

# Aplicații ale Schemelor de Partajare a Secretelor

Dragoș Alin Rotaru

Universitatea din București

9 februarie, 2015

# Cuprins pentru secțiunea 1

## 1 Overview

- Motivație

## 2 Scheme de partajare

- Schema Shamir
- Schema unanimă XOR
- Schema Ito, Saito și Nishizeki

## 3 Sisteme de stocare

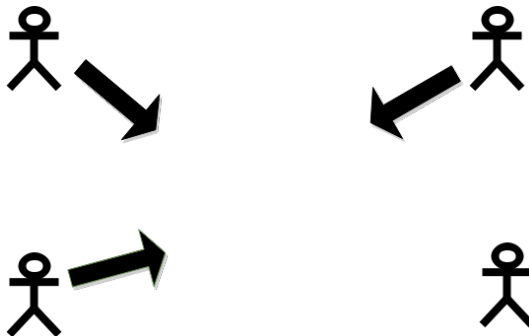
- RAID
- PASIS

## 4 Alouneh et al.

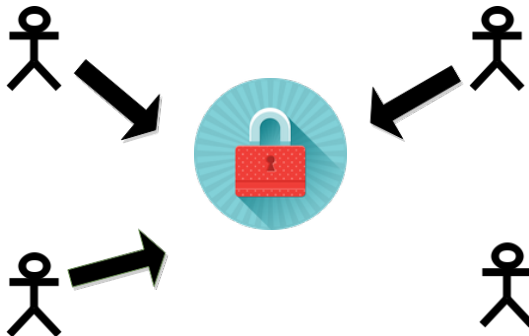
## 5 Rezultate personale

- Detectarea tipului de fișier partajat
- Determinarea conținutului de fișier
- Detectarea unui pattern repetitiv dintr-un fișier

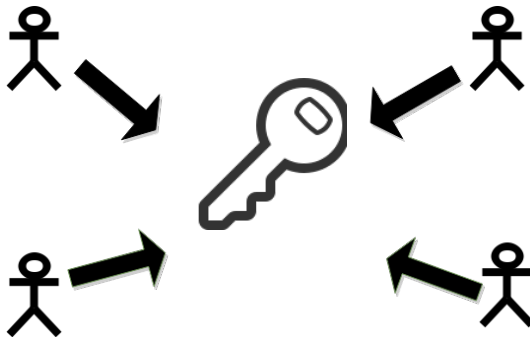
# Motivație: scheme de partajare



# Motivație: scheme de partajare



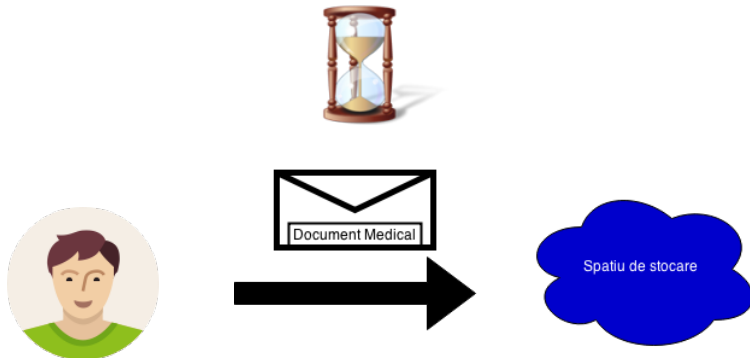
# Motivație: scheme de partajare



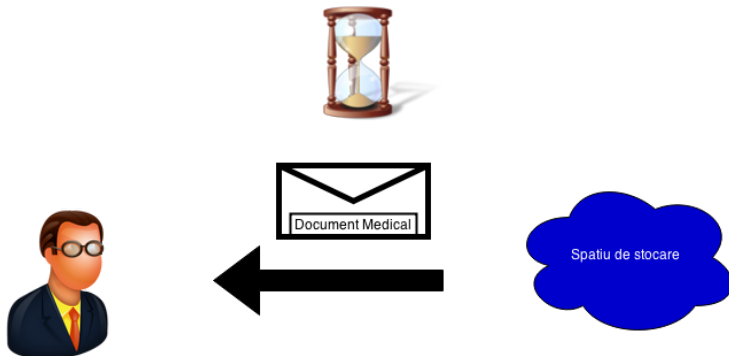
# Motivație: sisteme de stocare



# Motivație: sisteme de stocare



# Motivație: sisteme de stocare





# Cuprins pentru secțiunea 2

## 1 Overview

- Motivație

## 2 Scheme de partajare

- Schema Shamir
- Schema unanimă XOR
- Schema Ito, Saito și Nishizeki

## 3 Sisteme de stocare

- RAID
- PASIS

## 4 Alouneh et al.

## 5 Rezultate personale

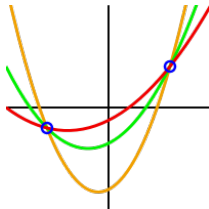
- Detectarea tipului de fișier partajat
- Determinarea conținutului de fișier
- Detectarea unui pattern repetitiv dintr-un fișier

- $k$  puncte distincte în plan definesc o curbă polinomială unică având grad  $k - 1$

- $k$  puncte distincte în plan definesc o curbă polinomială unică având grad  $k - 1$
- Mai puțin de  $k$  puncte nu pot reconstitui polinomul original

# Schema Shamir - intuiție

- $k$  puncte distincte în plan definesc o curbă polinomială unică având grad  $k - 1$
- Mai puțin de  $k$  puncte nu pot reconstitui polinomul original



"3 polynomials of degree 2  
through 2 points" by

- Secret  $\mathcal{S}$

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

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

- 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  $\mathcal{S}$



- 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  $k - 1$  având coeficienți aleatori, termenul liber fiind  $\mathcal{S}$

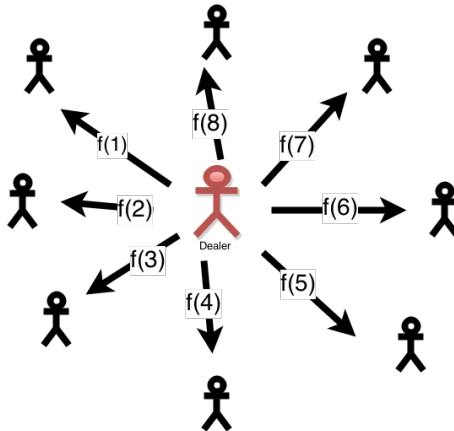
- Secret  $\mathcal{S}$
- Schema  $(k, n)$  majoritară
- Oricare  $k$  participanți din cei  $n$  pot reconstitui  $\mathcal{S}$
- Mai puțin de  $k$  participanți nu obțin nici o informație despre  $\mathcal{S}$
- Se alege un polinom  $f$  de grad  $k - 1$  având coeficienți aleatori, termenul liber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

- 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  $k - 1$  având coeficienți aleatori, termenul liber fiind  $\mathcal{S}$
- Participantul  $P_i$  primește  $f(i)$ ,  $i = \{1, 2, \dots, n\}$
- După reconstituire secretul  $\mathcal{S}$  se află în  $f(0)$ .

## 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 majoritară  $(n, n)$ .

# Schema unanimă XOR

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

# Schema unanimă XOR

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

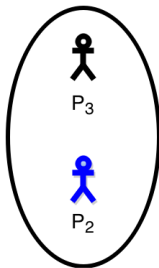


# Schema unanimă XOR

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

- Schema Shamir e insuficientă pentru a realiza partajarea lui  $S$  unui grup oarecare de participanți.

- Schema Shamir e insuficientă pentru a realiza partajarea lui  $S$  unui grup oarecare de participanți.



$S$  poate fi reconstruit  
doar din  $\{P_2, P_3\}$  sau  
 $\{P_2, P_4\}$

# Cuprins pentru secțiunea 3

- 1 Overview
  - Motivație
- 2 Scheme de partajare
  - Schema Shamir
  - Schema unanimă XOR
  - Schema Ito, Saito și Nishizeki
- 3 Sisteme de stocare
  - RAID
  - PASIS
- 4 Alouneh et al.
- 5 Rezultate personale
  - Detectarea tipului de fișier partajat
  - Determinarea conținutului de fișier
  - Detectarea unui pattern repetitiv dintr-un fișier

# 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

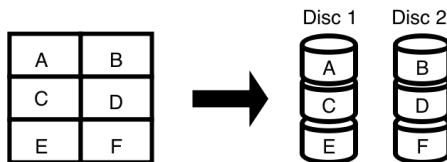
- RAID (Redundant Array of Independent Disks) combină 2 concepte ortgonale:
  - Data striping
  - Redundanța datelor

# Asigurarea disponibilității cu ajutorul sistemelor RAID

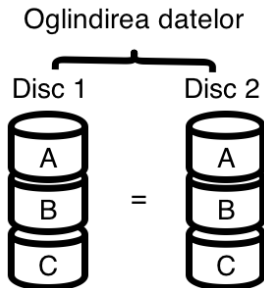
- RAID (Redundant Array of Independent Disks) combină 2 concepte ortgonale:
  - Data striping
  - Redundanța datelor
- Datele sunt distribuite în moduri diferite denumite niveluri RAID.



# Nivelul 0 Raid - Data Striping



# Nivelul 1 Raid - Redundanța datelor



- Securitatea este asigurată cu ajutorul schemelor de partajare.

# Sisteme securizate de stocare de lungă durată

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

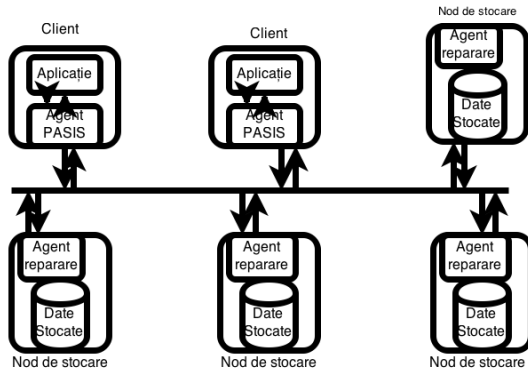
# PASIS (Perpetually Available and Secure Information Systems)

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

# PASIS (Perpetually Available and Secure Information Systems)

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

# PASIS (Perpetually Available and Secure Information Systems)



# Cuprins pentru secțiunea 4

- 1 Overview
  - Motivație
- 2 Scheme de partajare
  - Schema Shamir
  - Schema unanimă XOR
  - Schema Ito, Saito și Nishizeki
- 3 Sisteme de stocare
  - RAID
  - PASIS
- 4 Alouneh et al.
- 5 Rezultate personale
  - Detectarea tipului de fișier partajat
  - Determinarea conținutului de fișier
  - Detectarea unui pattern repetitiv dintr-un fișier



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

- 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 secvențială.

- 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 secvențială.
- Nodul cu indexul  $i$  primește valoarea polinomului  $f(i)$ .

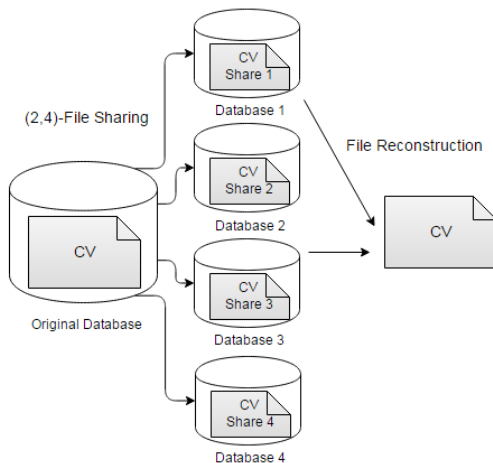
- Informația este partajată cu ajutorul unei aplicații la nivelul clientului folosind o versiune modificată a schemei Shamir.
- Coeficienții polinomului  $f$  nu mai sunt aleși aleator ci sunt luați direct din fisierul partajat în maniera secvențială.
- Nodul cu indexul  $i$  primește valoarea polinomului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

## Exemplu

Fie un fișier *File* având octeții: 10 15 în această ordine.

Polinomul după care se realizează partajarea este  $f(x) = 10 + 15x$ . Nodul  $i$  primește valoarea  $f(i)$

# Alouneh et al. (2013): partajare + reconstrucție



# Cuprins pentru secțiunea 5

- 1 Overview
  - Motivație
- 2 Scheme de partajare
  - Schema Shamir
  - Schema unanimă XOR
  - Schema Ito, Saito și Nishizeki
- 3 Sisteme de stocare
  - RAID
  - PASIS
- 4 Alouneh et al.
- 5 Rezultate personale
  - Detectarea tipului de fișier partajat
  - Determinarea conținutului de fișier
  - Detectarea unui pattern repetitiv dintr-un fișier

- Construirea polinomului este deterministă!

- Construirea polinomului este deterministă!
- Componentele rezultate vor fi aceleași pentru fișiere identice partajate.



Considerând că dealerul  $\mathcal{D}$  nu schimbă numărătoarea nodurilor la diferite distribuții:

- Compararea între 2 tipuri de fișiere partajate pe același nod este fezabilă
- Detectarea fișierelor având conținut similar sau diferit
- Detectarea unui pattern repetitiv dintr-un fișier

# Alouneh et al. (2013) - determinarea tipului de fișier partajat

Prin obținerea informațiilor dintr-un singur nod, se poate constata tipul de fișier 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. (2013) - determinarea tipului de fișier partajat

Prin obținerea informațiilor dintr-un singur nod, se poate constata tipul de fișier 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	-


# Alouneh et al. (2013) - determinarea conținutului de fișier



File Edit View Go Bookmarks Help


1 of 1 163,43%

 **europass** Автобиография

**ЛИЧНА ИНФОРМАЦИЯ** Иван Иванов Петров

 бул. Цар Освободител 23 7000 Русе

 +359 29123456  +359 812345678

 [ivan.petrov@mail.bg](mailto:ivan.petrov@mail.bg)

**Дата на раждане** 12 Април 1981 | **Националност** българин

**ПОЗИЦИЯ, ЗА КОЯТО СЕ КАНДИДАТСТВА** Счетоводител

**ТРУДОВ СТАЖ**

01 Март 2005 - 01 Май 2012 **Счетоводител**


Жити Ад - Русе

Производство на нисковъглеродни стоманени топове, гвоздеи (строителни и специални), скрепителни елементи, мрежи

CV Europass BG

# Alouneh et al. (2013) - determinarea conținutului de fișier


File Edit View Go Bookmarks Help






Curriculum vitae

PERSONLIG INFORMATION

Philippe Sønderberg

 Ramundsvej 41, 2300 København S (Danmark)

 +45 33123450  +45 41234567

 ps@usmail.dk

ANSØGTE STILLINGER

Datafagtekniker

ERHVERVSERFARING

September 2009 - Nuværende

Datafagtekniker

- vedligeholdelse af edb-anlæg
- vejledning og instruktion af kollegaer

ALMEN OG ERHVERVSRETTET UDDANNELSE

September 2005 - Juni 2009


Datafagtekniker

CV Europass DK

# Alouneh et al. (2013) - determinarea conținutului de fișier

File Edit View Go Bookmarks Help

1 of 5 157,77%

 **MOBILITATE EUROPASS**

**1. ACEST DOCUMENT DE MOBILITATE EUROPASS SE ACORDĂ**

Nume	Prenume	Fotografie
(1)(*) <input type="text" value="IONESCU"/>	(2)(*) <input type="text" value="Victor"/>	(4) <input type="text"/>
Adresa (număr, stradă, cod poștal, oraș, țară)		
(3) <input type="text" value="Aleea Florilor nr.14, bl. C23, ap.21, sector 3, CP 1024, București, România, 7000"/>		
Data nașterii	Naționalitate	Semnătura titularului
(5) <input type="text" value="03"/> <input type="text" value="04"/> <input type="text" value="1988"/> zz ll aaaa	(6) <input type="text" value="Română"/>	(7) <input type="text"/>

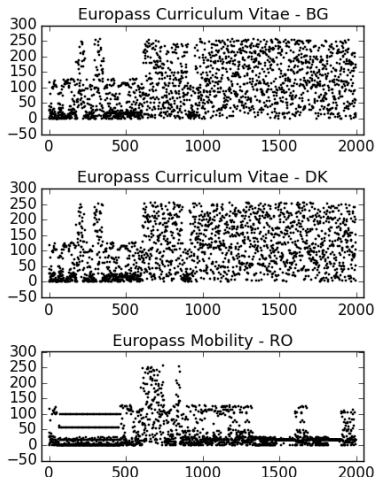
NB : Rubricile marcate cu asterisc sunt obligatorii.

**2. ACEST DOCUMENT DE MOBILITATE EUROPASS SE ELIBEREAZĂ DE CĂTRE :**

Europass Mobility RO

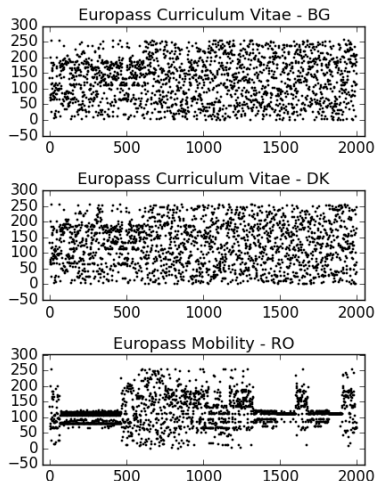
Partajarea celor 3 fișiere  
cu schema (2, 4).

Adversarul obține  
componentele aflate pe  
nodul 1:

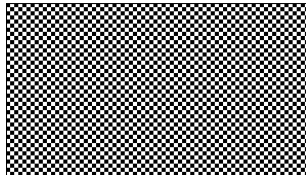


Partajarea celor 3 fișiere  
cu schema (2, 4).

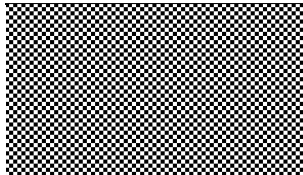
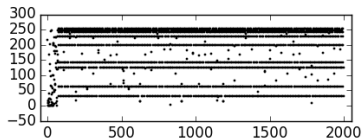
Adversarul obține  
componentele aflate pe  
nodul 2:





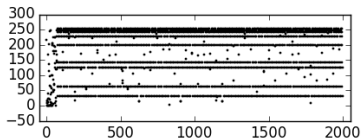


# Alouneh et al. (2013) - determinarea unui pattern în fișier

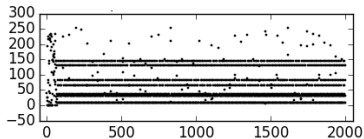
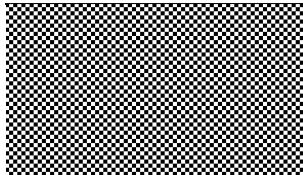


Nod 1

# Alouneh et al. (2013) - determinarea unui pattern în fișier

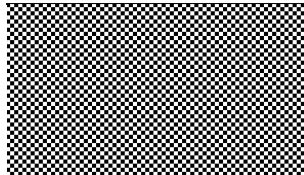
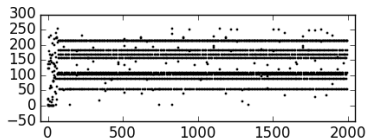


Nod 1



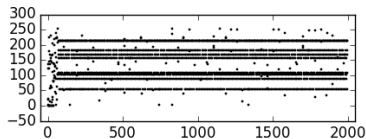
Nod 2

# Alouneh et al. (2013) - determinarea unui pattern în fișier

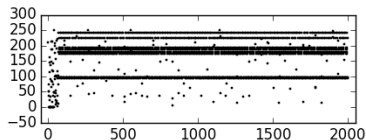
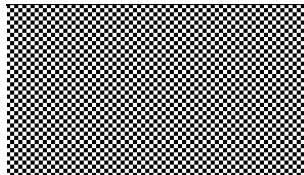


Nod 3

# Alouneh et al. (2013) - determinarea unui pattern în fișier



Nod 3



Nod 4

# Mulțumesc!