților schemei lui Tassa și găsirea de similitudini între aceasta și schema lui Shamir, iar mai apoi folosirea unor proprietăți pentru crearea unor noi scheme care sa pună în reflexie proprietățile schemei lui Shamir. Studiul principal a fost realizat în cadrul schemelor în care pentru partajarea a două secrete diferite se păstrează aceeași structură de acces.

Capitolul 3

Scheme de partajare cu prag

Partajarea de secrete cu prag a fost introdusă în 1979 de către Shamir și Blakley. Ambele scheme presupun un dealer și n jucători: $P_1, P_2, ..., P_n (n > 1)$. Dealer-ul își generează un secret s pe care îl va partaja (în mod privat către ceilalți participanți). Pragul t, al schemei de partajare are rolul de a indică numărul minim de jucători necesari de care este nevoie pentru a reconstrui secretul. Orice submulțime cu mai puțin de t jucători nu poate reconstrui secretul. Schemă lui Shamir se bazează pe interpolarea Lagrange.
Fiind date d puncte (x_i, y_i) există un unic polinom F cu $deg(F) \leq d - 1$ astfel încât pentru orice $i \in \{1, 2, ..., d\}$ este satisfacută relația $y_i = F(x_i)$.

3.1 Schema lui Shamir

În schema lui Shamir apar următoarele etape:

SETUP
Dealer-ul alege în mod secret $t - 1$ valori $a_1, a_2, ..., a_{t-1}$ din corpul F_p, unde p este un număr prim ce se generează tot în partea de setup. Se formează polinomul F = $\sum_{l=1}^{t-1} a_l X^l + s$.

SHARE
Fiecare participant, etichetat cu i , P_i (etichetă ce mai târziu se va numi id) primește, în mod privat, secretul său, $F(i)$.

RECONSTRUCȚIE

Este nevoie de (cel puțin) t participanți pentru a recosntrui secretul. Ei își vor pune la comun secretul primit, și astfel, aplicând formula de interpolare Lagrange, se poate afla $F(0) = s$.

$$s = \sum_{j \in I} F(j) \prod_{i \in I, i \neq j} \frac{i}{i - j}$$

unde $I = \{j_1, j_2, ..., j_t\}$ este mulțimea etichetelor participanților care reconstruiesc secretul.

3.1.1 Demonstrație de securitate

Scehma lui Shamir este atât corectă cât și perfectă.

*** proprietatea de corectitudine se referăla faptul că la sfârșitul fazei de reconstrucție, secretul s este deteminat corect. Acest lucru se demosntrează ușor, formând matricea sistemului pentru cele t ecuații puse la comun de către participanții care reconstruiesc secretul. Matricea sistemului este de tip Vandermonde. Cum participanții la reconstruire au o identitate diferită unul față de altul, matricea sistemului are determinant nenul, deci are soluție unică. Astfel, jucătorii pot determina coeficienții polinomului generat de dealer în faza de setup, în particular, coeficientul liber al polinomului, adică secretul s.

*** proprietatea de perfecțiune se referă la faptul că mai puțin de t participanți nu pot reconstrui secretul și nu pot extarge nicio informație cu privire la secretul s. Presupunem că schema dispune de canale sigure și private de transmitere a secretelor de la dealer către participanți și la punerea în comun a secretelor de către participanți.
Cum condiția de securitate se referă la scurgerea de informații, devine comod să lucrăm cu teoria informației, în particular cu funcția de entropie a lui Shannon.

Un element $\mathbf{v} \in \mathbf{V}$ este descris de o variabilă aleatoare V din V.
Fie X și Y două variabile aleatoare. Atunci avem următoarele definiții:

*** entropia lui X este $H(X) = -\sum_{x \in X} P(X = x) log_2 P(X = x)$
*** entropia joint $H(X, Y) = -\sum_{x \in X} \sum_{y \in Y} P(X = x, Y = y) log_2 P(X = x, Y = y)$
*** entopia condițională $H(X|Y) = \sum_{y \in Y} P(Y = y) H(X|Y = y)$, unde $H(X|Y = y) = -\sum_{x \in X} P(X = x|Y = y) log_2 P(X = x|Y = y)$

Fie X, Y, Z trei variabile aleatorii. Avem următoarele proprietăți:

* $H(X) \geq H(X|Y)$ (1)
* $H(X,Y) = H(X) + H(Y|X) = H(Y) + X(X|Y)$ (2)
* $0 \leq H(X) \leq log_2|X|$ (3)
* dacă $H(Y|Z) = 0$ atunci $H(X|Y) \geq H(X|Z)$ (4)
* dacă $H(Y|Z) = 0$ atunci $H(X|Y,Z) = H(X|Z)$ (5)

Fie polinomul $F = a_0 + a_1X + ... + a_{t-1}X^{t-1}$, unde t este pragul schemei, iar $a_0 = s$ și $a_i, i \in \{1, 2, ..., t-1\}$ sunt selectați random din F_p. Fie $P_{i_1}, P_{i_2}, ..., P_{i_t}$ cei t participanți care doresc reconstrucția secretului. Fie S variabilă random ce descrie secretul, F_i variabilă aleatorie care descrie share-ul $F(i)$ și A_i variabilă ce descrie coeficietul a_i al polinoului F. Pentru a demonstra corectitudinea trebuie să arătăm că $H(S|F_{i_1}, ..., F_{i_t}) = 0$ (6), iar pentru perfecțiune trebuie să artam că $H(S|F_{i_1}, ..., F_{i_t}) = H(S)$.

Demonstrația 1. Schemă lui Shamir este corectă.
Pentru a demonstra corectitudinea, trebuie să arătăm că pentru orice $l \geq t$ avem relația $H(S|F_{i_1}, ..., F_{i_l}) = 0$ (6). Adică, din punct de vedere informațional, trebuie să arătăm că dacă cel puțin t participanți pun la comun share-urile lor, se poate afla secretul.
Știm că în urmă interpolarii, polinomul este unic determinat de cele t perechi $(P_{i_k}, F(i_k))$. Din punct de vedere informațional aceasta este echivalent cu

$$H(A_0, A_1, ..., A_{t-1}|F_{i_1}, ..., F_{i_t}) = 0 \qquad (8)$$

Din faptul că vom afla share-urile pe care dealur-ul le transmite participanților, $F_{i_1}, ..., F_{i_t}$, doar cunoscând coeficienții $A_0, A_1, ..., A_{t-1}$, din punct de vedere informațional, putem trage concluzia că

$$H(F_{i_1}, ..., F_{i_t}|A_0, A_1, ..., A_{t-1}) = 0 \qquad (9)$$

Din relațiile (8) și (4) obținem că

$$H(S|A_0, A_1, ..., A_{t-1}) \geq H(S|F_{i_1}, ..., F_{i_t})$$

Din relațiile (9) și (4) obținem că

$$H(S|A_0, A_1, ..., A_{t-1}) \leq H(S|F_{i_1}, ..., F_{i_t})$$

Deci $H(S|A_0, A_1, ..., A_{t-1}) = H(S|F_{i_1}, ..., F_{i_t})$. Dar $A_0 = s$, deci $H(S|A_0, A_1, ..., A_{t-1}) = H(S|S, A_1, ..., A_{t-1}) = 0$. Va rezulta că $H(S|F_{i_1}, ..., F_{i_t}) = 0$. Utilizând acum proprietatea (1), va rezulta că $H(S|F_{i_1}, ..., F_{i_{t+\alpha}}) \leq H(S|F_{i_1}, ..., F_{i_t}), \alpha \geq 0$, adică tocmai proprietatea (6).

Demonstrația 2. Schema lui Shamir este perfectă.
Pentru a demonstra că schemă este perfectă, trebuie să demomnstram că

$$H(S|F_{i_1},...,F_{i_l}) = H(S), \forall l \leq t \qquad (7)$$

Adică, din punct de vedere informațional, trebuie să arătăm că dacă mai puțin de t participanți pun la comun secretul lor, nu vor obține nicio informație cu privire la secretul s. Entropia joint dintre $(A_0, A_1, ..., A_{t-1})$ și $(F_0, F_{i_1}, F_{i_2}, ..., F_{i_{t-1}})$ este

$$H(A_0, A_1, ..., A_{t-1}, F_0, F_{i_1}, F_{i_2}, ..., F_{i_{t-1}}) = H(F_0, F_{i_1}, F_{i_2}, ..., F_{i_{t-1}}) +$$
$$+H(A_0, A_1, ..., A_{t-1}|F_0, F_{i_1}, F_{i_2}, ..., F_{i_{t-1}}) = H(F_0, F_{i_1}, F_{i_2}, ..., F_{i_{t-1}})$$

(folosind relația (8)).

Analog se obține $H(A_0, A_1, ..., A_{t-1}, F_0, F_{i_1}, F_{i_2}, ..., F_{i_{t-1}}) = H(A_0, A_1, ..., A_{t-1})$. Deoarece $F_0 = a_0 = s$, obținem $H(S, F_{i_1}, F_{i_2}, ..., F_{i_{t-1}}) = H(S, A_1, ..., A_{t-1})$ (*). Astfel, $H(S)+H(F_{i_1}, F_{i_2}, ..., F_{i_{t-1}}|S) = H(A_1, ..., A_{t-1})+H(S|A_1, ..., A_{t-1})$ (10). Dar coeficientii polinomului sunt aleși uniform din K, deci $H(A_1, ..., A_{t-1}) = log_2|K|^{t-1}$. Totodată, coeficientii polinomului sunt independenți de secretul s, deci $H(S|A_1, ..., A_{t-1}) = H(S)$. Folosind acum relația (10) obținem că $H(F_{i_1}, F_{i_2}, ..., F_{i_{t-1}}|S) = log_2|K|^{t-1}$. Din (1) avem că $H(F_{i_1}, F_{i_2}, ..., F_{i_{t-1}}) \geq H(F_{i_1}, F_{i_2}, ..., F_{i_{t-1}}|S) = log_2|K|^{t-1}$ (11) . Dar din (3), avem că $H(F_{i_1}, F_{i_2}, ..., F_{i_{t-1}}) \leq log_2|K|^{t-1}$. Rezultă deci că $H(F_{i_1}, F_{i_2}, ..., F_{i_{t-1}}) = log_2|K|^{t-1}$. Rescriind acum relația (*) sub formă $H(F_{i_1}, F_{i_2}, ..., F_{i_{t-1}}) + H(S|F_{i_1}, F_{i_2}, ..., F_{i_{t-1}}) = H(A_1, ..., A_{t-1}) + H(S|A_1, ..., A_{t-1})$. Cum $H(A_1, ..., A_{t-1}) = H(F_{i_1}, F_{i_2}, ..., F_{i_{t-1}})$ și $H(S|A_1, ..., A_{t-1}) = H(S)$, obținem $H(S|F_{i_1}, F_{i_2}, ..., F_{i_{t-1}}) = H(S)$. Fie acum un număr $k, k \leq t-1$. Din (1), $H(S) \geq H(S|F_{i_1}, F_{i_2}, ..., F_{i_k}) \geq H(S|F_{i_1}, F_{i_2}, ..., F_{i_{t-1}}) = H(S)$. Urmează că $H(S|F_{i_1}, F_{i_2}, ..., F_{i_k}) = H(S)$, adică tocmai ceea ce era de demonstrat.

3.1.2 Proprietăți ale schemei Shamir

Această secțiune are rolul de a descrie succint trei proprietăți interesante ale schemei Shamir, urmând apoi a fi transpuse către o altă formă de partajare a secretelor.

1. Proprietatea de homomorfism/multiplicitate

Fie S mulțimea de secrete și S_{shares} mulțimea posibilă de secrete partajate. Fie $*$ o operație asociativă, comutativa și binară peste S. Spunem că o schemă de partajare(split,

combine) este multiplicativă dacă pentru orice structura de acces A, există o familie de funcții publice $f_{(i,A)}|i \in A$ definită de la S_shares la S astfel încât

$$(\forall s \in S)((S <---->_A^{(split,combine)} I_1, I_2, ..., I_n) => S = *_{i \in A} f_{(i,A)}(I_i)).$$

O subclasa importantă a schemelor de partajare homomorfice este este clasa schemelor liniare de partajare a secretelor. O schemă liniară de partajare este o schemă cu proprietatea de mai sus, dar care are proprietatea că funcțiile $f_(i, A)$ sunt homomrorfisme.

Propoziția 1. Schemă lui Shamir este liniară.
Demonstartie.
Vrem să demonstrăm că dacă secretul S se partajeaza prin Shamir, splitat în secretele $I_1, I_2, ..., I_n$, atunci el poate fi reaflat combinând cele n subsecrete. Pentru schema lui Shamir putem scrie astfel:

$$S <-- >_{(k,n)}^{Shamir} => S = \sum_{i \in A} f_{(i,A)}(I_i)$$

Fie $P_1, P_2, ..., P_n$ cei n participanți ai schemei. Presupunem că participantul P_i are identitatea i. Fie s_1, s_2 cele două secrete ce se doresc a fi partajate. s_1 va fi partajat prin polinomul $f_{s_1}(x) = s_1 + a_1x + a_2x^2 + ... + a_tx^t$, iar secretul s_2 va fi partajat folosind polinomul $f_{s_2}(x) = s_2 + b_1x + b_2x^2 + ... + b_tx^t$.
Participantul i va primi $f_{s_1}(i)$ și $f_{s_2}(i)$. Adunând cele două secrete primite, P_i va ști

$$f_{s_1}(i) + f_{s_2}(i) = s_1 + s_2 + i(a_1 + b_1) + i^2(a_2 + b_2) + ... + i^t(a_t + b_t)$$

.
Dar această sumă este de fapt $f_{s_1+s_2}(x) = (s_1 + s_2) + (a_1 + b_1)x + ... + (a_t + b_t)x^t$. Cum coeficienții polinoamelor f_{s_1} și f_{s_2} au fost aleși random, $f_{s_1}(i) + f_{s_2}(i)$ va fi o valoare random iar polinomul $f_{s_1+s_2}(x)$ are grad cel mult egal cu t. Astfel, $s_1 + s_2$ va fi aflat punând la comun secretele a t participanți.

Propoziția 2. Înmulțirea cu o constantă (publică) c produce liniaritate.
Demonstrație.
Fie S secretul ce se vrea a fi partajat și c un număr real. Presupunem că participantul P_i are identitatea i. Atunci share-ul său va fi $f_S(i)$, unde f_S este polinomul ales de dealer în faza de setup. Atunci, după înmulțirea cu c, P_i va avea share-ul $cf_S(i) = cS + ca_1i + ca_2i^2 + ... + ca_ti^t$. Dar acestea sunt valorile polinommului f_{cS} evaluat în identitățile participanților.
Cum coeficienții polinomului sunt random, va rezulta că înmulțind fiecare cooeficient cu

c, rezultatul va fi tot aleator. Gradul maxim al polinomului rezultat după înmulțirea cu c va fi tot t. Cum coeficientul liber al polinomului este cS, participanții vor afla secretul cS.

Putem trage concluzia că împărțirea secretului în subsecrete și inmutirea lui cu o constantă publică producea aflarea secretului astfel modificat.

Propoziția 3. Dacă $c_1, c_2, ..., c_n$ sunt constante și $s_1, s_2, ..., s_n$ secrete partajate. Atunci se poate află secretul $\sum c_i s_i$.
Demonstrație.
Proprietatea rezultă din combinarea propozițiilor 1 și 2.

Propoziția 4. Schemă lui Shamir nu produce o schemă valida în vederea obținerii produsului a două secrete.
Demosntratie.
Fie $P_i, i \in \{1, ..., n\}$ cei n participanți a unei scheme Shamir de prag t cu secretele S_1, S_2, $n \geq 2t + 1$ (În ideea că mai puțîn de jumătate din participanți pot recupera secretul). Presupunem, fără a restrânge generalitatea că fiecare participant P_i are identitatea i. Fie g un polinom pentru care $g(i) = f_{S_1}(i) f_{S_2}(i)$. Evident, gradul lui g va fi cel mult $2t$ (deoarece polinomul g este definit de cel mult $2t + 1$ puncte ce reprezintă share-urile participanților).
Fie acum $p(x) = f_{S_1}(x) f_{S_2}(x)$. Cum f_{S_1} și f_{S_1} au gradul cel mult t, rezultă că p are gradul cel mult $2t$. Dar $p(i) = g(i), \forall i \in \{1, 2, ..., n\}$. Cum $deg(p) \leq 2t$ și $deg(q) \leq 2t$, iar p, g sunt egale în cel puțin $2t + 1$ puncte ($m \geq 2t + 1$), rezultă că $p = g$.

Lema 1. Fie f_1, f_2 două polinoame de grad cel mult d, ambele. Dacă mulțimea $A = \{x | f_1(x) f_2(x)\}$ are cel puțin $d + 1$ elemente rezultă că $f_1 = f_2$.

Demonstrație.
Într-adevăr, fie polinomul P cu $P(x) = f_1(x) - f_2(x)$. Cum $deg(f_1) \leq d$ și $deg(f_2) \leq d$ rezultă că $deg(P) \leq d$. Dar $P(x) = 0, \forall x \in A$. Asta înseamnă că P are $d + 1$ rădăcini. Dar cum gradul lui P este cel mult d, rezultă că P este polinomul nul.

Reintorcandu-ne la demonstrație, am obținut că $g = p$. Polinomul p are termenul liber tocmai $S_1 S_2$. Totuși, motivul pentru care acesta nu este bun, este tocmai acela că p nu determina o distribuție uniformă a coeficienților săi.
Într-adevăr, p este întotdeauna reductibil peste F_p, deci se exclud polinoamele cu coeficienți din F_p care sunt ireductibile.

2. Proprietatea de a fi dealer-free

Una dintre problemele mari a unei scheme de partajare este aceea că după ce t utilizatori pun la comun share-urile, toate secretele partajate și secretul inițial vor fi cunoscute de toți participanții. O soluție ar fi că dealer-ul să partajeze mai multe secrete de la bun început. O altă soluție ar fi că participanții să genereze noi secrete fără a fi nevoie de implicarea dealer-ului. Aici intervin schemele dealer-free, în care participanții generează noi secrete. În cazul unei astfel de scheme secretul va fi implicit.

Schemă propusă.

Fie $P_1, P_2, ..., P_n$ cei n participanți ai unei scheme de partajare cu prag t. Presupunem că fiecare participant P_i generează random, un număr x_i, cu $x_i \in F_p$. Fiecare particpant în parte va folosi schema lui Shamir pentru a partaja secrete celorlalți participanți. Deci, va folosi un polinom f_i cu termenul liber x_i și va transmite participantului P_j valoarea $f_i(id_{P_j})$, unde id_{P_j} este identitatea jucătorului P_j. După ce fiecare participant execută acest protocol, participantul P_j va deține share-ul $s_j = f_1(id_{P_j}) + f_2(id_{P_j}) + ... + f_n(id_{P_j})$, obținut prin adunarea secretelor primite de la ceilalți participanți.
Astfel, noul secret va fi $S = x_1 + x_2 + ... + x_n$.

Într-adevăr, fie $q_{i,d}, d \in 1, 2, ..., t-1$ coeficientii generați random de participantul P_i pentru a partaja către ceilalți participanți secretul x_i. Astfel $f_i(x) = x_i + q_{1,1}x + q_{1,2}x^2 + ... + q_{1,t-1}x^{t-1}$.
Va rezulta că P_j are $s_j = (x_1 + x_2 + ... + x_n) + (q_{1,1} + q_{2,1} + ... + q_{n,1})id_{P_j} + ... + (q_{1,t-1} + q_{2,t-1} + ... + q_{n,t-1})id_{P_j}^{t-1}$. Se observă că se obține un polinom de grad $t-1$ ce are ca și termen liber suma $S = x_1 + x_2 + ... + x_n$.
Folosind acum interpolarea pe oricare t noduri din mulțimea de participanți, obținem secretul S. Se modifică astfel secretul și shere-urile, fără a fi nevoie de un dealer online. Se poate observă că la transmiterea și adunarea secretelor primite de către participantul P_j, s-a folosit proprietatea de liniaritate a schemei lui Shamir.

3. Schimbarea pragului.

În cazul unei scheme de partajare a secretelor pot apărea următoarele:

(*)Share-ul unui participant poate deveni invalid deoarece acesta a părăsit organizația sau și-a pierdut secretul.
(*)O nouă persoană poate intră în organizație
(*)Schimbarea pragului schemei.

Dacă se cunoaște din avans vreo posibilă schimbare asupra structurii schemei de partajare, delaer-ul poate acționa de cuviință. Vom propune în continuare o schemă dealer-free de schimabre a pragului.

Schemă de descreștere a pragului.

1. Jucătorii selectează un id j, astfel încât j să nu se afle în mulțimea identităților jucătorilor implicați în schemă. Fie $P_1, P_2, ..., P_t$ cei t jucători care doresc să refacă un secret. Apoi fiecare calucleaza constanta folosită pentru polinomul de interpolare Lagrange:
$\gamma_i = \prod_{1 \leq k \leq t, i \neq k} \frac{j-k}{i-k}$

2. Fiecare jucător P_i își va înmulți share-ul său $f(id_i)$ cu γ_i. Mai apoi, va "splita" secretul sau în t porțiuni:
$\gamma_i f(id_i) = \phi_{1i} + \phi_{2i} + ... + \phi$ți$, 1 \leq i \leq t$

3. Jucătorii schimbă între ei valorile ϕ_{ij}. Valoarea ϕ_{ij} reprezintă valoarea trimisă de jucătorul j către jucătorul i astfel,
$\sigma_i = \phi_{i1} + \phi_{i2} + ... + \phi_{it}$
va fi ceea ce va deține jucătorul P_i și va pune la comun cu restul jucătorilor care reconstruiesc secretul.

4. Jucătorii adună valorile γ_k, $1 \leq k \leq t$ și caluleaza
$f(j) = \sum_{k=1}^{t} \sigma_k$

5. Fiecare P_i combină share-ul său privat $f(i)$ cu $f(j)$ după următoarea formulă:
$f_0(i) = f(j) - j(\frac{f(i)-f(j)}{i-j})$ (**) .
Cum id-ul j nu se află printre mulțimea id-urilor participanților, expresia f_0 este bine definită (fractia $\frac{f(i)-f(j)}{i-j}$ nu are numitorul egal cu 0).

6. Polinomul f_0 este un polinom de gradul $t-1$, cu $f_0(0) = f(0)$. Va rezulta că pragul $t-1$ este noul prag al schemei.

În cele ce urmează vom demonstra că $f_0(0) = f(0)$, iar gradul lui f_0 este $t-2$.
Presupunem că s-a făcut publică perechea $(j, f(j))$. Știm că pentru orice polinom cu coeficienți întregi, are loc:

$$(x-y)|f(x)-f(y)$$

unde "|" semnifică divizibilitatea de polinoame. Fie f_1 un polinom de gradul $t-1$ definit astfel:

$$f_1(x) = \frac{f(x)-f(j)}{x-j} \qquad (i)$$

Fiecare participant P_i trebuie să calculeze

$$f_1(id_i) = \frac{f(id_i)-f(j)}{id_i-j} \qquad (i)$$

Folosind (i), secretul asociat cu f_1 este : $f_1(0) = \frac{f(0)-f(j)}{-j}$. (iii)
Folosind relația (iii), obținem $f(0) = f(j) - jf_1(0)$.
Noul polinom este definit astfel:

$$f_0(x) = f(j) - jf_1(x) = f(j) - j\frac{f(x)-f(j)}{x-j}$$

.
Rezultă că $f_0(i) = f(j) - j\frac{f(i)-f(j)}{i-j}$. Rezultă că

$$f_0(0) = f(j) - jf_1(0) = f(0)$$

.
Evident polinomul f_0 are gradul cel mult $t-2$, iar mai sus am arătat că $f(0) = f_0(0)$, de unde rezultă tocmai concluzia schemei propuse.
Din nou, am folosit proprietatea de liniaritate a schemei lui Shamir atunci când s-au distribuit cantitățile ϕ_{ij}.
Securitatea schemei de reducere a pragului se bazează pe securitatea schemei lui Shamir prezentată mai devreme.

Capitolul 4

Interpolarea Birkhoff

Problemele de interpolare cu valorile date $c_{i,k}$ ale polinomului P_n, de grad cel mult n, în $n+1$ puncte

$$P_n^{(k)}(x_i) = c_{i,k} \qquad (2.1)$$

pot fi despărțite în două clase. Cele în care secvența ordinelor derivatelor formează un șir de numere $d_i, i \in 1, 2, ..., n+1$ cu proprietatea că $d_{i+1} - d_i \leq 1$ și cele în care șirul derivatelor nu respectă proprietatea anterioară. În primul caz, interpolarea Lagrange (prezentată pentru schemă lui Shamir) este un caz particular al interpolării Hermite, pentru șirul derivatelor egal cu 0. Polinomul de interpolare pentru această clasa există și este întotdeauna unic.

Dacă secvență derivatelor din ecuațiile (2.1) este lacunară, atunci avem interpolare Birkhoff (sau lacunară). Unii consideră interpolarea Hermite un caz special al interpolării Birkhoff, deși ele sunt foarte diferite una față de cealaltă.

Perechile (i, k) care apar în (2.1) sunt cel mai bine descrise de matricea de interpolare $E = [e_{i,k}]_{i=1}^{m}{}_{k=0}^{n}$ a problemei. Vom consideră $e_{i,k} = 1$ dacă perechea (i, k) apare în sistemul de ecuațîi (2.1) și $e_{i,k} = 0$ dacă perechea (i, k) nu apare în sistemul (2.1).

În 1996, Schoenberg a pus problema aflării tutror matricilor E pentru care problema interpolării are soluție, indiferent de alegerea punctelor $(x_i, c_{i,k})$. Vom numi o astfel de matrice *regular*, iar restul matricelor vor fi numite *singulare*.

Deși aflarea unei forme generale a matricelor regulare a fost în centrul studiului problemelor de interpolare de-a lungul timpului, încă de când Schoenberg a propus această provocare, se pare că sistemul (2.1) ascunde provocări interesante și pentru noduri x_i fixate. Însuși G.D. Birkhoff a discutat asupra interpolării ce îi poartă numele, în singură lucrare ce a dedicat-o acestei teme, făcând presupunerea că sistemul (2.1) are soluții.

Din 1995, Turan, studenții săi și urmăritorii săi au studiat cazul în care matricea E a problemei este regulară, dar având la dispoziție mulțimi particulare de noduri x_i (care aveau să fie zerouri ale unor polinoame ortogonale).
Primele lucrări care studiază cazul general au fost cele ale lui Atkinson și Sharma și D. Ferguson. În mod surprinzător, nu prea s-au mai găsit imbunatairi ale consditiiilor acestora, de-a lungul timpului, în ciuda noilor metode folosite pentru rezolvarea problemei găsirii condițiilor de regularitate.

4.1 Notiuni de baza

Fie $G = \{g_0, g_1, ..., g_N\}$ un sistem de funcții liniar independente, de n ori continuu-diferențiabile ce iau valori reale pe o mulțime A care este un interval $[a, b]$ (vom lua în considerare doar cazul algebric - existând definiții și pentru metode trigonometrice). O combinație liniară $P = \sum_{j=0}^{N} a_j g_j$, cu a_j numere reale, va fi numită *polinom* peste mulțimea de funcții G.
Se poate, de asemenea, să se considere G o mulțime de funcții cu valori complexe, iar P un polinom cu coeficienți complecși.
Matricea

$$E = [e_{i,k}]_{i=1}^{m}{}_{k=0}^{n}, m \geq 1, n \geq 0 \qquad (2.2)$$

este o *matrice de interpolare* dacă are toate elementele $e_{i,k}$ egale cu 0 sau cu 1 și dacă numărul de elemente de 1 din matricea E este egal cu $N+1$, adică $|E| = \sum e_{i,k} = N+1$. O matrice de interpolare nu trebuie să conțină rânduri goale (adică pline cu zerouri - $e_{i,k} = 0k = 0, 1, 2, ..., n$). Un set de noduri $X = \{x_1, x_2, ..., x_m\}$ este format dn m puncte distincte ale mulțimii A. Elementele E, X, G și mulțime de date $c_{i,k}$ definite pentru $e_{i,k} = 1$ determina o problema de interpolare Birkhoff. Această problema constă în găsirea polinomului P ce satisface

$$P^{(k)}(x_i) = c_{i,k}, e_{i,k} = 1 \qquad (2.3)$$

Sistemul (2.3) constă în $N + 1$ ecuații liniare cu $N + 1$ necunoscute, și anume a_j, rerezentand coeficientii polinomului P.
Perechea (E, X) se numește *regular* dacă sistemul (2.3) are soluție unică, oricare ar fi datele $c_{i,k}$, altfel, perechea (E, X) se numește *singular*. Perechea (E, X) este regulară dacă determinantul sistemului

$$D(E,X) = det[g_0^{(k)}(x_i), g_1^{(k)}(x_i), ..., g_N^{(k)}(x_i)|e_{i,k} = 1] \qquad (2.3.1)$$

este diferit de 0.
În formula determinantului de mai sus am afișat un singur rând al matricei sistemului. Liniilie matricei vor fi corespunzătoare unei singure perechi (i,k) cu $e_{i,k} = 1$. Ordonăm liniile matricei E în ordine lexicografică după tuplele (i,k) : perechea (i,k) precede (i',k') dacă și numai dacă $i < i'$, iar dacă $i = i'$ atunci $k < k'$. Vom nota cu $A(E,X)$ matricea $(N+1) \times (N+1)$ din (2.3.1).
O noțiune de baza introdusă de *Shoenberg*, este cea de matrice *poised* de interpolare. Această proprietate presupune că perechea (E,X) să fie regulară pentru orice set X de o anumită clasa dată. Tipuri importante de regularitate sunt următoarele: E este regulară ordonată dacă X este o mulțime de puncte ordonate $x_1 \leq x_2 \leq ... \leq x_m$ de numere din $[a,b]$; E este regulară reală dacă perechea (E,X) este regulară pentru orice mulțime de numere reale X. Pentru clasa reală distingem două subclase: singularitate *tare* când $D(E,X)$ ia valori de semne diferite, singularitate *slab*, când $D(E,X)$ se anulează, dar fără schimbare de semn.
O matrice este singulară dacă și numai dacă, pentru un polinom netrivial P, matricea E îl anulează, adică au loc relațiile:

$$P^{(k)}(x_i) = 0, e_{i,k} = 1.$$

Pentru o matrice singulară, fie $r(E)$ rangul cel mai mic al matricei $A(E,X)$. Atunci,

$$d = d(E) = N + 1 - r(E) \qquad (2.4)$$

este $defectul$ lui E, și reprezintă cea mai mare dimensiune a subspatiului polinoamelor P care sunt anulate de E, pentru un anumit set X.
Deși inițial problema era de a găsi toate matricile regulare ordonate, descrise de proprietățile lor față de datele $c_{i,k}$, acest lucru s-a dovedit a fi difficil, rezolvându-se doar anumite cazuri particulare.

Exemple:
O matrice de interpolare Lagrange are $m = N+1, n = 0$, iar E are o coloana plină de 1. Ecuațiile (2.3) devin $P(x_i) = c_i, i = 1,2,...,N+1$. Evident, avem regularitate dacă P are cel mult N rădăcini în A (astfel, cel puțin una din valorile $P(x_i)$ va fi diferită de 0).

O matrice Taylor E e o linie $1 \times (n+1)$ cu eucatiile din (2.3) fiind $P^{(k)}(x_i) = c_k, k = 0, 1, ..., n$.

O matrice Abel este o matrice $(n+1) \times (n+1)$ cu $N = n$ și exact un singur 1 pe fiecare linie și fiecare coloana.

Vom numi un rând i din E hermitian dacă pentru un anumit r_i, $e_{i,k} = 1$, pentru $k \leq r_i$ și $e_{i,k} = 0$, pentru $k \geq r_i$. O matrice hermitiana are toate rândurile hermitiane. O matrice $semi - hermitiana$ este o matrice care are doar liniile $i, 1 \leq i \leq m$ hermitiane.

Considerăm următoare lemă ce ajută la deciderea singularității tari a unei matrici E.

LEMA1. Fie $\Phi(X)$ o funcție continuă de $X = \{x_1, x_2, ..., x_m\}$ pe intervalul $[a, b]$: $a \leq x_1 \leq x_2 \leq ... \leq x_m \leq b$, care își schimbă semnul și se anulează într-un set care nu este dens din A. Atunci ϕ își schimbă semnul în una din variabilele x_i, $i \in \{1, 2, , ..., m\}$.

Demonstrație. Fie $\Phi(X^0) \leq 0 \leq \Phi(Y^0)$ pentru $X^0 = \{x_1^0, x_2^0, ..., x_m^0\}$, $Y^0 = \{y_1^0, y_2^0, ..., y_m^0\}$. Presupunem, fără a restrânge generalitatea că $x_i^0 < y_i^0$, pentru $i = 1, 2, ..., m$. Atunci, aceeași inegalitate pentru X^0, Y^0 va avea loc, dacă substituim X^0, Y^0 cu X, Y, cu $X \in U$ și $Y \in V$, unde U, V sunt vecinitati ale lui X^0, Y^0 respectiv. Funcțiile $\Phi_r, r = 0, ..., m$, definite pe $U \times V$, astfel încât $\Phi_r = \Phi(\{x_1, ..., x_r, y_{r+1}, ..., y_m\})$ sunt continue și se anulează doar pe un set ne-dens în $U \times V$. Rezultă imediat că produsul funcțiilor Φ_r va avea aceeași proprietate, $\Gamma = \prod_{r=0}^{m} \Phi_r$. Astfel, există $X \in U$, $Y \in V$ astfel încât $\Phi_r(X, Y) \neq 0$, pentru $r = 0, 1, ..., m$. Cum Φ_0 și Φ_m au semne diferite (deoarece această revine la $\Phi(X) \leq 0 \leq \Phi(Y)$, inegalitate justificată de alegerea lui X, Y în vecinitatile lui X^0, Y^0), rezultă că există un r astfel încât $\Phi_r \Phi_{r+1} \leq 0$. Rezultă că Φ își schimbă semnul în x_{r+1}.

4.2 Cazul Algebric

Vom trata doar cazul algebric al interpolării Birkhoff.
Fie $A = [a, b]$ și fie G mulțimea puterilor:

$$g_0(x) = 1, g_1(x) = \frac{x}{1!}, ..., g_N(x) = \frac{x^N}{N!} \qquad (2.5)$$

Atunci P este un polinom algebric de grad cel mult N. Se observă că $P^{(k)} = 0$, pentru $k \geq N$. Astfel, putem presupune că $n \leq N$, chiar mai mult, prin adăugare de coloane

pline cu 0-uri, putem presupune că $n = N$.
O matrice cu numărul de 1-uri egal cu numărul de coloane se va numi matrice *normal*.
Pentru o matrice normală și sistemul (2.5), cu $N = n$, determinantul sistemului (2.3.1) este egal cu

$$D(E, X) = det[\frac{x_i^{-k}}{(-k)!}, ..., \frac{x_i^{n-k}}{(n-k)!}; e_{i,k} = 1] \qquad (2.6)$$

unde vom folosi convenția de a înlocui $\frac{1}{r!}$ cu 0, dacă $r \leq 0$. Astfel, rândul corespunzător perechii (i, k) din matricea $D(E, X)$ conține k zerouri, pe primele poziții. Determinantul sistemului este un polinom în variabilele x_i. Dacă $D(X, E)$ nu este identic nul, atunci se anulează într-un set închis care nu este dens, de măsură Lebegue. Astfel, putem aplică LEMA1; dacă E este "tare" singulară, atunci $D(E, X)$ își schimbă semnul pentru una din variabilele x_i, dacă restul variabilelor sunt fixate.

Fie a, α numere reale arbitrare. Vom scrie că $aX = \{ax_1, ax_2, ..., ax_m\}$; $X + \alpha = \{x_1 + \alpha, x_2 + \alpha, ..., x_m + \alpha\}$, unde $X = \{x_1, x_2, ..., x_m\}$.

Sunt valabile următoarele proprietăți:
Determinantul $D(E, X)$ este un polinom omogen în $x_1, x_2, ..., x_m$ de grad

$$1 + 2 + ... + n - \sum_{e_{i,k}=1} k = \rho$$

și satisface, pentru orice a, α :
(i)$D(E, aX) = a^\rho D(E, X)$, (2.7.2)
(îi) $D(E, X + \alpha) = D(E, X)$. (2.7.3)
Pentru (i), este suficient să scoatem factorul a^{-k} de pe linia (i, k) a determinantului $D(E, aX)$, iar apoi, din determinantul obținut, să scoatem factorul a^r, pentru fiecare coloana r.
Pentru (îi), observăm că $D(E, X + \alpha)$ este un polinom în α. Dacă vom calcula derivata acestui polinom, observăm că derivata fiecărei coloane este coloana precedentă. Derivata primei coloane este 0. Astfel, rezultă că $D(E, X + \alpha)$ este independent de α.
Se poate deduce că aplicând transformări linaire asupra determinantului $D(E, X)$, acesta se înmulțește cu o constantă diferită de 0. Rezultă imediat că proprietatea de singularitate "tare" sau "slabă" nu depinde de alegerea intervalului $[a, b]$.
Complementul algebric al ultimei coloane a determinantului $D(E, X)$, este notat cu $D_{i,k}(X)$. Acesta diferă doar prin semn de matricea $D(E_{i,k}, X)$, unde $E_{i,k}$ este matricea E, dar din care am înlocuit $e_{i,k} = 1$ cu 0, și eliminând ultima coloana a lui E.
Aplicând formulă (2.7.3) minorilor, obținem

$$D(E,X) = det[\frac{(x_i+\alpha)^{-k}}{(-k)!}, ..., \frac{(x_i+\alpha)^(n-k-1)}{(n-k-1)!}, \frac{(x_i^{n-k})}{(n-k)!}; e_{i,k} = 1]$$

.

Folosind inducție după n obținem un rezultat mai general:

$$D(E,X) = det[\frac{(x_i+\alpha_0)^{-k}}{(-k)!}, ..., \frac{(x_i+\alpha_1)^(n-k-1)}{(n-k-1)!}, \frac{(x_i^{n-k})+\alpha_n}{(n-k)!}; e_{i,k} = 1]$$

Exemple.

Matricea $(n+1)\times(n+1)$ a unei probleme de interpolare Lagrange are 1 pe toate pozițiile $e_{i,0} = 1, i = 1, ..., n+1$. Determinantul $D(E,X)$ al problemei de interpolare este determinantul Vandermonde

$$det[1, \frac{x_i}{1!}, ..., \frac{x_i^n}{n!}] = \prod_{i>j}(x_i - x_j) \neq 0$$

Matrice Taylor $1 \times (n+1)$ este de asemenea regulară, având $D(E,X) = 1$. Pentru un sistem arbitrar G și $X = \{x\}$, determinantul mattricei Taylor este Wronskianul

$$D(E,X) = W(x) = det[g_0^{(k)}(x), ..., g_n^{(k)}(x); k = 0, ..., n]$$

Pentru $X = \{0, x, 1\}$ cu $0 \leq x \leq 1$, cu sistemele:

$$E_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$$E_2 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$E_3 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

(Exemplul *)

Se observă că E_1 este tare regulară, iar E_2 este slab regulară. Ultimul Sistem are $D(E_3, X) = x(x-1)(15x^2 - 15x + 4)$, iar pentru $0 \leq x \leq 1$, $D(E_3, X) \neq 0$, deci este sistem regular.

4.2.1 Condiţiile Polya şi Matricele Birkhoff

Fie E o matrice $m \times (n+1)$ de interpolare. Fie $m_k = \sum_i e_{i,k}$, numărul de 1-uri de pe coloana k, şi fie

$$M_r = \sum_{k=0}^{r} m_k = \sum_{k=0}^{r} \sum_{i=0}^{m} e_{i,k}$$

numărul de 1-uri de pe coloanele matricei E cu numărul $0, 1, ..., r$. Pentru maticele normale (cu număr de linii egale cu număr de coloane), condiţia *Polya* este

$$M_r \geq r+1, r = 0, 1, ..., n \qquad (2.8).$$

Se observă că $M_n = n+1$. Dar $M_n = \sum_{k=0}^{n} m_k$ şi scăzând din $M_r = \sum_{k=0}^{r} m_k \geq r+1$, se obţine

$$\sum_{k=r+1}^{n} m_k \leq n - r \qquad (2.8.1)$$

Această inegalitate o vom denumi condiţia Polya superioară (care va fi folositoare pentru matrici cu mai puţin de $n+1$ de 1). Rezultă că o submatrice E_1 a lui E satisface (2.8.1) dacă E satisface (2.8.1).
Vom arată că *Polya* este condiţia *necesar* pentru regularitatea perechii (E, X).

PROPOZIŢIA 1.
Condiţiile Polya

$$M_r \geq r+1, r = 0, 1, ..., n$$

sunt necesare pentru ca perechea (E, X) să fie regulară, dacă sistemul G este cel stabilit în cazul algebric din secţiunea anterioară.

Demonstraţia 1.
Într-adevăr, să prsupunem că (2.8) nu sunt îndeplinite. Atunci $M_r \leq r$, pentru cel puţin

un $r, r \leq n$. Fie P_r un polinom de grad cel mult r. Atunci $P_r^{(k)}(x_i) = 0$ pentru $k \geq r$. Pe de altă parte, din presupunerea făcută, rezultă că în primele r rânduri avem cel mult r de 1, adică sunt cel mult r ecuații de formă $P_r^{(k)}(x_i) = 0, e_{i,k} = 1$, cu $k \leq r$.
Dar orice sistem omogen linear cu r ecuații și $r+1$ necunoscute are soluții netriviale (necunoscutele fiind tocmai cei $r+1$ coeficienți ai sistemului). Rezultă că există un polinom de grad cel mult $r, r \leq n$ ce este anulat de perechea (E, X).

Demonstratia 2.
Am făcut mai sus observația că rândul corespunzător perechii (i, k) începe cu k zerouri. Dacă $M_r \leq r$, atunci sunt cel mult r rânduri corespunzatore perechilor (i, k) cu $k \leq r$. Rezultă că toate rândurile, mai puțin r dintre ele încep cu $r+1$ zerouri. Primele $r+1$ coloane ale matricei $D(E, X)$ sunt liniar independente, deci $D(E, X) = 0$.

Deoarece s-a dovedit a fi dificil să se decidă când E este regulară, adică când $D(E, X) \neq 0, \forall X \in R^n$, s-a încercat să se răspundă la o întrebare mai simplă, și anume când este E condițional regulară. Echivalent, când $D(E, X)$ nu este identic nul sau $D(E, X) \neq 0$, pentru anumiți X.
Avem următoarea teoremă a lui Ferguson și Nemeth:

TEOREMA 1.
(a)O matrice normală care este condițional regulară pentru interpolare albegbrica, trebuie să satisfacă condițiile lui Polya.
(b)Dacă Wronskian-ul sistemului G nu este identic nul, și E satisface condițiile Polya, atunci E este condițional regulară. În particular, o matrice este condițional regulară pentru interpolare algebrică dacă și numai dacă satisface condițiile lui Polya. (în cazul algebric, s-a stabilit formă sistemului G)

O matrice normală satisface condițiile $Birkhoff$ dacă

$$M_r \geq r+2, r = 0, 1, ..., n-1 \qquad (2.9)$$

Pentru $n \geq 1$, condiția de mai sus presupune că prima coloană a lui E să conțină cel puțin doi de 1, și $M_{n-1} = M_n = n+1$. Condițiile se opresc la $r = n-1$ deoarece ultima coloana a lui E este plină de 0.
O matrice care satisface condițiile Polya sau Birkhoff se va numi simplu matrice $Polya$ sau $Birkhoff$, respectiv. Dintr-o matrice Birkhoff E, putem obține o matrice Polya $m \times n$ dacă un 1 în E este înlocuit cu 0, iar ultima coloană a lui E este omisă.
O matrice normală E este *decompozabil*, $E = E_1 1 \oplus E_2 2$ dacă poate fi împărțită vertical

în două matrici normale E_1, E_2, unde E_1 are $r+1$ coloane și conține exact $r+1$ valori de 1, iar E_2 conține $n-r$ coloane și are exact $n-r$ valori egale cu 1. Asta înseamnă că $M_r = r+1$. Rezultă că o matrice Polya E nu este decompozabilă, dacă și numai dacă nu satisface condițiile $Birkhoff$.
Pentru $E = E_1 \oplus E_2$, fie $A(X, E)$ sistemul de puteri. Rearanjăm rândurile matricei să avem primele $r+1$ rânduri corespunzătoare lui $e_{i,k} = 1$ din E_1, în ordine lexicografica, și annalog pentru E_2.

$$A(E, X) = \begin{pmatrix} A(E_1, X) & 0_{(r+1)X(n-r)} \\ 0_{(r+1)X(n-r)} & A(E_2, X) \end{pmatrix}$$

Fie X_1, X_2 submultimi ale lui X relevante pentru E_1, respectiv E_2, adică valorile din X care nu au corespunzătoare coloane de 0 în E_1, E_2. Rezultă că

$$D(E, X) = D(E_1, X_1)D(E_2, X_2) \qquad (2.10)$$

Rezultă astfel, o teorema datorată lui $Atkinson - Sharma, Ferguson$.

TEOREMA 2.
O matrice decompozabilă $E = E_1 \oplus E_2$ este regulară pentru interpolare albegrica dacă și numai dacă fiecare dintre componentele sale E_1, E_2 este regulară. Dacă vreuna din componentele sale este singulară, rezultă că E este singulară.
Este evident că

$$rang(A(E, X)) \geq rang(A(E_1, X_1)) + rang(A(E_2, X_2)) \qquad (2.11)$$

De o importanță majoră este descompunerea canonică $E = E_1 \oplus E_2 \oplus ... \oplus E_\mu$ a unei matrici Polya. Această descompunere este unică. Folosind definiția cu defectul, avem că pentru orice mulțime X,

$$rang(A(E, X)) \geq \sum_{\lambda=1}^{\mu} rang(A(E_\lambda, X_\lambda)) \geq (n+1) - \sum_{\lambda=1}^{\mu} d(E_\lambda)$$

Rezultă că $d(E) \leq \sum_{\lambda=1}^{\mu} d(E_\lambda)$ (2.12).

Exemple.
1. Matricea Abel $(n+1) \times (n+1)$ de interpolare, E, are un singur 1 în fiecare coloana. Descompunerea ei canonică constă în matrici normale cu coloane de 1. Conform cu TEOREMA 2, aceasta este regulară.

2. Pentru polinoame $n = mp - 1$, presupunem că avem derivatele $P^{(sp)}(x_i), s = 0, ..., m-1$ în p puncte distincte. Astfel, matricea de interpolare este regulară deoarece matricele din descompunerea canonică sunt matrici $p \times p$ Langrange.

4.2.2 Teoreme de Regularitate

Vom stabili, pentru cazul algebric, noi condiții de regularitate. Fie

11100110100

una din liniile lui E. Această conține 3 secvențe de 1-uri. Două dintre ele sunt *impare* (conțin un număr impar de 1) iar una este pară. Prima din cele 3 secvențe este 0 secvență Hermite (începe din coloana 0).
O secvență de pe linia i este *suport* dacă există valori de 1 în E, atât la nord-vest cât și la sud-vest față de primul element din secvență. Mai exact, dacă (i, k) este poziția primului element din secvență de 1-uri, trebuie să existe $e_{i_1,k_1} = e_{i_2,k_2} = 1$, cu $i_1 \leq i \leq i_2$ iar $k_1 \leq k$, $k_2 \leq k$. Reiese imediat că că prima sau ultima linie sau orice altă linie care începe cu 1 nu poate fi suport.

TEOREMA 3. O matrice normală de interpolare este ruglară la interpolare algebrică dacă satisface condițiile Polya și nu conține secvențe suport de lungime impare.
Demonstrația este una foarte interesantă, și nu este altceva decât o formă sofisticată a teoremei lui Rolle. Vom folosi următoarele:

LEMA 1. Între două rădăcini ale unei funcții analitice f, există un număr impar de rădăcini ale funcției f'.

Demonstrație.
Fie (x_0, x_1) cele două rădăcini consecutive ale lui f, cu x_0, x_1 numere reale. Pe intervalul (x_0, x_1) funcția f păstrează semn constant. Presupunem fără a restrânge generalitatea că f este pozitivă. În mod necesar, $f'(x) \geq 0$ pentru x într-o vecinătate a lui $x_0, x \geq x_0$ și $f'(x) \leq 0$ pentru x într-o vecinătate a lui $x_1, x \leq x_1$.
Rezultă că f' își schimbă semnul pe intervalul (x_0, x_1). Dacă f' are avea un număr par de rădăcini pe intervalul (x_0, x_1) atunci semnul pe vecinătatea lui x_0 ar coincide cu semnul pe vecinătatea lui x_1. Contradicție.

O funcție f este anulată de o matrice $m \times (n+1)$ de interpolare E și o mulțime X de noduri dacă are loc

$$f^{(k)}(x_i) = 0, e_{i,k} = 1 \qquad (2.13)$$

LEMA 2. Fie f o funcție anulată de E, X, cu $|E| \geq n+1$ și $X \in [a,b]$. Dacă E nu are secvențe suport de lungime împăra, atunci fie $f^{(n)}(\epsilon) = 0$, pentru un anumit $x_1 \leq \epsilon \leq x_m$ sau există o matrice $\mu \times n$ de interpolare E' cu cel puțîn n de 1 și care să nu conțînă secvență suport de lungime impară și o mulțime $X' = \{x'_1, x'_2, ..., x'_\mu\}$, cu $x_1 \leq x'_1, x'_\mu \leq x_m$ și cu elemente din intervalul $[a,b]$ care să anuleze f'.

Demonstrație.
Presupunem că (2.13) nu este adevărată. Dacă colana 0 a lui E are cel puțîn 2 valori de 1, fie α, β zerourile extreme ale lui f pe $[a,b]$ ce aparțîn lui X. Putem presupune că toate zeorurile lui f pe $[a,b]$ se află în X, altfel, le putem adaugă în X și vom introduce în E noi linii de tipul (1, 0, ..., 0). Astfel, dacă o secvență este suport atunci adăugând rânduri noi ea va rămâne tot suport în nouă matrice E.
Omitem în E coloana 0. Dacă coloana conține mai puțin de doi de 0 atunci fie $E^{'}$ matricea rămasă. Altfel, putem presupune că există $\alpha \leq \beta$ cu α, β elemente în coloana 0 a matrice E. Astfel, $E^{'}$ va conține niște valori de 1 în plus. Fie $\gamma \leq \delta$ două zerouri consecutive ale lui f pe intervalul $[\alpha, \beta]$. Dacă ϵ, $\gamma \leq \epsilon \leq \delta$ este un zero a lui $f^{'}$, atunci acesta va avea în E ca și corespondent un 1 care începe o secvență suport într-o anumită coloana. Această secvență este pară și se termină cu un 1 pe o poziție $\leq n$, altfel, ar avea loc relația (2.13).
Numărul total de zerouri ale lui f' în intervalul (γ, δ) este par. Dar conform Lemei 1, numărul de zerouri trebuie să fie impar. Rezultă că există un 0 în plus a lui f', care nu apare un mulțime X, sau e un zero cu un ordin de multiplicitate mai mare decât 1. Introducem în E' câte un 1 pentru fiecare astfel de zero "absent", valoare ce va fi inserată la final de fiecare secvență pară. Nouă mulțime X' este obținută prin adăugarea zerourilor ale lui f' la X, și prin eliminarea acelor x_i care nu sunt zerouri ale lui $f^{(r)}$, $r = 1, 2, ..., n$. În mod evident, E' are cel puțîn n valori de 1 și fiecare secvență suport în E' este secvență suport și în E, dat fiind faptul că E' nu are secvențe suport impare.

Pentru E, f că în Lema 2, există un ϵ, $x_1 \leq \epsilon \leq x_m$ pentru care $f^{(n)}(\epsilon) = 0$. (***)
Să ne întoarcem acum la demonstrația teormei 3.
Fie E o matrice $m \times (n+1)$ de interpolare ce satisface ipotezele teoremei, iar mulțimea X a valorilor una arbitrară. Fie P un polinom anulat de E, X. Aplicăm (***) pentru P și E_r, unde E_r este matricea formată din primele $r+1$ coloane ale lui E. Matricea

E_r satisface condițiile din Lema 2, sau conține un element $e_{i,r} = 1$ pentru un anumit i. Atunci, pentru fiecare $r = 0, ..., n$ este valorile ϵ_r, cu $x_1 \leq \epsilon_r \leq \epsilon_m$ cu proprietatea că $P^{(r)}(\epsilon_r) = 0$. Pentru $r = n$ se obține că x^n are coeficient nul în P. Inductiv se arată ușor că P este polinomul identic nul. Deci P este identic nul și E este regulară.

Exemple.
1. O matrice E de tipul Lagrange, Taylor, Hermite sau quasi-Hermitiană nu are secvențe suport și deci este regulară pentru polinoame de grad corespunzător.
2. O matrice Polya cu două linii nu are secvențe suport deci este regulară. În acest caz condițiile lui Polya sunt necesare și suficiente pentru regularitatea a matricelor cu două linii.
3. Matricea din (Exemplul *) arată că nu sunt necesare condițiile Teoremei 3. Există matrici normale regulare ce conțîn secvențe suport impare.

Fie $E = E_1 \oplus E_2 \oplus ... \oplus E_\mu$ descompunerea canonică a lui E, despre care presupunem că este o matrice Polya. O secvență suport de 1 în E se va numi *esențial* dacă este conținută în întregime în una din matricele E_λ, și este de asemenea secvență de suport împără în E_λ.
Avem următoarea teorema.

TEOREMA 4. O matrice Polya este regulară pentru X ordonată pentru interpolare algebrică dacă nu conține secvențe suport impare de 1.

4.2.3 Polinomul de interpolare

Putem obține ușor formula polinomului ce rezolvă problema de interpolare. Vom obține polinomul în cazul în care datele $c_{i,k}$ sunt valorile derivatelor unei funcții cunoscute $c_{i,k} = f^{(k)}(x_i)$, pentru $e_{i,k} = 1$, unde $f \in C^n[a.b]$. Folosind faptul că P, polinomul de interpolare, este o combinație liniară a funcțiilor din sistemul G, obținem relația:

$$a_0 g_0(t) + ... + a_N g_N(t) = P(t)$$

Eliminând coeficienții a_k obținem :

$$P(t) = \sum_{j=0}^{N} \frac{D(E, X, G_j)}{D(E, X)} g_j(t) \qquad (2.14)$$

unde G_j este mulțimea funcțiilor $\{g_0, g_1, ..., g_N\}$ în care g_j a fost încolcuit cu valorile lui f.

Muhlbach a găsit o formulă simplă de a reduce problema de interpolare cu o matrice Birkhoof E la o problema de interpolare cu o matrice mai mică dacă $G = \{1, x, ..., x^n/n!\}$. Presupunem că perechea E, X este regulară și că o submatrice $E_{i_0,k_0} = E^*$ a lui E este regulară, unde E^* a fost obținută prin înlocuirea elementului $e_{i_0,k_0} = 1$ cu $e_{i_0,k_0} = 0$ și s-a omis ultima coloana. Fie $g_n(t) = t^n/n!$ și fie $P_n(f, E, X; t) = P_n(t)$ polinomul care interpoleaza funcția $f \in C^n$. Atunci

$$P_n(f, E, X; t) = P_{n-1}(f, E*, X; t) + c[g_n(t) - P_{n-1}(g_n, E*, X; t)] \qquad (2.15)$$

unde c este o constanța,

$$c = \frac{f^{(k_0)}(x_{i_0}) - P_{n-1}^{(k_0)}(f, E^*, X; x_{i_0})}{g_n^{(k_0)}(x_{i_0}) - P_{n-1}^{(k_0)}(g_n, E^*, X; x_{i_0})}$$

Într-adevăr, fie $Q(t)$ membrul drept a relației (2.15). Dacă $e_{i,k}^* = 1$, avem că $Q^k(x_i) = f^{(k)}(x_i)$, din definiția lui P_{n-1}. Totodată $Q^{k_0}(x_{i_0}) = f^{(k_0)}(x_{i_0})$ din definiția lui c. Rămâne să verificăm că c este bine definit.

Dacă numitorul din expresia lui c este egal cu 0, atunci polinomul de grad $n-1$ $P_{n-1}(g_n, E^*, X; t)$ ar interpola de asemenea $g_n = t^n/n!$ pentru perechea E, X. Cum E, X este regulară, am avea că $g_n(t) = P_{n-1}(g_n, E^*, X; t)$, ceea ce este o contradicție.

Capitolul 5

Scheme de partajare ierarhice

O schemă (k, n) cu prag cu n participanți, U, este o metodă de partajare a secretelor astfel încât oricare k participanți să poată recupera secretul prin punerea în comun a share-urilor și totodată orice mulțime cu mai puțin de k marticipanti să nu poată recupera secretul.

Partajarea de secrete generalizată presupune situații în care mulțimile ce pot reconstrui secretul au proprietatea de monotonicitate. Astfel, dacă mulțimea $A \in \Sigma$ poate reconstrui secretul, atunci dacă $A \in B \in U$ rezultă că $B \in \Sigma$. Prin Σ am notat toate mulțimile de participanți ce pot reconstrui secretul. Σ se numește mulțime autorizată și orice mulțime inclusă în Σ poate reconstrui secretul și totodată orice mulțime inclusă în U dar care nu este inclusă în Σ nu poate reconstrui secretul.

Unul din scenariile în care poate apărea partajarea ierarhică de secrete poate fi următorul:

pentru a partaja o cheie secretă în rândul angajaților în cadrul unei bănci și pentru recuperarea ei este nevoie de (cel puțin) 3 angajați dintre care cel puțîn unul trebuie să fie manager de departament (iar restul pot fie jos în grad).

Definiția 3.1

Fie U mulțimea de n participanți despre care presupunem că este împărțită pe nivele $U = \bigcup_{i=0}^{m} U_i$, unde $U_i \cap U_j = \emptyset$ pentru orice i, j cu $0 \leq i \leq j \leq m$. Fie $K = \{k_i\}_{i=0}^{m}$ un șir crescător de numere întregi pozitive, $0 \leq k_0 \leq k_1 \leq ... \leq k_m$. Atunci sturctura de acces a schemei (K, n) ierahice este:

$$\Gamma = \{V \subset U : |V \cap (\bigcup_{j=0}^{i} U_j)| \geq k_i, \forall i \in \{0, 1, ..., m\}\} \qquad (3.1.1)$$

Structura ierarhică corespunzătoare este o schemă care realizează structura de acces, adică o metodă de a asigna fiecărui participant $u \in U$ un subsecret(share) $\sigma(u)$ a unui secret S astfel încât orice mulțime autorizată $V \in \Gamma$ să poată recupera secretul folosind mulțimea lor de share-uri: $\sigma(V) = \{\sigma(u), u \in V\}$, iar orice mulțime neautorizată ce nu se află în Γ să nu poată afla nici o informație cu privire la secretul partajat. Considerând acum secretul S o variabilă aleatorie ce ia valori dintr-un domeniu finit, se definesc pentru schemă ierarhică următoarele noțiuni similare cu cele din Capitolul 1:

$$(i)H(S|\sigma(V)) = 0, \forall V \in \Gamma \quad (accesibilitate) \qquad (3.1.2)$$

$$(ii)H(S|\sigma(V)) = H(S), \forall V \notin \Gamma \quad (securitate \ \ perfect) \qquad (3.1.3)$$

.

Fie Σ_u mulțimea tuturor share-urilor posibile ale participanților din U. Atunci rată informației a schemei va fi $\rho = \min_{u \in U} \frac{log_2|S|}{log_2|\Sigma_u|}$.
Dacă $\rho = 1$ schemă se numește ideală.
Condiția (3.1.2) este înțeleasă precum "V poate recupera secretul S", $\rho = 1$ implică situația ideală când mărimea share-urilor este aceeași cu ceea a secretului.

Problema structurilor ierarhice (sau multilevel) a fost studiată de către Shamir care a observat că în cazul anumitor situații de partajare a secretelor ar fi de dorit că fiecare utilizator să aibă autoritate personalizată (în funcție de nivelul de securitate pe care se află). A sugerat că acest lucru să fie realizat prin acordarea mai multor share-uri participanților de nivel înalt. Astfel, dacă U are structura ierarhică definită în (3.1.1), participanții de pe nivelul i, $U_i, 0 \leq i \leq m$ vor primi w_i share-uri de formă $(u, P(u)), u \in F$ unde șirul $(w_i)_{i \geq 0}$ are proprietatea că $w_0 \geq w_1 \geq ... \geq w_m$. Rezultă că rată informației este egală cu $1/w_0$. Rezultă că pentru a tinde spre a fi ideală, schemă ar trebui să aibă puțini utilizatori pe nivelele înalte.
Simmons și Brickell au imaginnat o altă setare ierarhică având în vedere scenariul unui transfer bancar în care transferul se poate efectua atunci când contribuie 2 vice-președinți sau 3 consilier bancari. Un alt scenariu posibil și natural ar fi cel în care 1 vice-președinte și 2 consilieri pot efectua transferul. Astfel au apărut două clase a partajării ierarhice: structuri ierarhice în *conjuncție* (conjunctive) și structuri ierarhice în *disjuncție* (disjunctive).
Definiția schemelor conjuctive rămâne cea din relația (3.1.1), pe când definiția schemelor disjunctive devine următoarea:

$$\Sigma = \{V \subset U | \exists i \in \{0, 1, ..., m\} : |V \cap (\bigcup_{j=0}^{i} U_j)| \geq k_i\} \qquad (3.1.4)$$

În continuare voi prezența schemă lui Tassa de paratajare ierarhică bazată pe interpolare

Birkhoff.

5.0.1 Schemă lui Tassa

Reamintim aici interpolarea Birkhoff
(*)$X = \{x_1, x_2, ..., x_k\}$ o mulțime de puncte din R ordonate, cu $x_1 < x_2 < ... < x_k$
(*)$E = (e_{i,j}{}_{i=0}^{k}{}_{j=0}^{l}$ o matrice cu valori de 1 și 0, și fie $I(E) = \{(i,j)|e_{i,j} = 1\}$ și $d = |I(E)|$
(*)$C = \{c_{i,j}|(i,j) \in I(E)\}$
Problema de interpolare ce corespunde tripletului $< X, E, C >$ este cea de a găsi polinomul de grad $d-1$, $P \in R[X]$ care satisface cele d egalități:

$$P^{(j)}(x_i) = c_{i,j}$$

Reamintesc că interpolarea Birkhoff poate să nu aibă soluție unică. Soluția se obține rezolvând sistemul $Ax = b$, unde x este vectorul coeficientilor polinomului P.
Pentru a recupara seceretul, avem nevoie că de pe fiecare nivel, U_i să participe cel puțin k_i participanți. Tot așa, pentru a rezolva interpolarea Birkhoff, este nevoie că pe primele k coloane să fie $k+1$ valori de 1. Din acest motiv, considerăm matricea E cu k_m coloane, unde k_m este valoarea maximă a pragului pe cele m nivele. Știm că *Polya* sunt condițiile necesare pentru a avea soluție la problema de interpolare. Se observă, așadar, echivalenta dintre condițiile Polya și definiția schemei conjunctive de interpolare.
În capitolul 2 al lucrării am ajuns la concluzia că pentru a avea soluție unică, problema interpolării în cazul algebric trebuie să aibă matricea E fără secvențe suport de lungime impară. Dar demonstrația acestei teoreme se bazează pe ordinea numerelor din R (această fiind o consecință a teoremei lui Rolle). Schemă lui Tassa va fi definită pe corpuri cu elemente întregi, deci nu avem ordine. Așadar, nu putem aplică teorema respectivă.
Ca și contraexemplu, fie problema de interoplare cu următoarele date:
$X = \{1, 2, 4\}$,

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

Astfel, vom cauta polinomul P, cu $deg(P) = 2$, $P = a_2x^2 + a_1x + a_0$ ce satisface
$P(1) = c_{1,0}, P(2) = c_{2,0}, P'(4) = c_{3,1}$

. Scriind matricea sistemului de mai sus, obținem,

$$A(E,X) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 0 & 1 & 8 \end{pmatrix} \tag{5.1}$$

Este ușor de văzut că matricea E nu are secvențe suport de lungime impară. Se calculează imediat că $det(A(E,X)) = 5$. Totuși, dacă facem setup-ul în F_5, matricea $A(E,X)$ devine neinversabila, și astfel perechea (E,X) devine singulară.
Fie schema de partajare ierarhică dată de (K,n), unde $K = \{k_i\}_{i=0}^{m}$. Fie F un corp finit de dimensiune q, unde q este cel puțîn egal cu numărul de secrete posibile. Fie $k = k_m$ numărul de participanți necesari pentru recuperarea unui secret. Atunci schemă lui Tassa va fi următoarea:

1. Dealer-ul selectează aleator polinomul $P \in F_{k-1}[x]$, unde

$$P(x) = \sum_{i=0}^{k-1} a_i x^i, \quad a_0 = S \qquad (3.2.1)$$

2.Dealerul atribuie fiecărui participant $u \in U$ un element al corpului F. Din motive de simplitate, vom presupune că participantul u are identitatea u. Astfel, U devine submultime a lui F.

3.Dealer-ul distribuie participanților share-uri în următorul mod:
Fiecare participant de pe nivelul i din ierarhia de nivele, $u \in U_i$, $0 \leq i \leq m$ primește share-ul $P^{(k_{i-1})}(u)$, adică derivată polinomului P de ordinul nivelului anterior. Facem convenția că $k_{-1} = 0$, adică participanții de pe cel mai înalt nivel vor primi derivatele de ordin 0 ale polinomului.

Derivată unui polinom definit peste un corp $F[x]$ este definită astfel :

$$P'(x) = \sum_{i=0}^{k-1} i a_i x^{i-1}$$

.

Exemplu.
Fie o ierarhie pe 3 nivele $U = U_0 \cup U_1 \cup U_2$ cu nivelurile $K = \{k_0, k_1, k_2\} = \{2, 4, 7\}$. Mulțimea autorizată, V trebuie să fie formată din 7 participanți dintre care cel puțin 4

trebuie să fie de pe nivelele $U_0 \cup U_1$ și cel puțin 2 de pe nivelul U_0 (evident, din definiție participanții de pe nivelurile mai importante pot înlocui participanții de pe nivelulurile inferioar).

Cum $k = 7$, dealur-ul va selecta un polinom de grad 6, $P(x) = \sum_{i=0}^{6} a_i x^i$, unde $a_0 = S$ este secretul partajat. Conform pasului 3 al schemei, participanții de pe nivelul 0, U_0, vor primi $P(u)$, unde u este identitatea participantului. Deoarece pragul nivelului 0 este 2, rezultă că participanții de pe nivelul 1, U_1 vor avea că share $P^{(2)}(u)$. Deoarece pragul nivelului 1 este 4, rezultă că participanții de pe nivelul 2, U_2 vor primi că share $P^{(4)}(u)$. Schemă este ideală deoarece participantiii primesc share-uri din aceeași mulțime din care este ales și secretul S. Schemă lui Shamir prezentată în primul capitol este un caz particular al schemei lui Tassa, pentru cazul în care avem un sigur nivel, U_0, deci nu sunt implicate derivatele polinomului.

Vom urma ordinea ideilor din primul capitol și vom schița demonstrația de securitate a schemei, după care voi încerca să aduc scheme noi care să reproducă proprietățile schemei lui Shamir.

5.0.2 Demonstrație de securitate

Pentru a demonstra securitatea schemei lui Tassa trebuie să avem în vedere condițiile (3.1.2) și (3.1.3). Fie $v = |V|$ cardinalul unei mulțimi autorizate a schemei de partajare, deci $V = \{u_1, u_2, ..., u_v\}$. Presupunem că

$$\begin{aligned} u_1, .., u_{l_0} &\in U_0 \\ u_{l_0+1}, ..., u_{l_1} &\in U_1 \\ &... \\ &... \\ &... \\ u_{l_{m-1}+1}, ..., u_{l_m} & \end{aligned}$$

unde $0 \leq l_0 \leq l_1 \leq ... \leq l_m = v$ iar l_i reprezintă numărul de participanți de pe nivelul i din mulțimea autorizată. Se observă imediat că V este autorizată dacă $l_i \geq k_i$ (adică avem cel puțin k_i participanți în mulțimea autorizată din nivelul i, U_i). Fie $r(x) = (1, x, x^2, ..., x^{k-1})$ și pentru fiecare $i \geq 0$, notăm cu $r(i)$ derivată de ordin i a vectorului. Astfel, folosind această notație, observăm că participantul $u \in U_i$ are share-ul $\sigma(u) = r^{(k_{i-1})}(u)a$, unde a este vectorul coeficientilor lui P, $a = (a_0 = S, a_1, ..., a_{k-1})$. Astfel, când participanții își pun la comun share-urile, ei trebuie să rezolve sistemul ce are că soluție vectorul a. Sistemul este $M_V a = \sigma$, unde

$$M_V = \begin{pmatrix} r(v_1) & ... & r(v_{l_0}) \\ r^{(k_0)}(v_{l_0+1}) & ... & r^{(k_0)}(v_{l_1}) \\ ... & ... & ... \\ r^{(k_{m-1})}(v_{l_{m-1}+1}) & ... & r^{(k_m)}(v_{l_m}) \end{pmatrix}$$

iar $\sigma = (\sigma(v_1), \sigma(v_2), ..., \sigma(v_{l_m}))^T$.

Propoziția 1. Problema de interpolare ce trebuie rezolvată de o mulțime autorizată trebuie să satisfacă condițiile lui Polya. Invers, problema de interpolare ce este rezolvată de un grup neautorizat, nu tebuie să satisfacă condițiile Polya.

Demonstrație.
Fie V o mulțime autorizată și e t un număr astfel încât $0 \leq t \leq k_{m-1}$. Cum pragurile nivelelor sunt în ordne strict crescătoare $k_{-1} = 0 \leq k_0 \leq k_1 \leq ... \leq k_m$, rezultă că există $i, 0 \leq i \leq m$ cu $k_{i-1} \leq t \leq k_i$. Astfel, în V se află derivate de ordin cel mult t ale lui P, $P^{(t)}$ în $|V \cap (\cup_{j=0}^{i} U_j)|$ puncte. Dar cum $V \in \Gamma$, adică V ete autorizată, trebuie să avem în V cel puțin k_i participanți de pe niveluri cel puțin la fel de importante că nivelul i, deci $|V \cap (\cup_{j=0}^{i} U_j)| \geq k_i \geq t + 1$, așa cum se impune în codițiile lui Polya.
Acum, fie V o mulțime neautorizată. Deci există un $i, 0 \leq i \leq m$ astfel încât $|V \cap (\cup_{j=0}^{i} U_j)| \leq k_i$. În acest caz, condițiile lui Polya nu sunt indeplinitite pentru derivate de ordin $j, j \geq i + 1$.

Presupunem în continuare că există un utilizator special, u_0 din cel mai înalt nivel, U_0. Vom studia regularitatea matricei $A(E, X)$ peste F_q.

Teorema 1. Fie $u_0 \in U_0$, și presupunem că matricea M_V este regulara în F_q ($det(M_V) \neq= 0$). Atunci condițiile (3.1.2) și (3.1.3) sunt îndeplinite.

Demonstrație.
Fie V o mulțime autorizată minimală, adică $|V| = k(= k_m)$ ce nu conține elementul u_0. Dacă V este minimală, rezultă că V este o matrice pătrătica și este regulară (deoarece mulțimea de particpanti din V este autorizată). Rezultă că participanții din mulțimea autorizată pot recupera secretul coeficientii polinomului P, deci și secretul S. Dacă V nu este minimală, $|V| \geq k$, atunci există submultimea $V_0 \subset V$, cu $|V_0| = k$ care este autorizată. Astfel, cum cele $|V|$ ecuații din sistemul $M_V a = \sigma$ sunt consistente, și cum M_{V_0}

este rugulara, rezultă că soluția a a sistemului este unică. Rezultă de aici prorpeitatea (3.1.2) de accesibilitate a schemei lui Tassa.

Fie V o submultime a mulțimii părților lui $(U - u_0) - \Gamma$ care nu este autorizată. Vom arată că dacă toți participanții din V își pun în comun share-urile, aceștia nu vor extrage nicio informație cu privire la secretul S. Fiecare mulțime neautorizată poate fi transformată în mulțime autorizată dacă îi adăugăm cel mult k particpanti în ea.

Fără a restrânge generalitatea, presupunem că lui V îi lipsește exact un singur participant pentru a deveni autorizată. Astfel, adăugând la V pe participantul u_0, mulțimea $V_1 = V \cup \{u_0\} \in \Gamma$ devine autorizată, deoarece am convenit că u_0 aparține celui mai înalt nivel din ierarhie.

Avem că $|V| = k - 1$ iar $|V_1| = k$. Matricea M_{V_1} este pătrătica și regulara deci liniile ei formează un sistem de vectori independenți liniar. Așadar, linia din M_{V_1} corespunzătoare utilizatorului u_0 este independentă de cele $k-1$ linii inițiale ale matricei V. Astfel, valoarea lui S este independentă de valorile puse la comun de cei $k - 1$ participanți din V.

Prespunem acum că $|V| \geq k - 1$. Presupunem că singurul participant care mai lipsește mulțimii V că această să fie autorizată este unul de pe nivelul j, $0 \leq j \leq m$. Avem $l_i \geq k_i, 0 \leq i \leq j-1, l_j = k_j - 1$ și $l_j \geq k_i - 1$ pentru $j + 1 \leq i \leq m$. (3.3.1). Cum $|V| = l_m \geq k - 1$, va rezultă că $l_m - l_j \geq k - k_j$. Toate cele $l_m - l_j$ ale matricei M_V care corespund participanților de pe nivelele de le $j+1$ până la m, au cel puțin k_j pe primele valori din linie, deoarece corespund derivatelor de ordin cel puțin k_j. Astfel, aceste linii aparțin unui subspatiu a lui F^k de dimensiune $k-k_j$. Putem extrage dintre acestea $k-k_j$ linii care vor genera același subspațiu ca cele $l_m - l_j$ linii inițiale. Fie W submultimea lui V de linii (corespunzătoare unor particpanti) nefolositoare în generarea subspatiului menționat anterior. Aceste linii se află printre ultimele $l_m - l_j$ linii ale matricei M_V și fie $V_0 = V \setminus W$. Din (3.3.1) avem

$$|V_0| = |V| - |W| = l_m - |(l_m - l_j) - (k - k_j)| = l_j + k - k_j = k - 1$$

.

În mod evident, eliminarea din V a participanților din W nu creează noi deficiențe și astfel mulțimii V_0, că și mulțimii V, îi lipsește tot un participant de pe nivelul j pentru a deveni autorizată. Folosind aceleași argumente că mai sus, se constată că u_0 este independent de celelalte linii ale matricei M_{V_0}. Dar spațiul generat de liniile lui M_{V_0} este același cu spațiul generat de liniile lui M_V. Așadar, u_0 va fi independent și față de participanții din V.

Rezultă așadar și proprietatea (3.1.3) de securitate perfectă.

5.0.3 Alocarea Identităților Participanților

O strategie de alocare a identităților participanților este cea random. Așadar, dacă $|U| = n$, iar $|F| = q$, atunci probabilitatea că două mulțimi de n elemente din F să coincidă este de

$$Prob(U = W) = \frac{1}{C_{q-1}^{n}}, \forall W \in F \setminus \{0\}, |W| = n$$

.

Teorema 2.
Fie V o mulțime arbitrată de participanți aleasă din 2^U. Atunci, dacă $V \in \Sigma$ avem

$$Prob(H(S|\sigma(V)) = 0) \geq 1 - \epsilon \qquad (3.4.1)$$
$$Prob(H(S|\sigma(V)) = H(S)) \geq 1 - \epsilon \qquad (3.4.2)$$

, unde $\epsilon = \frac{(k-2)(k-1)}{2(q-k)}$.

Demonstrație.
Dacă V este o mulțime autorizată, atunci ea conține o mulțime autorizată minimală, și fie aceasta $V_0 \subset V, |V_0| = k$, astfel încât dacă $det(M_{V_0}) \neq 0$, atunci mulțimea V de participanți poate recupera secretul. Pe de altă parte, dacă $V \notin \Gamma$, am văzut din Teorema 1 că dacă $u_0 \in U_0$, atunci există o mulțime autorizată minimală V_0 asfel încât $det(M_{V_0}) \neq 0$ implică că participanții din V nu pot afla secretul S. Astfel, pentru a demonstra (3.4.1) și (3.4.2), este suficient să demonstrăm că dacă $u_0 \in U_0$ și V este o m ultime autorizată minimală, atunci $det(M_{V_0})$ este nenul cu o probabilitate mai mare de $1 - \epsilon$, adică o probabilitate foarte aproopiata de 1.
Într-adevăr, fie V o mulțime autorizată minimală în care participanții sunt ordonați pe nivelele din ierarhie. Vom arăta următoarea:

$$Prob(deț(M_V) = 0) \leq \frac{(k-2)(k-1)}{2(q-k)} \qquad (*_1)$$

Evident, proprietatea de mai sus are loc pentru $k = 1$ și $k = 2$. Vom demonstra $*_1$ prin inducție după k. Avem două cazuri:
(i)Ultima linie din M_V este $r^{(h)}(v_k)$, unde $h \leq k-1$, și aceasta este posibilă dacă pragul penultimului nivel k_{m-1} verifică relația $k_{m-1} < k_m - 1$ sau dacă în V nu sunt participanți de pe ultimul nivel.
(ii)Ultima linie din M_V este $r^{(k-1)}(v_k)$ și această se întâmplă când $k_{m-1} = k_m - 1$
Dacă suntem în primul caz, considerăm $v = (v_1, ..., v_k)$ și $(v, v_k) = (v_1, ..., v_k)$ vectorul

participanților din V. Fie $\mu_{k-1} = \mu_{k-1}(v)$ determinantul minorului de ordin $k-1$ obținut din M_V care este obținut prin eliminarea ultimei linii și ultimei coloane din M_V. Astfel, dezvoltând determinantul după ultima linie, putem să îl scriem ca un polinom în v_k:

$$det(M_V) = \sum_{i=0}^{k-2-h} c_i v_k^i + \frac{(k-1)!}{(k-1-h)!}\mu_{k-1} v_k^{k-1-h} \qquad (3.4.3)$$

unde c_i este o constantă ce depinde de vectorul v. Fie Ω mulțimea tuturor vectorilor pentru care $\mu_{k-1} = \mu_{k-1}(v) = 0$. Atunci, folosind formulă probabilității totale, obținem că:

$$\begin{aligned} Prob(det(M_V) = 0) = &\sum_{v \in F^{k-1} \setminus \Omega} Prob(det(M_V) = 0|v) Prob(v) \\ &+ \sum_{v \in \Omega} Prob(det(M_V) = 0|v) Prob(v) \end{aligned} \qquad (3.4.4)$$

Dacă $v \in F^{k-1} \setminus \Omega$, atunci $det(M_V)$ este polinom de gradul $k-1-h$ în v_k, deci determinantul este nul în cel mult $k-1-h$ valori. Deci, pentru a calcula $Prob(det(M_V) = 0|v)$, cu $v \in F^{k-1} \setminus \Omega$, avem că numărul cazurilor favorabile este cel mult $k-1-h$. Cum participanții sunt distincți și sunt selectați din $F \setminus \{0\}$, rezultă că numărul de cazuri posibile (de alegere a lui v_k) este $(q-1)-(k-1)$. Rezultă că

$$Prob(det(M_V) = 0|v) \leq \frac{k-1-h}{(q-1)-(k-1)} \qquad (3.4.5)$$

pentru orice $v \in F^{k-1} \setminus \Omega$. Valoarea lui h poate fi între 0 și $k-2$. Dacă $h = 0$, înseamnă că ultima linie din M_V este cu particpant de pe nivelul 0, deci toți participanții sunt de pe nivelul 0, așadar determinantul matricei M_V este un determnant Vandermonde. Cum participanții sunt distincți, rezultă că determinantul este nenul. Dacă $h \neq 0$, atunci valoarea maximă a probabilității din relația (3.4.4) se obține când $h = 1$. Rezultă că

$$Prob(det(M_V) = 0|v) \leq \frac{k-2}{q-k} \forall v \in F^{k-1} \setminus \Omega \qquad (3.4.6)$$

Dacă $v \in \Omega$, atunci gradul polinomului corespunzător lui $det(M_V)$ este de grad cel mult $k-2-h$. Dar, din ipoteza de inducție avem că

$$Prob(v \in \Omega) \leq \frac{(k-3)(k-2)}{2(q-k+1)}$$

Utilizând relațiile de mai sus în (3.4.4), obținem că

$$Prob(det(M_V) = 0) \leq \frac{(k-3)(k-2)}{2(q-k+1)} \leq \frac{(k-2)(k-1)}{2(q-k)}$$

Acum inducția este completă, deci și demonstrația teoremei.

Exemple.

1.

Fie structura ierarhică cu $K = (k_0 = 3, k_1 = 4, k_2 = 6)$. Fie V o mulțime autorizată cu $l_0 = 3$ participanți de pe U_0, cu $l_1 = 5$ participanți de pe $U_0 \cap U_1$ și cu $l_2 = 6$ participanți de pe $U_0 \cap U_1 \cap U_2$. Fie $\{v_i\}_{i=1}^{6}$ participanții la reconstructia secretului. Astfel, pentru aflarea vectorului de coeficienți ai polinomului de interpolare, $a = (a_0, a_1, ..., a_5)$, participanții trebuie să rezolve sistemul cu matricea

$$M_V \begin{pmatrix} 1 & v_1 & v_1^2 & v_1^3 & v_1^4 & v_1^5 \\ 1 & v_2 & v_2^2 & v_2^3 & v_2^4 & v_2^5 \\ 1 & v_3 & v_3^2 & v_3^3 & v_3^4 & v_3^5 \\ 0 & 0 & 0 & 6 & 24v_4 & 60v_4^2 \\ 0 & 0 & 0 & 6 & 24v_5 & 60v_5^2 \\ 0 & 0 & 0 & 0 & 24 & 120v_6 \end{pmatrix}$$

Dezvoltând acum după ultima linie, obținem că $det(M_V) = 120\mu_5 v_6 + c_0$, unde c_0 este o constantă ce depinde de valorile $v_i, i \in \{1, 2, ..., 5\}$, iar

$$\mu_5 = det \begin{pmatrix} 1 & \mathrm{v}_1 & \mathrm{v}_1^2 & \mathrm{v}_1^3 & \mathrm{v}_1^4 \\ 1 & \mathrm{v}_2 & \mathrm{v}_2^2 & \mathrm{v}_2^3 & \mathrm{v}_2^4 \\ 1 & \mathrm{v}_3 & \mathrm{v}_3^2 & \mathrm{v}_3^3 & \mathrm{v}_3^4 \\ 0 & 0 & 0 & 6 & 24\mathrm{v}_4 \\ 0 & 0 & 0 & 6 & 24\mathrm{v}_5 \end{pmatrix}.$$

Dacă $\mu_5 \neq 0$, atunci $det(M_V)$ se va anula în exact o valoare a lui v_6. Dacă $\mu_5 = 0$ atunci există două situații:

(i) Dacă $c_0 \neq 0$, atunci $det(M_V) \neq 0$, indiferent de valoarea lui v_6

(ii) dacă $c_0 = 0$, atunci $det(M_V) = 0$ pentru orice valoare a lui v_6

Dar conform teoremei 2, M_V este singulară cu o probabilitate de cel mult $\frac{(6-2)(6-1)}{2(q-6)} = \frac{10}{q-6}$.

2.

Presupunem acum că $K = (k_0 = 3, k_1 = 5, k_2 = 6)$, iar V este de aceeași structura că mai sus. Atunci

$$M_V \begin{pmatrix} 1 & \mathrm{v}_1 & \mathrm{v}_1^2 & \mathrm{v}_1^3 & \mathrm{v}_1^4 & \mathrm{v}_1^5 \\ 1 & \mathrm{v}_2 & \mathrm{v}_2^2 & \mathrm{v}_2^3 & \mathrm{v}_2^4 & \mathrm{v}_2^5 \\ 1 & \mathrm{v}_3 & \mathrm{v}_3^2 & \mathrm{v}_3^3 & \mathrm{v}_3^4 & \mathrm{v}_3^5 \\ 0 & 0 & 0 & 6 & 24\mathrm{v}_4 & 60\mathrm{v}_4^2 \\ 0 & 0 & 0 & 6 & 24\mathrm{v}_5 & 60\mathrm{v}_5^2 \\ 0 & 0 & 0 & 0 & 0 & 120 \end{pmatrix}$$

În acest caz, a_5 va fi găsit și ne rămân 5 ecuații cu neconscutele $(a_0, a_1, ..., a_4)$. Aplicând din nou teorema 2 obținem M_V este nesingulara cu o probabilitate de cel mult $\frac{(5-2)(5-1)}{2(q-5)} = \frac{6}{q-5}$.

Teorema 2 implică faptul că dacă la reconstrucție, valoarea lui k este relativ mică, atunci probabilitatea ca M_V să fie nul este de ordinul $\Phi(\frac{1}{q})$. Cum q trebuie ales în așa fel încât $|F|$ să fie cel puțin de aceeași mărime ca și spațiul de secrete, rezultă că probabilitatea ca schemă să fie eronată este aproximativ egală cu probabilitatea de a ghici secretul (cel mult egală cu $1/q$).
Presupunem că dorim să realizăm o schemă ierarhică de partajare a secretelor folosind o alocare aleatorie a participanților. Atunci, probabilitatea că schemă să întrunească atât accesibilitate și securitate perfectă este de cel puțin $1 - C_{n+1}^k \epsilon$, unde ϵ este de forma celui dedus în Teormea 2.
Astfel, alocarea random devine sigură în cazul în care corpul F este de lungime

$$q = |F| > C_{n+1}^k \frac{(k-2)(k-1)}{2} + k$$

Alocarea monotonă a participanţilor.
Pentru fiecare $0 \leq i \leq m$ fie $n_i = |\cup_{j=0}^{i} U_i|$ și $n_{-1} = 0$. Vom asocia participanților nivelului U_i (în număr de $n_i - n_{i-1}$) doar identități din intervalul $[n_{i-1} + 1, n_i] \subset F_q$. Astfel, participanții sunt distribuiți monoton pe nivele :
$a \in U_i, b \in U_j, i \leq j => id_a \leq id_b$
unde inegalitățile sunt în sensul inegalității uzuale între întregi din inetrvalul $[0, q-1]$.

Lemma 1. Fie (K, n) o schemă de partajare ierarhică. Presupunem că participanții din U au primit identități folosind o alocare monotonă. Fie $N = maxU$. Mai presupunem că

$$2^{-k}(k+1)^{(k+2)/2} N^{k(k-1)/2} \leq q = |F_q| \qquad (***).$$

Atunci schemă de partajare a secretelor ierarhică prezentată anterior satisface și corectitudinea și securitatea perfectă.

Demonstraţie.
Vom demonstra că dacă avem o mulțime V minimală, autorizată, ce conține participantul u_0, atunci matricea M_V este regulară. Presupunem că identitățile participanților din V sunt în ordine, în sesnul de ordonare pe mulțimea numerelor reale, $v_1 \leq v_2 \leq .... \leq v_k$. Mai întâi arătăm că $det(M_V) \neq 0$ pe R, apoi vom demonstra că tot pe R avem relația $|det(M_V)| \leq q$, dacă sunt respectate condițiile din (***).
Din cele două relații de mai sus va rezultă că $det(M_V) \neq 0$ în F_q.
Observăm că valorile de 1 din matricea E de interpolare sunt poziționate în ordine crescătoare din perspectiva liniilor lui E. În primele l_0 întâlnit 1 în coloana $j = 0$, în următoarele $l_1 - l_0$ linii întâlnim valorile de 1 în coloana $j = l_0$ și așa mai departe. Astfel, matricea nu are secvențe suport de lungime impară. Astfel, pe mulțimea numerelor reale, matricea M_V este regulară.
Folosim acum teorema lui Hadamard. Dacă o matrice A cu elemente reale de dimensiuni $k \times k$ cu proprietatea că

$$|A_{i,j}| \leq 1, 0 \leq i, j \leq k \qquad (3.6)$$

atunci $|det(A)| \leq 2^{-k}(k+1)^{(k+1)/2}$.
Fie A matricea obținută din M_V prin împărțirea coloanei j la N^j, $0 \leq j \leq k-1$. Astfel, matricea A satisface condiția (3.6), deci putem aplică teorema lui Hadamard.
Rezultă concluzia anunțată de lema.

5.0.4 Operații pe scheme de partajare Ierarhice

Reamintim notațiile folosite în capitolul 2 al lucrării, și fie

$$A(E,X,G) = \begin{pmatrix} g_0^{(o_1)(x_1)} & g_1^{(o_1)(x_1)} & \cdots & g_{t-1}^{(o_1)(x_1)} \\ g_0^{(o_2)(x_2)} & g_1^{(o_2)(x_2)} & \cdots & g_{t-1}^{(o_2)(x_2)} \\ . & . & ... & . \\ . & . & ... & . \\ g_0^{(o_r)(x_r)} & g_1^{(o_r)(x_r)} & \cdots & g_{t-1}^{(o_r)(x_r)} \end{pmatrix}$$

unde matricea $A(E,X,G)$ a fost completată cu derivatele de ordin o_i ale punctelor x_i, corespunzător cu datele din matricea E.
Am văzut în capitolul 2 că polinomul de interpolare este

$$P(t) = \sum_{j=0}^{N} \frac{D(E, X, G_j)}{D(E, X)} g_j(t) \qquad (2.14)$$

unde G_j este mulțimea funcțiilor $\{g_0, g_1, ..., g_N\}$ în care g_j a fost incolcuit cu valorile lui f.
Dar, utilizatorul j din mulțimea autorizată "deține" doar linia j din matricea de interpolare, acolo fiind share-ul lui. Așadar, în cazul reconstrucției secretului, vom modifică formulă de calcul al polinomului, dezvolatand după fiecare linie determinantii corespunzători.

$$P(x) = \sum_{k=0}^{t-1} a_k x^k = \sum_{k=0}^{t-1} \sum_{l=1}^{r} a_{l,k} x^k$$

unde $a_{l,k} = \sigma_{i_l,j_l}(-1)^{l-1+k} \frac{det(A_{l-1,k}(E,X,G))}{det(A(E,X,G))}$ este calculat de participantul corespunzător liniei perechii i_l, j_l din E, cu $l = 1, ..., r$, iar $A_{l-1,k}(E, X, G)$ reprezintă matricea $A(E, X, G)$ din care am eliminat linia l și coloana $k + 1$.

Fie mesaje $m_1, m_2 \in F_q$ și o mulțime S de participanți ce se supun următoarelor presupuneri:

(i) Structura de acces Γ rămâne aceeași pentru transmiterea ambelor mesaje: m_1, m_2. Aceasta presupune ca polinoamele f, h să aibă același grad. Participantul corespunzător perechii (i, j), $s_{i,j}$ primește share-ul $\sigma_{i,j}(m_1) = f^{(j)}(i)$ pentru mesajul m_1 și $\sigma_{i,j}(m_2) = h^{(j)}(i)$ pentru mesajul m_2.
(ii) Gradul polinoamelor f, h, $t = deg(f) = deg(h)$ este ales în așa fel încât $2t \leq n$, unde n este numărul total de participanți.
(iii) Id-ul participantului $s_{i,j}$ este ales astfel încât acesta să fie unic printre Id-urile participanților și în așa fel încât problema de interpolare atașată mulțimii care încearcă să recupereze secretul să admită soluție unică.
(iv) Participanții comunica cu dealer-ul și între ei folosind canale de transmitere a datelor private.

Schema lui Tassa bazată pe interpolare Birkhoff are proprietatea de liniaritate. Astfel, la finalul pasului de reconstrucție se va extrage mesajul $m = \lambda_1 m_1 + \lambda_2 m_2$, unde λ_1, λ_2 sunt două constante din F_q.

Algoritmul Liniar.

Input: Share-urile $\sigma_{i,j}(m_1), \sigma_{i,j}(m_2) \in F_q$ și $\lambda_1, \lambda_2 \in F_q$
Output: Share-ul $\sigma_{i,j}(m) = \lambda_1\sigma_{i,j}(m_1) + \lambda_2\sigma_{i,j}(m_2) \in F_q$ pentru participantul $s_{i,j}$

Teorema 3.
Algoritmul Liniar de mai sus calculeazza corect share-urile pentru mesajul $m = \lambda_1 m_1 + \lambda_2 m_2$. Mai mult, securitatea este menținută în timpul execuției algoritmului Liniar.

Demonstrație.
Fie $\sigma_{i,j}(m)$ share-ul calculat de algoritmul Liniar pentru participantul $s_{i,j} \in R$, unde $r \in \Gamma$ este o mulțime autorizată. Pentru a arată corectitudinea, trebuie să demonstrăm că mesajul care se reconstruiește după punerea în comun a share-urilor $\sigma_{i,j}(m)$ este chiar mesajul $m =_1 m_1 + \lambda_2 m_2$. Vom arata că share-urile se vor interpolă folosind un polinom $p(x) = c_0 + c_1 x + c_2 x^2 + ... + c_{t-1}x^{t-1}$ pentru care $c_0 = \lambda_1 m_1 + \lambda_2 m_2$. Pentru a demonstra securitatea perfectă trebuie demonstrat că algoritmul liniar calculează share-urile $\sigma_{i,j}(m)$ fără a scurge informații cu privire la m. Mai mult, vom mai arată că orice mulțime neautorizată $U \notin \Gamma$ nu obține informații cu privire la m.
Polinomul de interpolare se calculează astfel:

$$p(x) = \sum_{k=0}^{t-1} c_k x^k = \sum_{k=0}^{t-1} \sum_{s_{i,j} \in R} p_{(i,j),k} x^k$$

unde $c_0 = \lambda_1 m_1 + \lambda_2 m_2$.
Mesajul m_1 a fost împărțit între particpanti folosind polinomul $f = a_0 + a_1 x + a_2 x^2 + ... + a_{t-1}x^{t-1}$. Coeficienții lui f sunt:

$$a_k = \sum_{l=1}^{r} a_{l,r} = \sum_{l=1}^{r} \sigma_l(m_1)(-1)^{l-1+k} \frac{det(A_{l-1,k}(E, X, G))}{det(A(E, X, G))}$$

pentru $k = 0, ..., t-1$, unde $\sigma_l(m_1)$, pentru $l = 1, ..., r$, sunt share-urile $\sigma_{i,j}(m_1)$ cu indicele luat în ordinea lexicografică a perechilor (i, j).
Similar, mesajul m_2 a fost share-uit cu polinomul $h(x) = b_0 + b_1 x + ... + b_{t-1}x^{t-1}$, unde

$$b_k = \sum_{l=1}^{r} a_{l,r} = \sum_{l=1}^{r} \sigma_l(m_2)(-1)^{l-1+k} \frac{det(A_{l-1,k}(E, X, G))}{det(A(E, X, G))}$$

pentru $k = 0, 1, ..., t-1$, unde $\sigma_l(m_2)$ pentru $l = 1, ..., r$, sunt share-urile $\sigma_{i,j}(m_1)$ cu indicele luat în ordinea lexicografică a perechilor (i, j).
Din cauza proprietăților homomorfice a polinoamelor, polinomum de interpolare p poate fi calculat că fiind o combinație liniară dintre f și g cu scalarii λ_1, λ_2, $p(x) = \lambda_1 f(x) +$

$\lambda_2 g(x)$. Astfel,

$$p(x) = \sum_{k=0}^{t-1} \lambda_1 a_k + \lambda_2 b_k = \sum_{k=0}^{t-1} \sum_{l=1}^{r} \lambda_1 a_{l,k} + \lambda_2 b_{l,k}$$

.

Rezultă că termenii $p_{l,k} = p_{(i,j),k} := \lambda_1 a_{l,k} + \lambda_2 b_{l,k}$ sunt calculați corect pentru polinomul de interolare p. Deoarece calculul share-ului $\sigma_{i,j}(m)$ este calculat doar de participantul corespunzător perechii (i, j), acest calcul nu poate duce la scurgeri de informații cu privire la secretul S.
Mai mult, deoarece structura de acces Γ se păstrează, rezultă că mulțimile neautorizate $U \notin \Gamma$, nu pot recupera secretul. Demonstrația este acum completă.

Acum, că am demonstrat proprietatea de liniaritate a schemei ierarhice de partajare a secretelor bazată de interpolare Birkhoff, vom încerca să arătăm că și această schemă se bucură de proprietățile enunțate în primul capitol al lucrării.

5.0.5 Schemă Dealer-Free

Pentru a elimina posibilitatea de fraudă după ce a avut loc interpolarea celor t secrete a participanților din mulțimea autorizată, participanții pot "reîmprospăta" secretul. Într-adevăr, după o interpolare, toți partipantii care au reconstruit secretul, știu share-urile celorlalți $t-1$ particpanti. Una dintre soluții este cea în care dealer-ul împarte un nou secret printre particpanti, sau cea în care participanții generează noi secrete.
În cazul unei astfel de scheme secretul va fi implicit.

Schema propusă.
Fie $P_1, P_2, ..., P_n$ cei n participanți ai unei scheme de partajare ierarhice împărțită pe m nivele $U_1, U_2, ..., U_m$. Presupunem că fiecare participant generează random un număr x_i, cu $x_i \in F_q$. Acum, fiecare particpant va distribui secretul sau tuturor celorlalți participanți, dar de dată această folosind schemă lui Tassa.
Așadar, participantul P_i transmite participanților de pe nivelul U_k share-ul $s_{i,j,k} = p_i^{(k-1)}(u_{k,j})$, adică derivată de ordin $i-1$ (nivelul inferior) a polinomului p_i, de grad $t-1$ generat de utilizatorul P_i, calculată în identitatea utilizatorului , $u_{k,j}$.
Astfel, la final, utilizatorul j de pe nivelul k va avea share-ul: $S_{j,k} = s_{1,j,k} + s_{2,j,k} + ... + s_{n,j,k}$.
Noul secret va fi $S = x_1 + x_2 + ... + x_n$.
Folosind acum proprietatea de liniaritate a scehemei lui Tassa, și presupunând că schemă respectă cele 4 proprietăți menționate în subsecțiunea anterioară, cei n participanți vor

putea reconstrui noul secret S, ce este o combinație liniară a secretelor generate de fiecare ultilizator în parte.

5.0.6 Schimbarea pragului

Dacă se cunoaște din avans vreo posibilă schimbare asupra structurii schemei de partajare, dealer-ul poate acționa de cuviință. O posibilă situație practică pentru utilizarea unei astfel de necesități, o putem imagina în cazul în care unul dintre participanți părăsește vreun nivel. Vom propune în continuare o schemă dealer-free de schimabre a pragului în cazul schemei lui Tassa.

Schemă de descreștere a pragului.

1. Jucătorii selectează un id j, astfel încât j să nu se afle în mulțimea identităților jucătorilor implicați în schemă. Fie $P_1, P_2, ..., P_t$ cei t jucători care doresc să refacă un secret. Apoi fiecare calculează constanța folosită pentru polinomul de interpolare Birkhoff:

$$\gamma_i = \sum_{k=0}^{t-1} a_{i,k} j^k$$

unde $a_{l,k} = \sigma_{i_l,j_l}(-1)^{l-1+k}\frac{det(A_{l-1,k}(E,X,G))}{det(A(E,X,G))}$ este calculat de participantul corespunzător liniei perechii i_l, j_l din E, cu $l = 1, ..., r$, iar $A_{l-1,k}(E, X, G)$ reprezintă matricea $A(E, X, G)$ din care am eliminat linie l și coloana $k + 1$.

2. Fiecare jucător P_i își va înmulți share-ul său $f(id_i)$ cu γ_i. Mai apoi, va "splita" secretul sau în t porțiuni:
$\gamma_i f(id_i) = \phi_{1i} + \phi_{2i} + ... + \phi ti, 1 \leq i \leq t$

3. Jucătorii schimbă între ei valorile ϕ_{ij}. Valoarea ϕ_{ij} reprezintă valoarea trimisă de jucătorul j către jucătorul i astfel,
$\sigma_i = \phi_{i1} + \phi_{i2} + ... + \phi_{it}$
va fi ceea ce va deține jucătorul P_i și va pune la comun cu restul jucătorilor care reconstruiesc secretul.

4. Jucătorii adună valorile γ_k, $1 \leq k \leq t$ și caluleaza
$f(j) = \sum_{k=1}^{t} \sigma_k$

5. Fiecare P_i combină share-ul sau privat $f(i)$ cu $f(j)$ după următoarea formulă: $f_0(i) = f(j) - j(\frac{f(i)-f(j)}{i-j})$ (**) .
Cum id-ul j nu se află printre mulțimea id-urilor participanților, expresia f_0 este bine definită (fractia $\frac{f(i)-f(j)}{i-j}$ nu are numitorul egal cu 0).

6. Polinomul f_0 este un polinom de gradul $t-1$, cu $f_0(0) = f(0)$. a rezultă că pragul $t-1$ este noul prag al schemei.

În cele ce urmează vom demonstra că $f_0(0) = f(0)$, iar gradul lui f_0 este $t-2$.
Presupunem că s-a făcut publică perechea $(j, f(j))$. Știm că pentru orice polinom cu coeficienți întregi, are loc:

$$(x-y)|f(x) - f(y)$$

unde "|" semnifică divizibilitatea de polinoame. Fie f_1 un polinom de gradul $t-1$ definit astfel:

$$f_1(x) = \frac{f(x) - f(j)}{x - j} \qquad (i)$$

Fiecare participant P_i trebuie să calculeze

$$f_1(id_i) = \frac{f(id_i) - f(j)}{id_i - j} \qquad (ii)$$

Folosind (i), secretul asociat cu f_1 este : $f_1(0) = \frac{f(0)-f(j)}{-j}$. (iii)
Folosind relația (iii), obținem $f(0) = f(j) - jf_1(0)$.
Noul polinom este definit astfel:

$$f_0(x) = f(j) - jf_1(x) = f(j) - j\frac{f(x) - f(j)}{x - j}$$

.
Rezultă că $f_0(i) = f(j) - j\frac{f(i)-f(j)}{i-j}$. Rezultă că

$$f_0(0) = f(j) - jf_1(0) = f(0)$$

.
Evident polinomul f_0 are gradul cel mult $t-2$, iar mai sus am arătat că $f(0) = f_0(0)$, de unde rezultă tocmai concluzia schemei propuse. Din nou, am folosit proprietatea de liniaritate a schemei lui Birkhoff (de dată această) atunci când s-au distribuit cantitățile ϕ_{ij}.
Securitatea schemei de reducere se bazează pe securitatea schemei lui Birkhoff.

Exemple:
Fie $G = \{1, x, x^2\}$, deci $g_0(x) = 1, g_1(x) = x, g_2(x) = x^2$. Presupunem că X și E sunt următoarele :
$X = \{1, 2, 3\}$,

$$E \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

iar datele sunt $p(1) = 15, p(2) = 29, p'(3) = 23$. Căutăm polinomul $p(x) = a_2x^2+a_1x+a_0$ ce satisface $p(1) = 15, p(2) = 29, p'(3) = 23$. Structura autorizată trebuie să admită 2 utilizatori de pe nivelul 0, U_0 și 3 utilizatori de nivelurile $U_0 \cup U_1$.

$$A(E, X, G) = \begin{pmatrix} g_0(x_1) & g_1(x_1) & g_2(x_1) \\ g_0(x_2) & g_1(x_2) & g_2(x_2) \\ g_0'(x_3) & g_1'(x_3) & g_2'(x_3) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 0 & 1 & 6 \end{pmatrix}$$

$$A(E, X, G_0) = \begin{pmatrix} p(x_1) & g_1(x_1) & g_2(x_1) \\ p(x_2) & g_1(x_2) & g_2(x_2) \\ p'(x_3) & g_1'(x_3) & g_2'(x_3) \end{pmatrix} = \begin{pmatrix} 15 & 1 & 1 \\ 29 & 2 & 4 \\ 23 & 1 & 6 \end{pmatrix}$$

$$A(E, X, G_1) = \begin{pmatrix} g_0(x_1) & p(x_1) & g_2(x_1) \\ g_0(x_2) & p(x_2) & g_2(x_2) \\ g_0'(x_3) & p'(x_3) & g_2'(x_3) \end{pmatrix} = \begin{pmatrix} 1 & 15 & 1 \\ 1 & 29 & 4 \\ 0 & 23 & 6 \end{pmatrix}$$

$$A(E, X, G_2) = \begin{pmatrix} g_0(x_1) & g_1(x_1) & p(x_1) \\ g_0(x_2) & g_1(x_2) & p(x_2) \\ g_0'(x_3) & g_1'(x_3) & p'(x_3) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 15 \\ 1 & 2 & 29 \\ 0 & 1 & 23 \end{pmatrix}$$

Observăm că $det(A(E, X, G)) = 3, det(A(E, X, G_0)) = 21, det(A(E, X, G_1)) = 15, det(A(E, X, G_2)) = 9$. Conform formulei de interpolare Birkhoff, polinomul căutat va fi

$$p(x) = \sum_{j=0}^{2} \frac{D(E, X, G_j)}{D(E, X, G)} g_j(x) = 7 + 5x + 3x^2.$$

Dar într-o schemă ierarhică, un utilizator nu poate calcula $A(E, X, G_i)$ deoarece el posedă un singur share dintre $p(1), p(2), p'(3)$.
Astfel, fiecare $A(E, X, G_i)$ va fi dezvoltat după coloana i.
Astfel, coeficientul pentru $x^0, (g_0(x))$ calculat de primul participant va fi,

$$c_0 = 15(-1)^{1+1} \begin{pmatrix} 2 & 4 \\ 1 & 6 \end{pmatrix}$$

coeficientul calculat tot de primul participant pentru $x^1, (g_1(x))$ va fi

$$c_1 = 15(-1)^{1+2} \begin{pmatrix} 1 & 4 \\ 0 & 6 \end{pmatrix}$$

iar coeficientul calculat pentru $x^2, (g_2(x))$ va fi

$$c_2 = 15(-1)^{1+3} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

Apoi, cei trei jucători își vor pune la comun coeficienții calculați, pe rând, pentru x^0, x^1, x^2 și vom putea aplica formulă de interpolare.
Pentru schema de micșorare a pragului, constanța calculată de primul participant, γ_1 va fi

$$\frac{c_0}{15} j^0 + \frac{c_1}{15} j^1 + \frac{c_2}{15} j^2$$

Dar, pentru a află secretul, este suficient că participanții să calculeze $p(0)$. Cum pentru $x = 0$, formulă de interes devine

$$S = \frac{det(A(E, X, G_0))}{det(A(E, X, G))}$$

deoarece secretul este chiar termenul liber al polinomului. Astfel, în schemă de schimbare de prag, fiecare γ_i va avea valoarea egală cu produsul dintre share-ul participantului și termenul corespunzător share-ului sau din dezvoltarea lui $A(E, X, G_0)$ după prima coloana.

Bibliografie

[1] G.G. Lorentz, etc. *(Section, Interpolation and approximation) - Birkhoff interpolation*. Longman Higher Education (1983)

[2] E. Ballico *Birkhoff Interpolation Over a Finite Field*. International Journal of Pure and Applied Mathematics, 2007

[3] Mehrdad Nojoumian, Douglas R. Stinson
On Dealer-free Dynamic Treshold Schemes NSERC research paper

[4] Giulia Traverso, Denise Demirel, Johannes Buchmann
Performing Computations on Hierarchically Shared Secrets

[5] Koji Shima, Hiroshima Doi
A Hierarchical Secret Sharing Scheme over Finite Fields of Characteristic 2 Journal of Information Processing, Vol 25, 875-883(Sep. 2017)

[6] K. Atkinson, S. Sharma
A partial Characterization Of Poised Hermite-Birkhoff Interpolation Problems Siam J. Numer. Anal. Vol 6, No. 2, June 1969