

# Aplicații ale Schemelor de Partajare a Secretelor

Dragoș Alin Rotaru

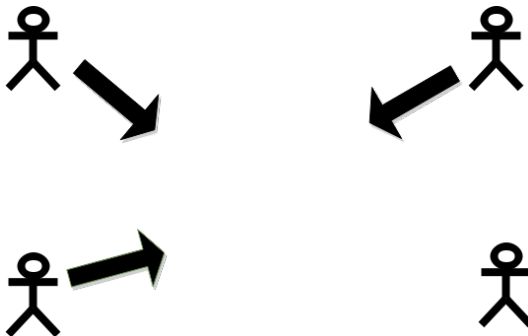
Universitatea din București

9 februarie, 2015

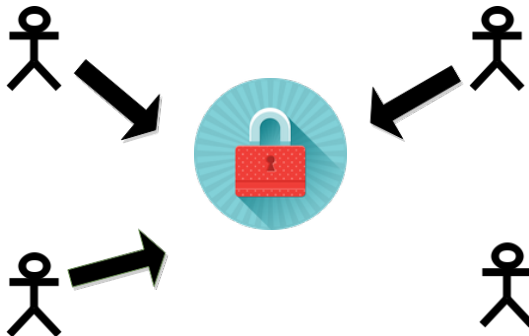
# Cuprins pentru secțiunea 1

- 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
- 6 Concluzii

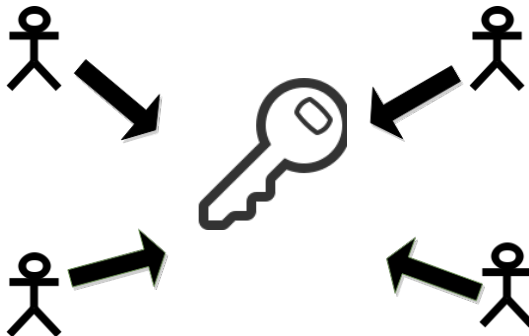
# Motivație: scheme de partajare



# Motivație: scheme de partajare



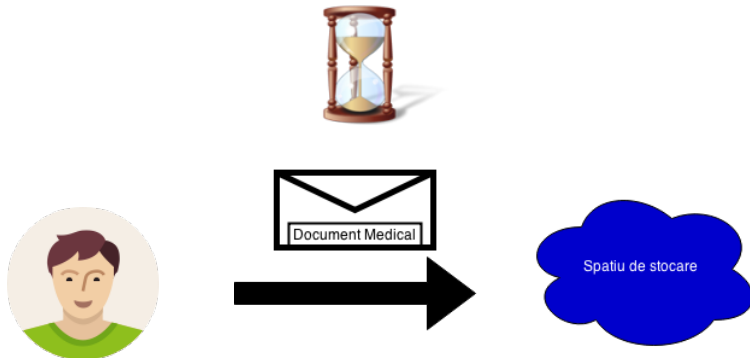
# Motivație: scheme de partajare



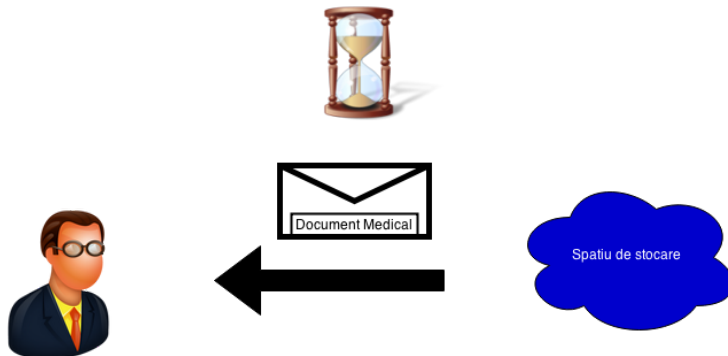
# Motivație: sisteme de stocare



# Motivație: sisteme de stocare



# Motivație: sisteme de stocare





# Cuprins pentru secțiunea 2

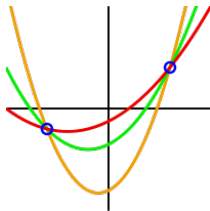
- 1 Overview
  - Motivație
- 2 Scheme de partajare
  - Schema Shamir
  - Schema unanimă XOR
  - Schema Ito, Saito și Nishizeki
- 3 Sisteme de stocare
  - RAID
  - PASIS
- 4 Alouneh et al.
- 5 Rezultate personale
  - Detectarea tipului de fișier partajat
  - Determinarea conținutului de fișier
  - Detectarea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

# 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

# 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  
Vlsergey

- Secret  $\mathcal{S}$

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

# Schema Shamir

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

- 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  $\mathcal{S}$



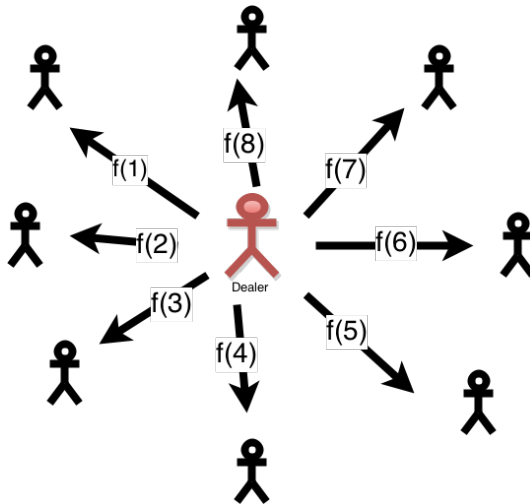
- Secret  $\mathcal{S}$
- Schema  $(k, n)$  majoritară
- Oricare  $k$  participanți din cei  $n$  pot reconstitui  $\mathcal{S}$
- Mai puțin de  $k$  participanți nu obțin nici o informație despre  $\mathcal{S}$
- Se alege un polinom  $f$  de grad  $k - 1$  având coeficienți aleatori, termenul liber 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 4 pot reconstitui secretul  $\mathcal{S}$ . Fie polinomul  $f(x) = a_3x^3 + a_2x^2 + a_1x + \mathcal{S}$ ,  $a_i \leftarrow^R Z_q$ ,  $a_i$  aleși în mod aleator din  $Z_q$ .

# Schema Shamir



# Schema unanimă XOR

- Schema majoritară  $(n, n)$ .

# Schema unanimă XOR

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

# 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  $S \oplus s_1 \oplus s_2 \oplus \dots \oplus s_{n-1}$ .

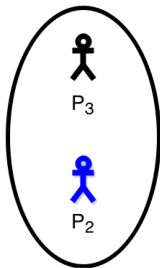
# Schema unanimă XOR

- 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
- 6 Concluzii

# 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

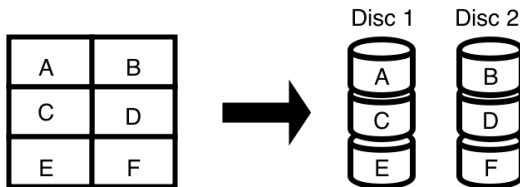
# Asigurarea disponibilității cu ajutorul sistemelor RAID

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

# Asigurarea disponibilității cu ajutorul sistemelor RAID

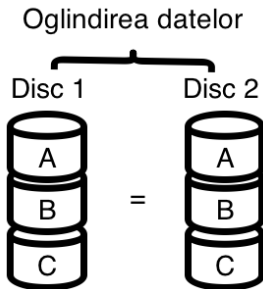
- RAID (Redundant Array of Independent Disks) combină 2 concepte ortgonale:
  - Data striping
  - Redundanța datelor
- Datele sunt distribuite în moduri diferite denumite niveluri RAID.

# Nivelul 0 Raid - Data Striping





# Nivelul 1 Raid - Redundanța datelor



- Securitatea este asigurată cu ajutorul schemelor de partajare.

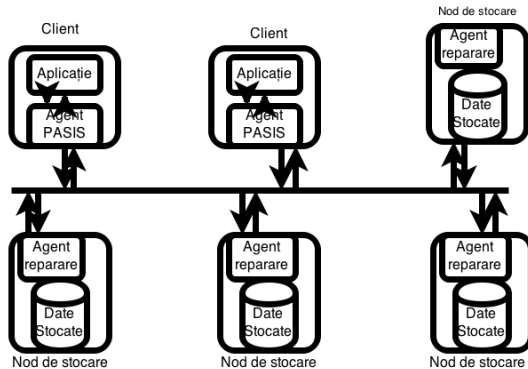
# Sisteme securizate de stocare de lungă durată

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

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

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

# PASIS (2000)



# 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
- 6 Concluzii

- 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  $f(i)$ .

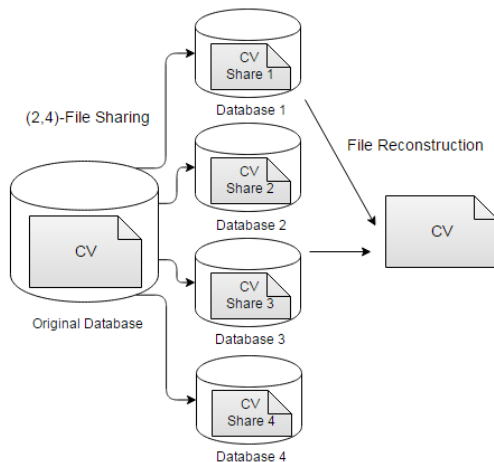
- Informația este partajată cu ajutorul unei aplicații la nivelul clientului folosind o versiune modificată a schemei Shamir.
- Coeficienții polinomului  $f$  nu mai sunt aleși aleator ci sunt luați direct din fisierul partajat in maniera secventială.
- Nodul cu indexul  $i$  primește valoarea polinomului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

## Exemplu

Fie un fișier *File* avand 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
- 6 Concluzii

- Construirea polinomului este deterministă!

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

Considerând că dealerul  $\mathcal{D}$  nu schimbă numerotoarea 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)(*) IONESCU	(2)(*) Victor	(4)
Adresa (număr, stradă, cod poștal, oraș, țară)		
(3) Aleea Florilor nr.14, bl. C23, ap.21, sector 3, CP 1024, București, România, 7000		
Data nașterii	Naționalitate	Semnătura titularului
(5) 03 04 1988 zz ll aaaa	(6) Română	(7)

NB : Rubricile marcate cu asterisc sunt obligatorii.

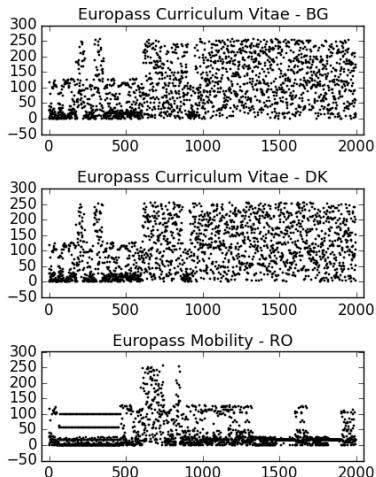
**2. ACEST DOCUMENT DE MOBILITATE EUROPASS SE ELIBEREAZĂ DE CĂTRE :**

Denumirea instituției emitente

Europass Mobility RO

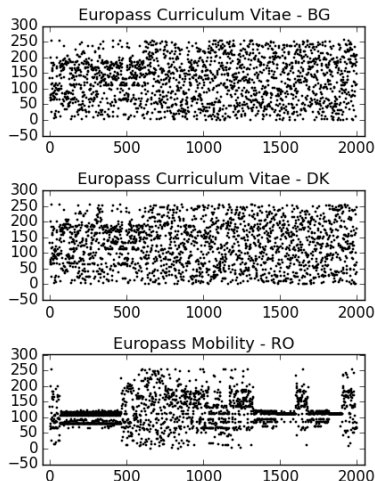
Partajarea celor 3 fișiere  
cu schema (2, 4).

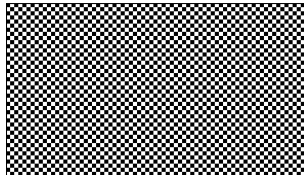
Adversarul obține  
componentele aflate pe  
nodul 1:



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

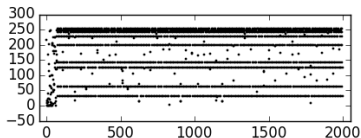
Adversarul obține  
componentele aflate pe  
nodul 2:



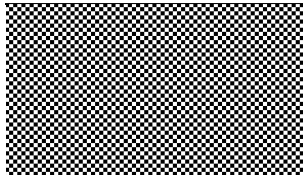




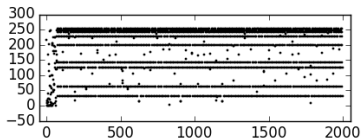
# Alouneh et al. (2013) - determinarea unui pattern în fișier



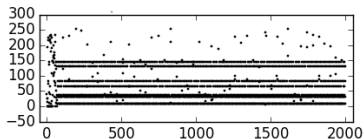
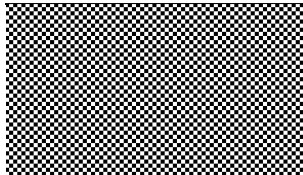
Nod 1



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

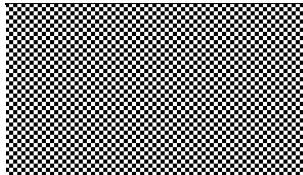
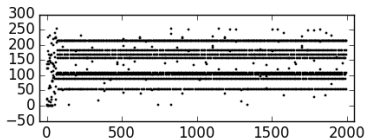


Nod 1



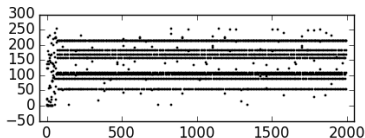
Nod 2

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

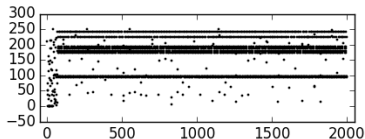
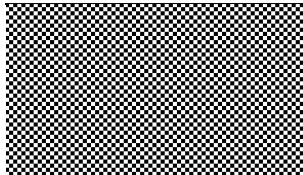


Nod 3

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



Nod 3



Nod 4

- Python 3.0
- Serializarea datelor: Cerealizer
- Grafice: Matplotlib

- Python 3.0
- Serializarea datelor: Cerealizer
- Grafice: Matplotlib
- Cod sursă: [▶ GitHub](#)

# Implementare

The screenshot shows the GitHub interface for the repository 'rdragos / splitting\_scheme'. At the top, there's a navigation bar with 'Explore', 'Gist', 'Blog', and 'Help'. Below this, the repository name is displayed along with statistics: 'Unwatch', '2' forks, '0' stars, and '0' forks. The main content area shows the 'splitting\_scheme' branch with a list of files and their commit history. The files listed are: generated\_shares, test\_data/Lenna, README, Tables.java, diff.py, generate.py, get\_shares.py, invtable.out, load.py, main.py, stats.py, and test.in. The README file is expanded, showing the text: 'Tested on python3.4.' and 'Requirements for running the script'. On the right side, there's a sidebar with links to 'Code', 'Issues', 'Pull Requests', 'Wiki', 'Pulse', 'Graphs', and 'Settings'. At the bottom of the sidebar, there's a section for 'HTTPS clone URL' and a 'Download ZIP' button.

some crypto implementation — Edit

27 commits 1 branch 0 releases 1 contributor

branch: master → splitting\_scheme / +

added diff

rdragos authored on 1 Nov 2014 latest commit a3ceda48br

generated_shares	moved generated shares	4 months ago
test_data/Lenna	added more stats	4 months ago
README	moved generated shares	4 months ago
Tables.java	scheme works now. next step: refactoring and finding some edge cases ...	4 months ago
diff.py	added diff	3 months ago
generate.py	refactored, added shares generator	4 months ago
get_shares.py	pretty file renaming	3 months ago
invtable.out	added more docs, cleaned up code	4 months ago
load.py	added loader	4 months ago
main.py	added more mem efficient main	4 months ago
stats.py	fixed little bug, this time including f(256)	3 months ago
test.in	gg lagrange	5 months ago

README

Tested on python3.4.

Requirements for running the script

Code

Issues

Pull Requests

Wiki

Pulse

Graphs

Settings

HTTPS clone URL

<https://github.com>

You can clone with HTTPS, SSH, or Subversion

Download ZIP

Cod GitHub

Articolul se află momentan în procesul de recenzie la Journal of Control Engineering and Applied Informatics (jurnal indexat ISI, categoria C)



Home > **Journal of Control Engineering and Applied Informatics**

## Journal of Control Engineering and Applied Informatics

Journal of Control Engineering and Applied Informatics

ISSN 1454-8658

ISI Impact Factor of our Journal is 0.228.

The Journal is promoting theoretical and practical results in a large research field of Control Engineering and Technical Informatics. It has been published since 1999 under the Romanian Society of Control Engineering and Technical Informatics coordination, in its quality of IPAC Romanian National Member Organization and it appears quarterly.

Each issue has 6-8 papers from various areas such as control theory, computer science, and applied informatics. Basic topics included in our Journal since 1999 have been time-invariant control systems, including robustness, stability, time delay aspects; advanced control strategies, including adaptive, predictive, nonlinear, intelligent, multi-model techniques; intelligent control techniques such as fuzzy, neural, genetic algorithms, and expert systems; and discrete event and hybrid systems, networks and embedded systems. Application areas covered have been environmental engineering, power systems, biomedical engineering, industrial and mobile robotics, and manufacturing.

Besides articles, this publication contains book views, correspondence and announcement regarding major scientific events organized in the area of Control Engineering and Technical Informatics, as well as PhD thesis presentations.

The Journal is supporting a forum for both theoretical and applied aspects of control and information technology and is elaborated in two versions: a theoretical version, including original papers whose contents has never been published before, and a version including papers of applicative quality, relevant for their technological contents and aiming at practical results. An important part of the mission of the Journal is to promote the C3 paradigm: computers and communications for control. A recent interest of the Journal consists in inclusion of cognitive techniques for achieving intelligent control under the C4 (C3+cognition) paradigm.

All the submitted articles are checked for plagiarism with [Plagiarism Detector](#).

### Announcements

#### All authors must upload the originality form.

All authors must upload the originality form together with each article.

Posted: 2015-01-28

[More...](#)

#### USER

Username   
Password   
☐ Remember me  
[Log In](#)

#### LANGUAGE

English 

#### JOURNAL CONTENT

Search   
All   
[Search](#)

#### Browse

- [By Issue](#)
- [By Author](#)
- [By Title](#)

#### INFORMATION

- [For Readers](#)
- [For Authors](#)
- [For Librarians](#)

## WebSite Jurnal

# Cuprins pentru secțiunea 6

- 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
- 6 Concluzii

Modificarea unor protocoale criptografice necesită demonstrații riguroase!

# Mulțumesc!