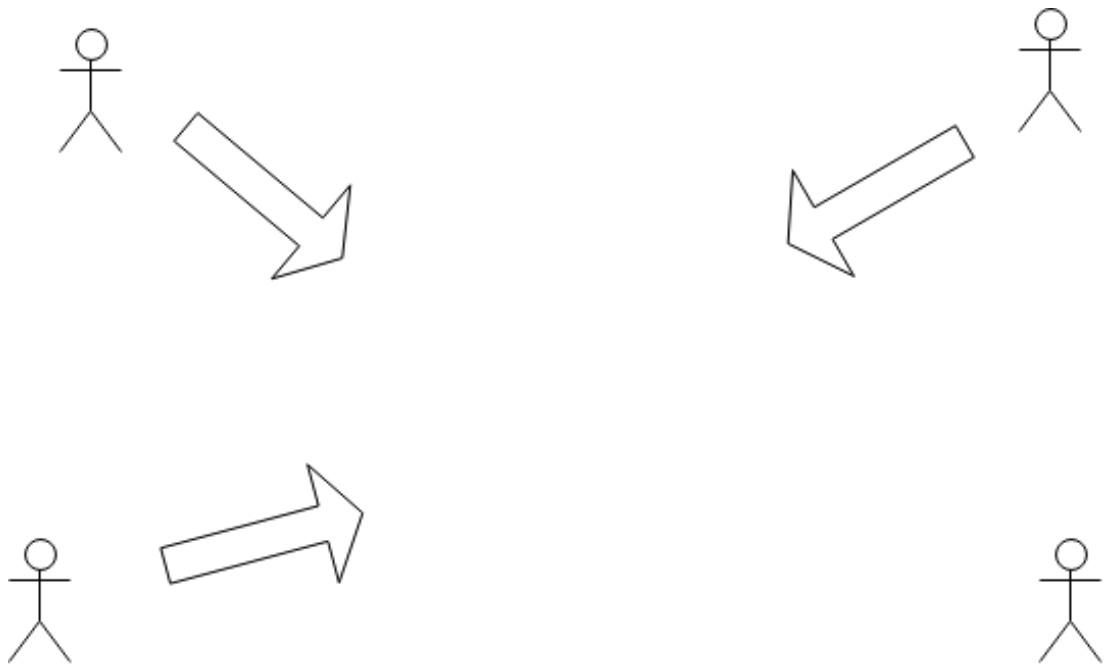
Aplicații ale Schemelor de Partajare a Secretelor

Dragoș Alin Rotaru

Universitatea din București

9 februarie, 2015

Motivație: scheme de partajare

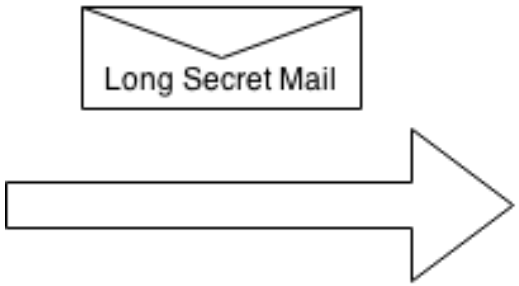


Motivație: scheme de partajare

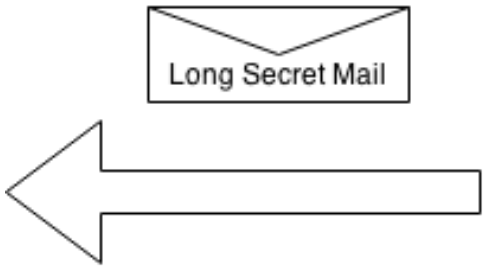
Motivație: scheme de partajare

Motivație: sisteme de stocare

Motivație: sisteme de stocare



Motivație: sisteme de stocare



Schema Shamir - intuiție

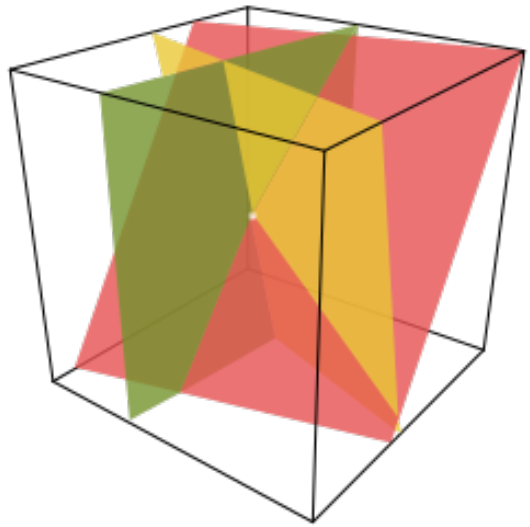
- k puncte distincte în plan definesc o curbă polinomială unică având acelasi grad

Schema Shamir - intuiție

- k puncte distincte în plan definesc o curbă polinomială unică având acelasi grad
- Mai puțin de k puncte nu pot reconstitui polinomul original

Schema Shamir - intuiție

- k puncte distincte în plan definesc o curbă polinomială unică având acelasi grad
- Mai puțin de k puncte nu pot reconstitui polinomul original



Schema Shamir

- Secret $\mathcal{S}$

Schema Shamir

- Secret $\mathcal{S}$
- Schema (k, n) majoritară

Schema Shamir

- Secret $\mathcal{S}$
- Schema (k, n) majoritară
- Oricare k participanți din cei n pot reconstitui $\mathcal{S}$

Schema Shamir

- Secret $\mathcal{S}$
- Schema (k, n) majoritară
- Oricare k participanți din cei n pot reconstitui $\mathcal{S}$
- Mai puțin de k participanți nu obțin nici o informație despre $\mathcal{S}$

Schema Shamir

- Secret $\mathcal{S}$
- Schema (k, n) majoritară
- Oricare k participanți din cei n pot reconstitui $\mathcal{S}$
- Mai puțin de k participanți nu obțin nici o informație despre $\mathcal{S}$
- Se alege un polinom f de grad k având coeficienți aleatori, termenul liber fiind $\mathcal{S}$

Schema Shamir

- Secret $\mathcal{S}$
- Schema (k, n) majoritară
- Oricare k participanți din cei n pot reconstitui $\mathcal{S}$
- Mai puțin de k participanți nu obțin nici o informație despre $\mathcal{S}$
- Se alege un polinom f de grad k având coeficienți aleatori, termenul liber fiind $\mathcal{S}$
- Participantul P_i primeste $f(i)$, $i = \{1, 2, ...n\}$

Schema Shamir

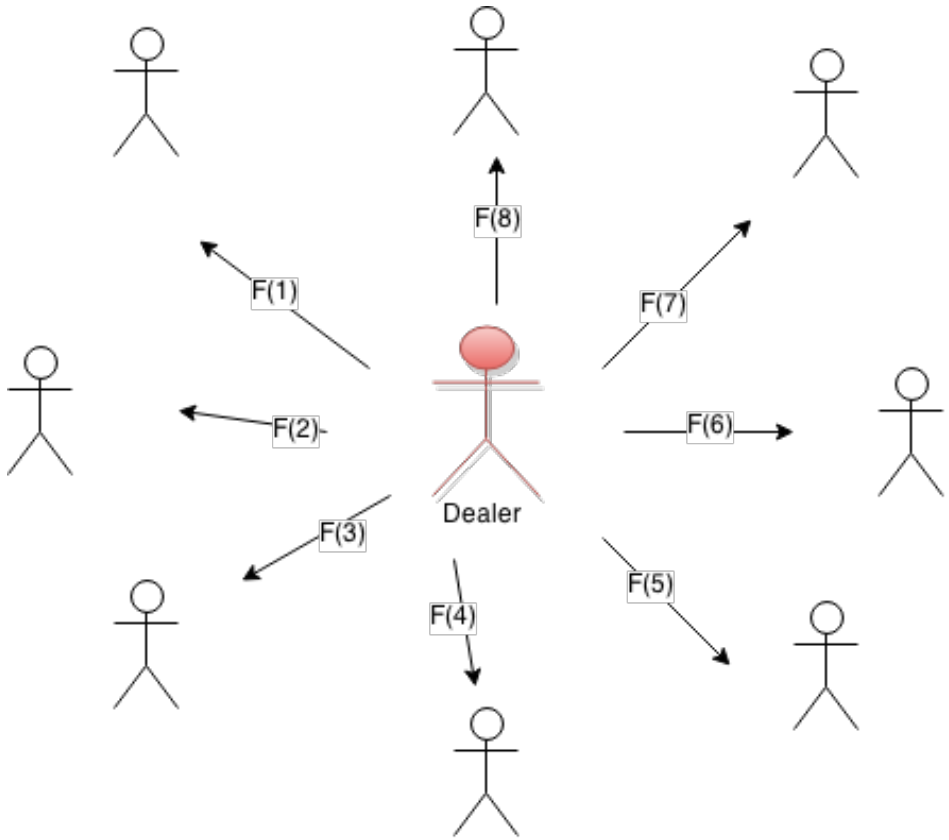
- Secret $\mathcal{S}$
- Schema (k, n) majoritară
- Oricare k participanți din cei n pot reconstitui $\mathcal{S}$
- Mai puțin de k participanți nu obțin nici o informație despre $\mathcal{S}$
- Se alege un polinom f de grad k având coeficienți aleatori, termenul liber fiind $\mathcal{S}$
- Participantul P_i primeste $f(i)$, $i = \{1, 2, ...n\}$
- Dupa reconstituire secretul $\mathcal{S}$ se afla în $f(0)$.

Schema Shamir

Exemplu

Se consideră 8 participanți, unde oricare 3 pot reconstitui secretul $\mathcal{S}$. Fie polinomul $f(x) = a_3x^3 + a_2x^2 + a_1x + S$, $a_i \leftarrow^R Z_q$, a_i aleși în mod aleator din corpul Z_q.

Schema Shamir



Schema unanimă XOR

- Schema majoritară (n, n).

Schema unanimă XOR

- Schema majoritară (n, n).
- $n - 1$ participanți primesc numere aleatoare: $s_1, s_2, \ldots s_{n-1}$.

Schema unanimă XOR

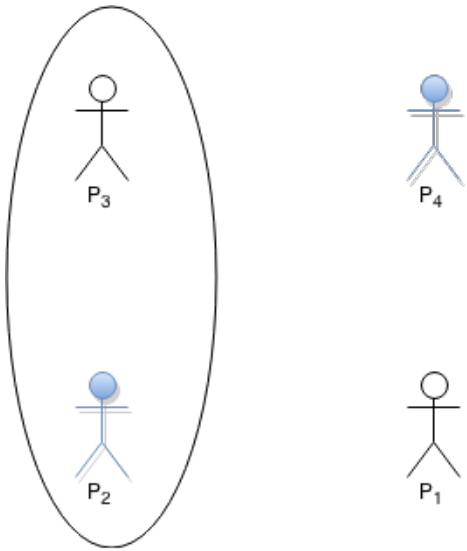
- Schema majoritară (n, n).
- $n - 1$ participanți primesc numere aleatoare: $s_1, s_2, \ldots s_{n-1}$.
- Cel de-al n-lea participant primește $S \oplus s_1 \oplus s_2 \oplus \cdots \oplus s_{n-1}$.

Schema Ito, Saito și Nishizeki

- Schema Shamir e insuficientă pentru a realiza partajarea lui $\mathcal{S}$ unui grup particular de participanți.

Schema Ito, Saito și Nishizeki

- Schema Shamir e insuficientă pentru a realiza partajarea lui $\mathcal{S}$ unui grup particular de participanți.



Asigurarea disponibilității cu ajutorul sistemelor RAID

- RAID (Redundant array of independent disks) combină 2 concepte ortgonale:

Asigurarea disponibilității cu ajutorul sistemelor RAID

- RAID (Redundant array of independent disks) combină 2 concepte ortgonale:
  - Data striping

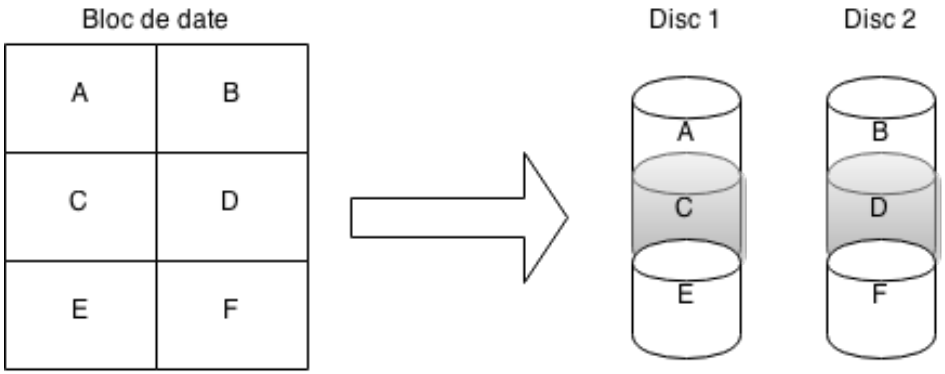
Asigurarea disponibilității cu ajutorul sistemelor RAID

- RAID (Redundant array of independent disks) combină 2 concepte ortgonale:
  - Data striping
  - Redundanța datelor

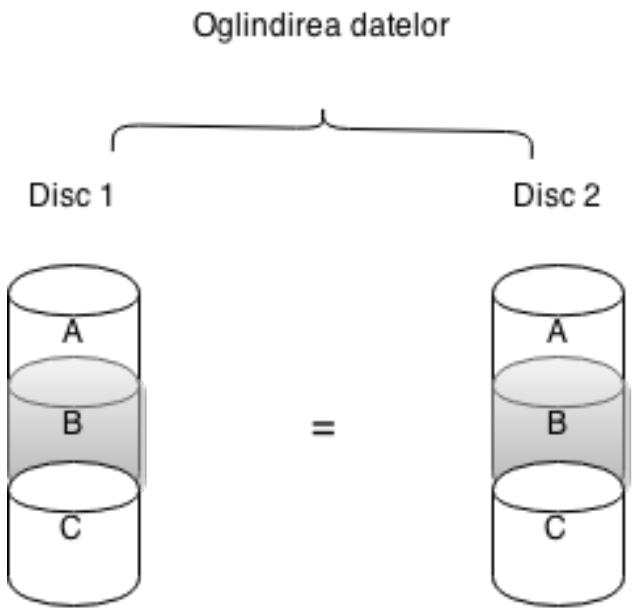
Asigurarea disponibilității cu ajutorul sistemelor RAID

- RAID (Redundant array of independent disks) combină 2 concepte ortgonale:
  - Data striping
  - Redundanța datelor
- Datele sunt distribuite în moduri diferite denumite niveluri RAID.

Nivelul 0 Raid - Data Striping



Nivelul 1 Raid - Redundanța datelor



Sisteme securizate de stocare de lunga durata

- Securitatea este asigurată cu ajutorul schemelor de partajare.

Sisteme securizate de stocare de lunga durata

- Securitatea este asigurată cu ajutorul schemelor de partajare.
- Disponibilitatea cu nivele RAID.

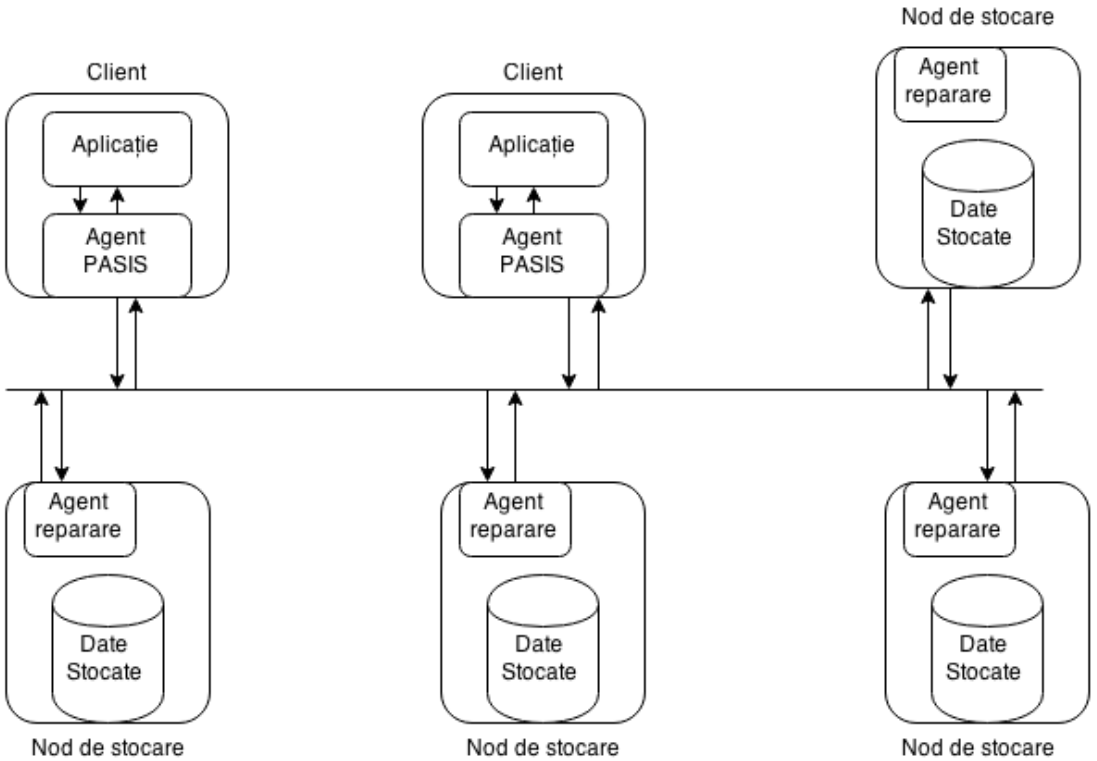
PASIS

- Informația este partajată cu ajutorul agenților PASIS folosind Schema Shamir.

PASIS

- Informația este partajată cu ajutorul agenților PASIS folosind Schema Shamir.
- Componentele (share-uri) rezultate in urma partajării sunt distribuite apoi nodurilor existente în rețea.

PASIS


Client
Aplicație
Agent PASIS
Client
Aplicație
Agent PASIS
Nod de stocare
Agent reparare
Date Stocate
Agent reparare
Date Stocate
Agent reparare
Date Stocate
Agent reparare
Date Stocate
Nod de stocare
Nod de stocare
Nod de stocare

Alouneh et al.

- Informația este partajată cu ajutorul unei aplicații la nivelul clientului folosind o versiune modificată a schemei Shamir.

Alouneh et al.

- Informația este partajată cu ajutorul unei aplicații la nivelul clientului folosind o versiune modificată a schemei Shamir.
- Coeficienții polinomului f nu mai sunt aleși aleator ci sunt luați direct din fisierul partajat in maniera secventială.

Alouneh et al.

- Informația este partajată cu ajutorul unei aplicații la nivelul clientului folosind o versiune modificată a schemei Shamir.
- Coeficienții polinomului f nu mai sunt aleși aleator ci sunt luați direct din fisierul partajat in maniera secventială.
- Nodul cu indexul i primește valoarea polinomului $f(i)$.

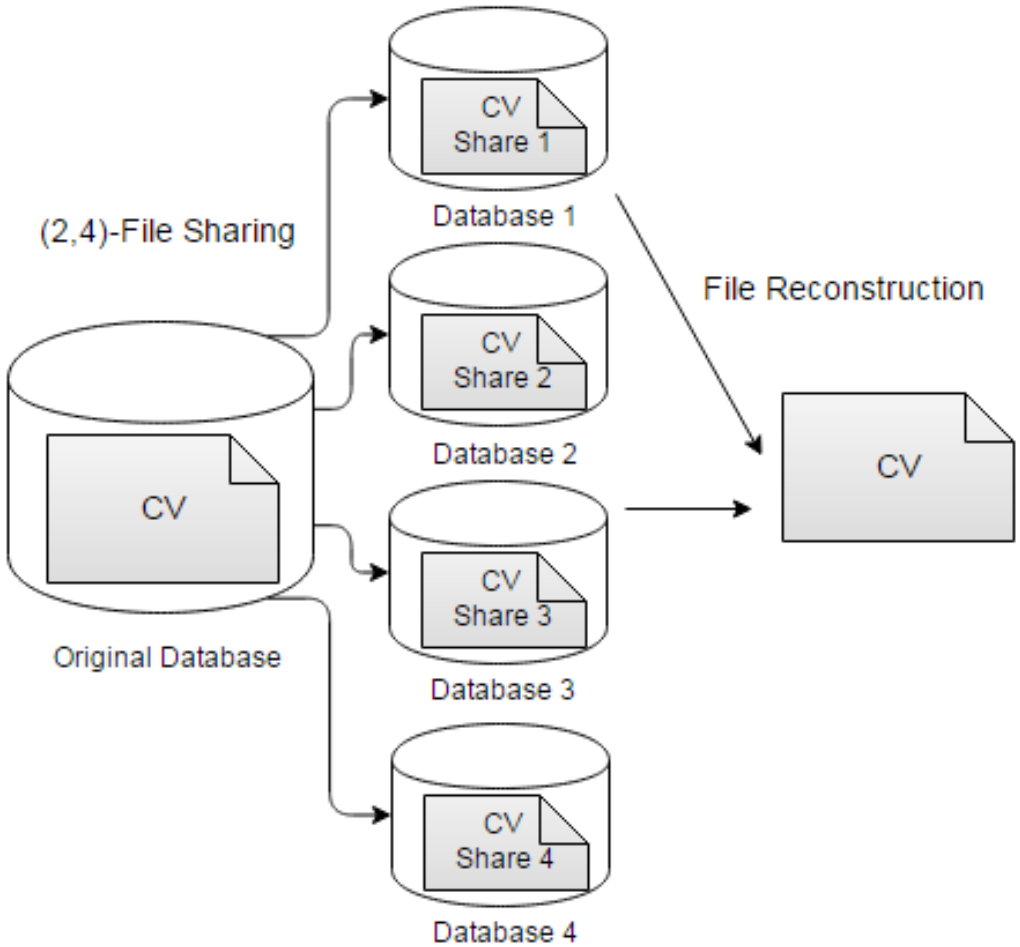
Alouneh et al.

- Informația este partajată cu ajutorul unei aplicații la nivelul clientului folosind o versiune modificată a schemei Shamir.
- Coeficienții polinomului f nu mai sunt aleși aleator ci sunt luați direct din fisierul partajat in maniera secventială.
- Nodul cu indexul i primește valoarea polinomului $f(i)$.

Exemplu

Fie un fișier *File* avand octetii: 10 15 in aceasta ordine. Polinomul după care se realizeaza partajarea este $f(x) = 10 + 15x$. Nodul i primeste valoarea $f(i)$

Alouneh et al.: partajare + reconstrucție



Alouneh et al. - atacuri

Construirea polinomului este determinista! $\rightarrow$ Componentele vor fi aceleași pentru fișiere identice partajate.

Alouneh et al. - determinarea tipului de fișier partajat

Prin obținerea informatiilor dintr-un singur nod, se poate constata tipul de fisier partajat inițial:

Semnături de fișiere

Tip fișier	Primii 4 octeți			
doc	D0	CF	11	E0
gif	47	49	46	38
pdf	25	50	44	46
png	89	50	4E	47
rar	52	61	72	21
wav	52	49	46	46
zip	50	4B	03	04

Alouneh et al. - determinarea tipului de fișier partajat

Prin obținerea informatiilor dintr-un singur nod, se poate constata tipul de fisier partajat inițial:

Indicele maxim i a.î. componentele primului bloc sa fie distincte($k = 3$)

Tip Fișier	doc	gif	pdf	png	rar	wav	zip
doc	-	63	-1	-1	-1	-1	-1
gif	63	-	-1	-1	-1	-1	-1
pdf	-1	-1	-	164	-1	119	-1
png	-1	-1	164	-	143	122	129
rar	-1	-1	-1	143	-	143	-1
wav	-1	-1	119	122	143	-	172
zip	-1	-1	-1	129	-1	172	-