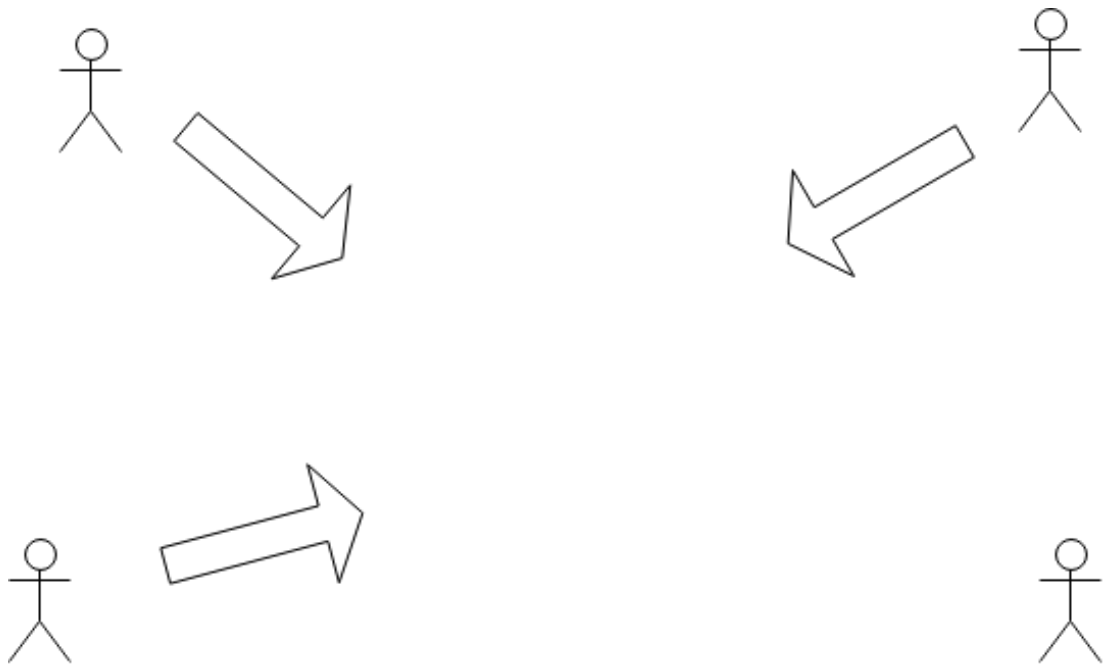
Aplicații ale Schemelor de Partajare a Secretelor

Dragoș Alin Rotaru

Universitatea din București

9 februarie, 2015

Motivație: scheme de partajare

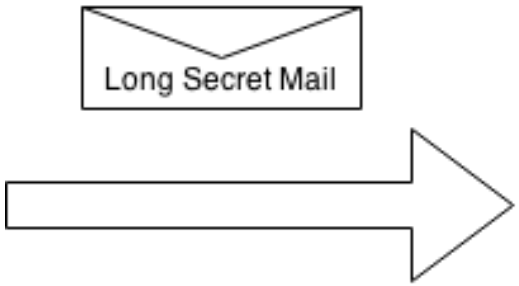


Motivație: scheme de partajare

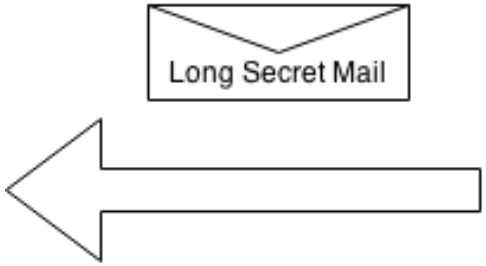
Motivație: scheme de partajare

Motivație: sisteme de stocare

Motivație: sisteme de stocare



Motivație: sisteme de stocare



Schema Shamir - intuiție

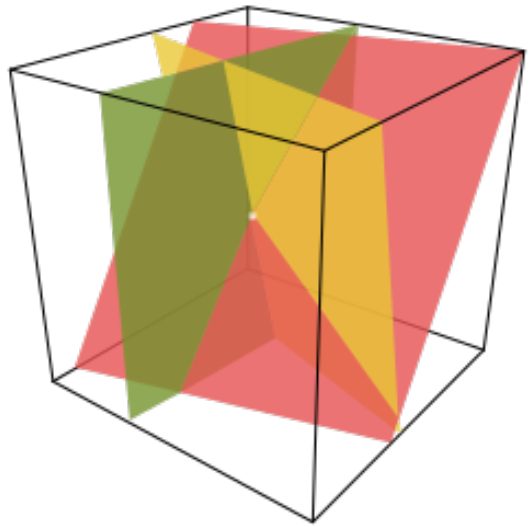
- k puncte distincte în plan definesc o curbă polinomială unică având acelasi grad

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

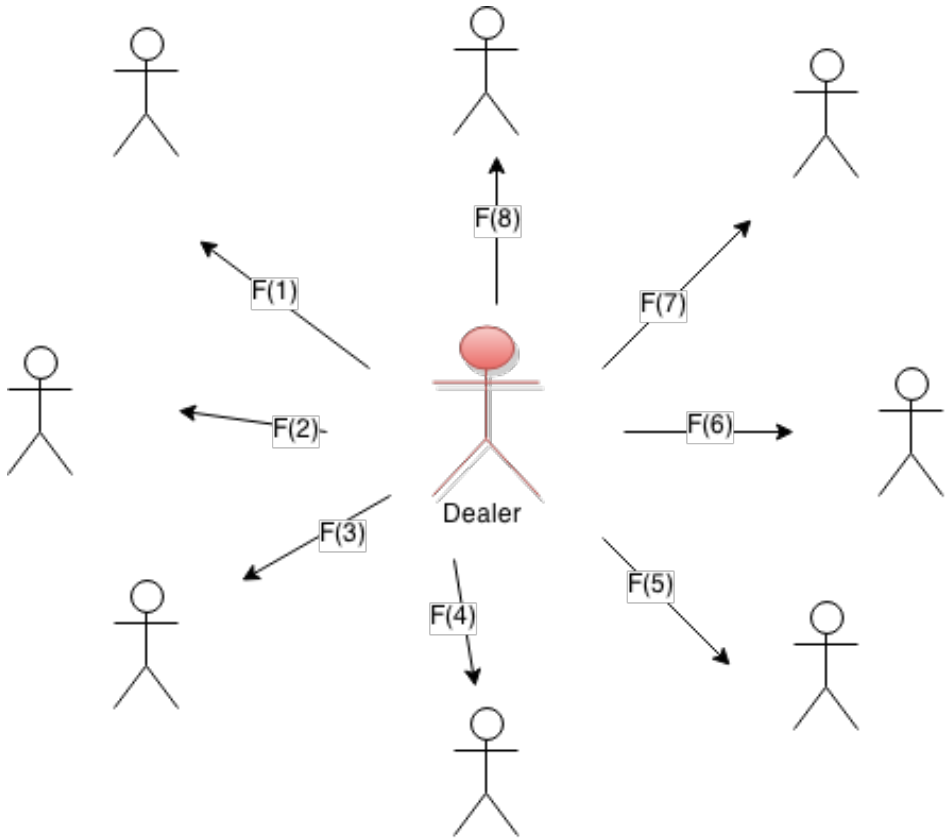
- Secret $\mathcal{S}$
- Schema (k, n) majoritară
- Oricare k participanți din cei n pot reconstitui $\mathcal{S}$
- Mai puțin de k participanți nu obțin nici o informație despre $\mathcal{S}$
- Se alege un polinom f de grad k având coeficienți aleatori, termenul liber fiind $\mathcal{S}$
- Participantul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

Schema Shamir

Example

Se consideră 8 participanți, unde oricare 3 pot reconstitui secretul $\mathcal{S}$. Fie polinomul $f(x) = 20x^3 + 14x^2 + 31x + S$

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

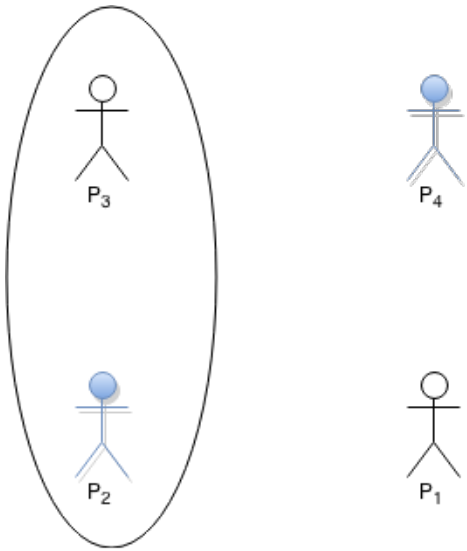
- Schema majoritară (n, n).
- $n - 1$ participanți primesc numere aleatoare: $s_1, s_2, \ldots s_{n-1}$.
- Cel de-al n-lea participant primește $S \oplus s_1 \oplus s_2 \oplus \cdots \oplus s_{n-1}$.

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 disponibiltății cu ajutorul sistemelor RAID