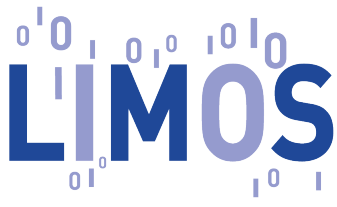
Recherche en sécurité

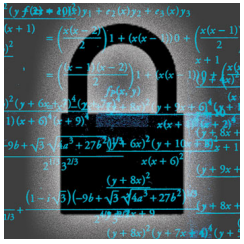
Pascal Lafourcade



23 Avril 2018
CIW

Security Activities @ LIMOS

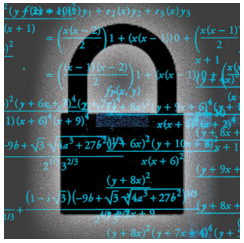
Designer



Attacker

Security Activities @ LIMOS

Designer

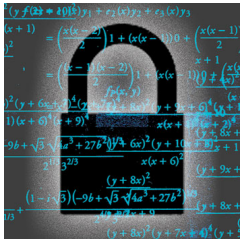


Attacker

Security Team

Security Activities @ LIMOS

Designer



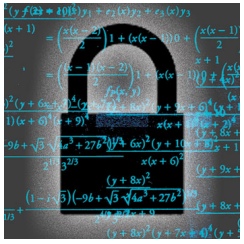
Attacker

Give a proof

Security Team

Security Activities @ LIMOS

Designer



Attacker

Give a proof

Find a flaw

Security Team

Applications

Outline

IOT and Security : Distance Bounding

Secure Matrix Multiplication with MapReduce

Ktimes Traceable Ring Signatures

Challenges

Outline

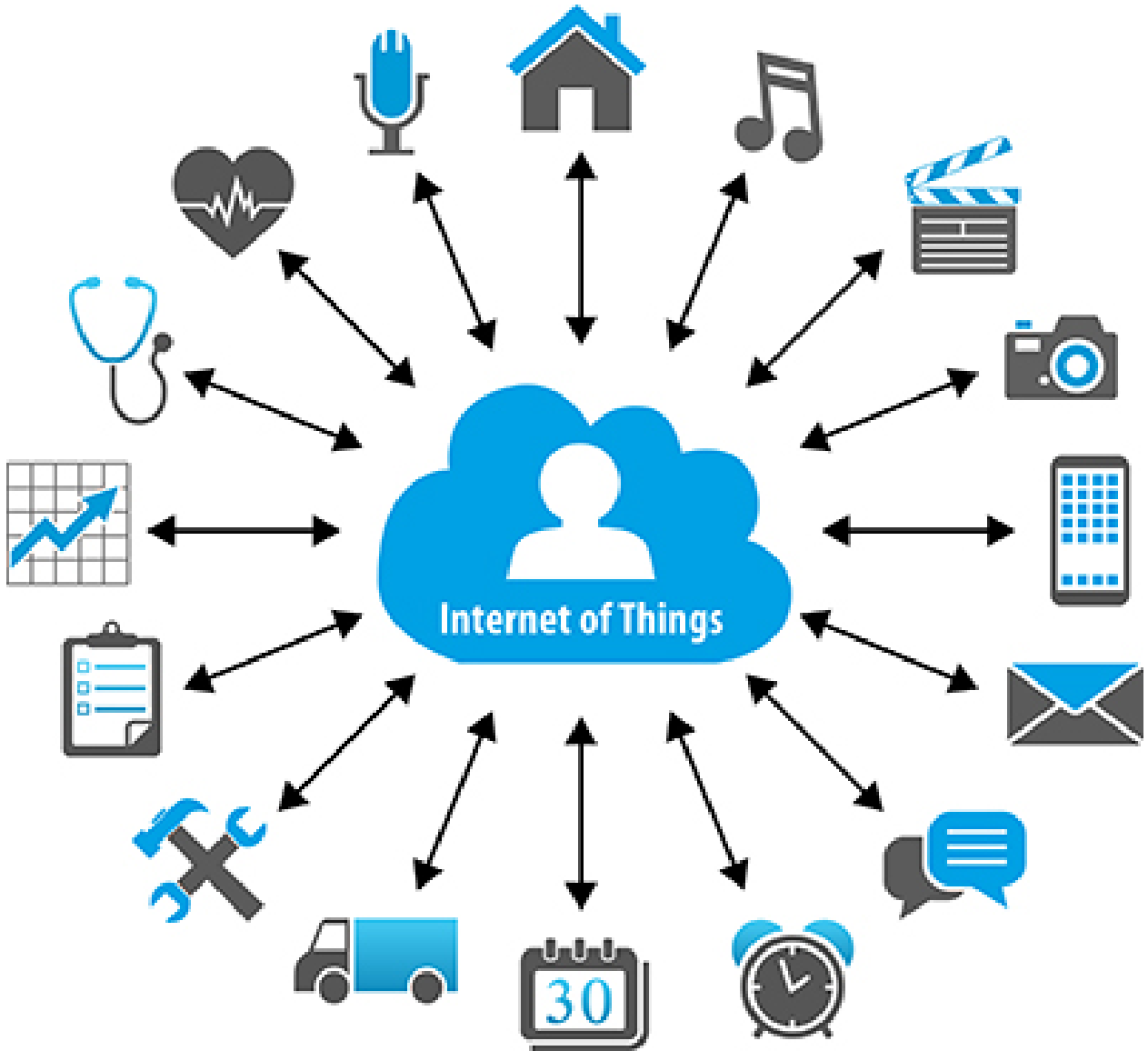
IOT and Security : Distance Bounding

Secure Matrix Multiplication with MapReduce

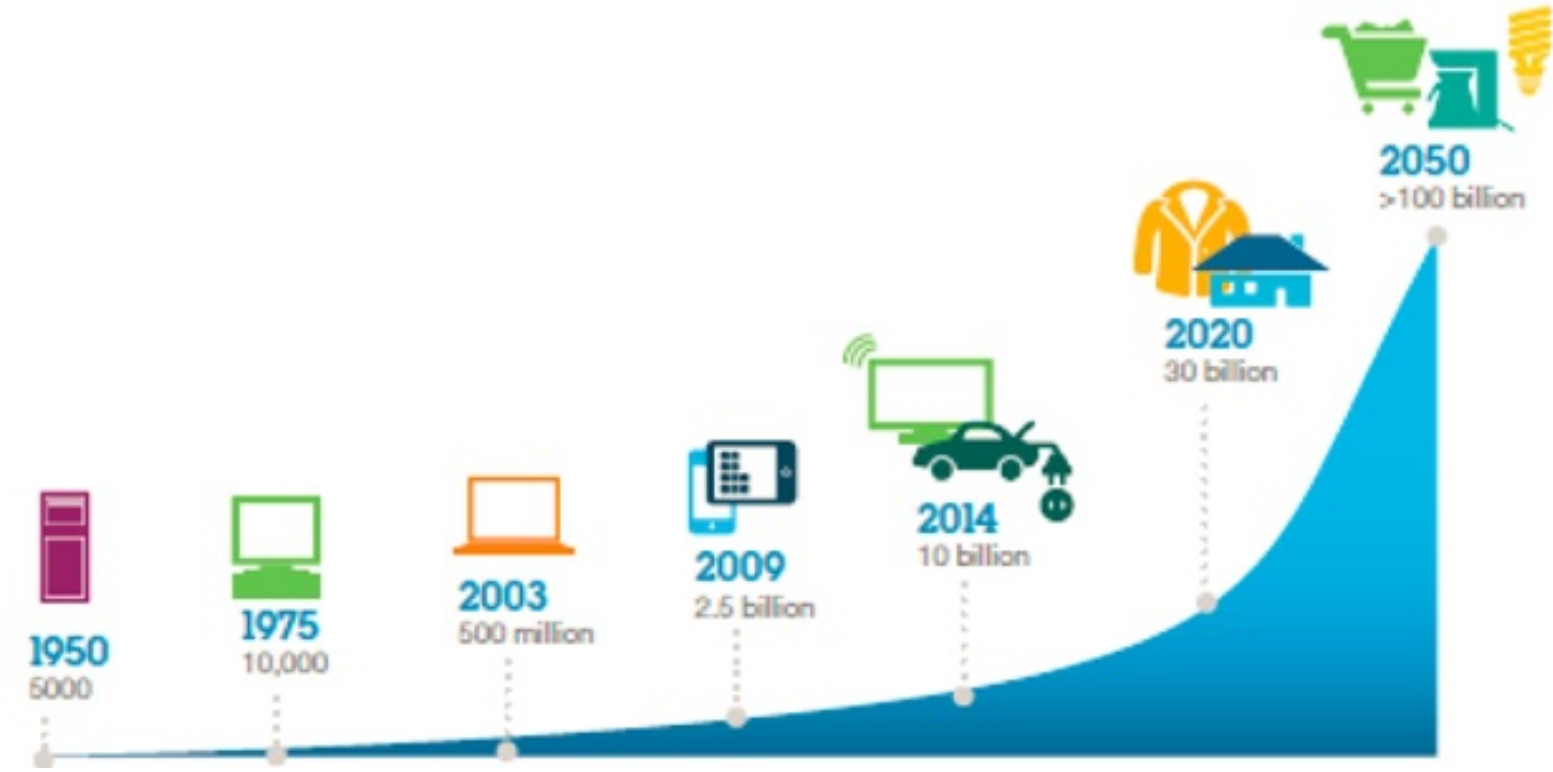
Ktimes Traceable Ring Signatures

Challenges

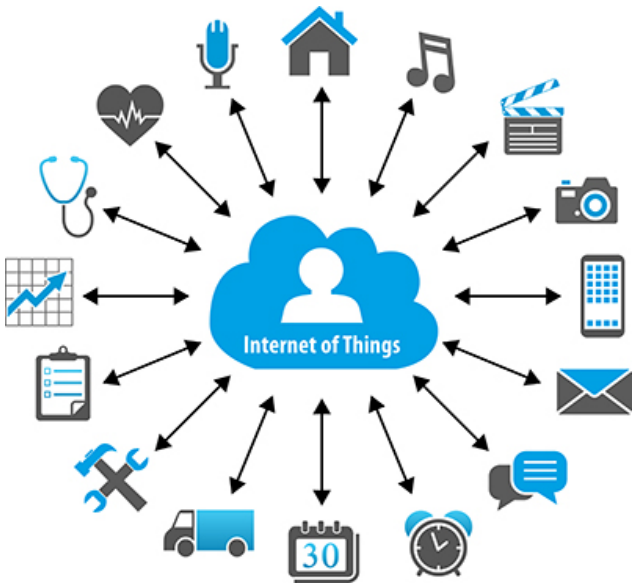
IoT



IoT


1950
5000
1975
10,000
2003
500 million
2009
2.5 billion
2014
10 billion
2020
30 billion
2050
>100 billion

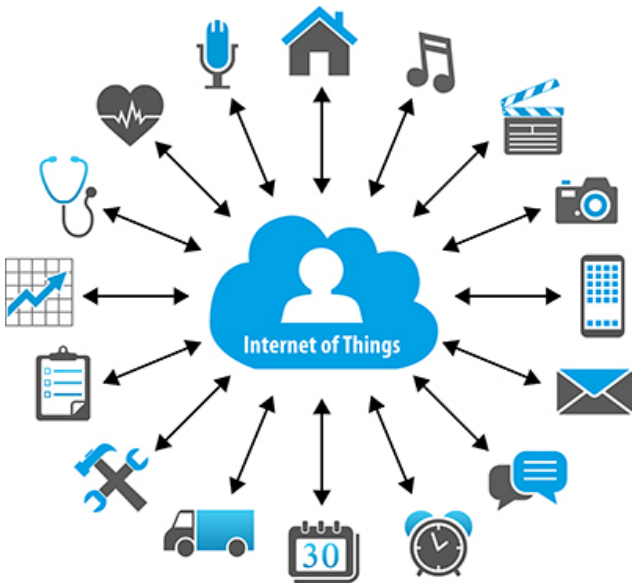
Reasons of the Succes of IOT



Usage

- Monitoring services
- Hyperconnectivity
- Avaibility
- Open data

Reasons of the Succes of IOT



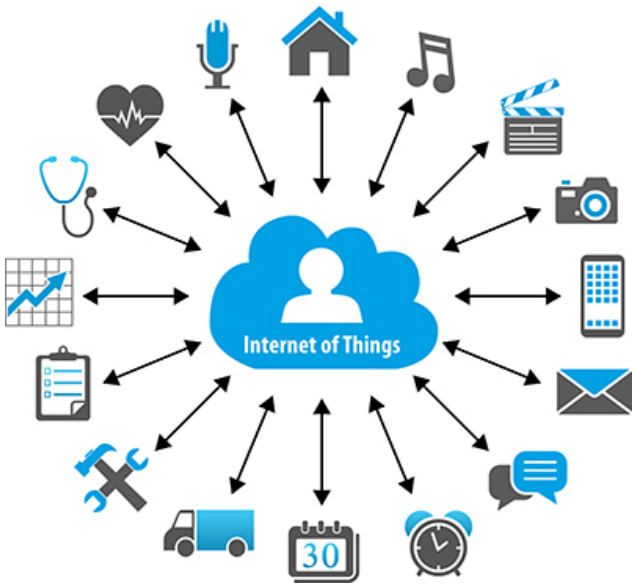
Usage

- Monitoring services
- Hyperconnectivity
- Avaibility
- Open data

Technology

- Wireless Communications: Wifi, 3G, 4G, Bluethooth ...
- Batteries
- CPU
- Sensors
- Price

Reasons of the Succes of IOT



Usage

- Monitoring services
- Hyperconnectivity
- Avaibility Security ?
- Open data

Technology

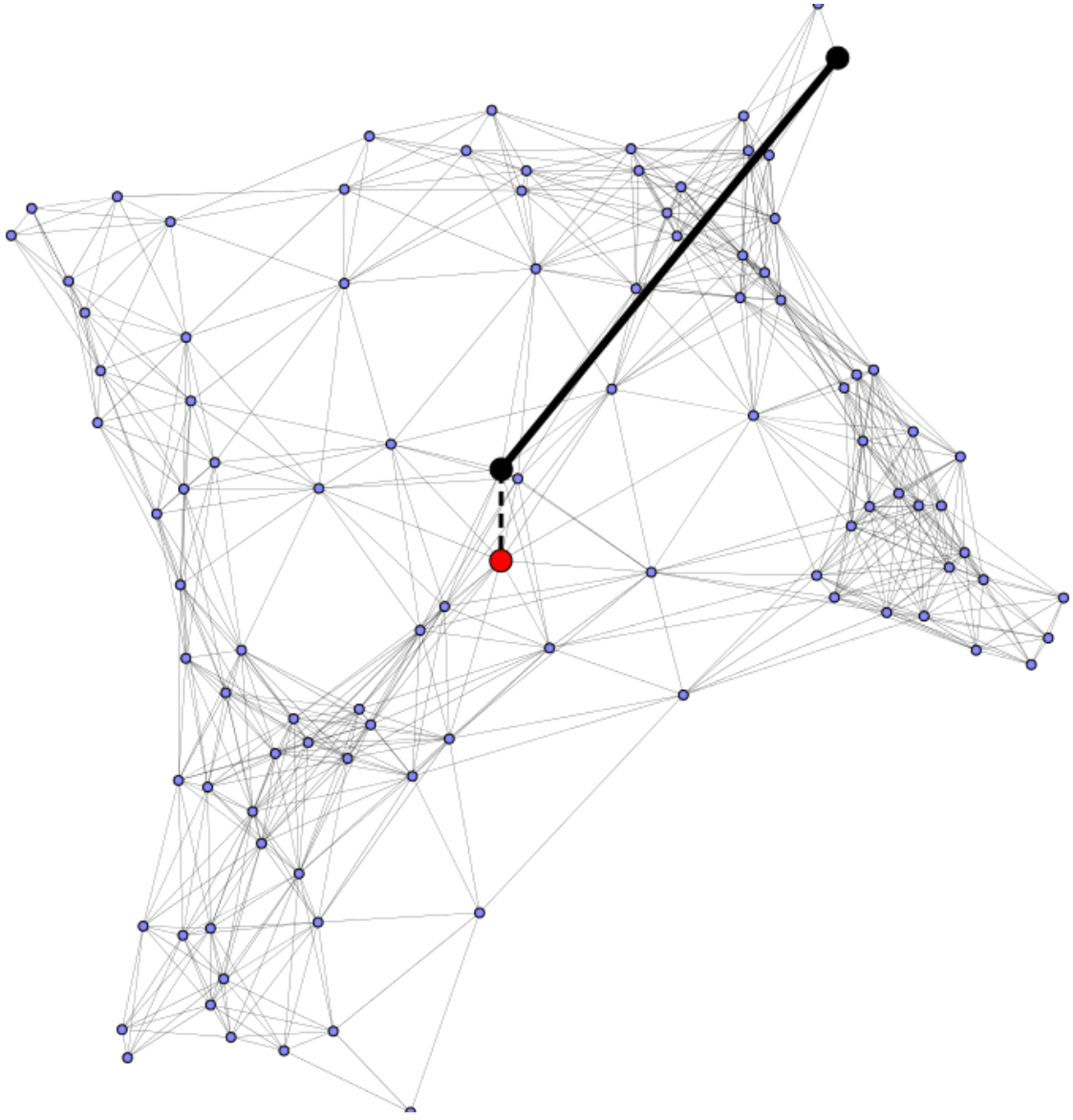
- Wireless Communications: Wifi, 3G, 4G, Bluethooth ...
- Batteries
- CPU
- Sensors
- Price

Proximity Devices Everywhere

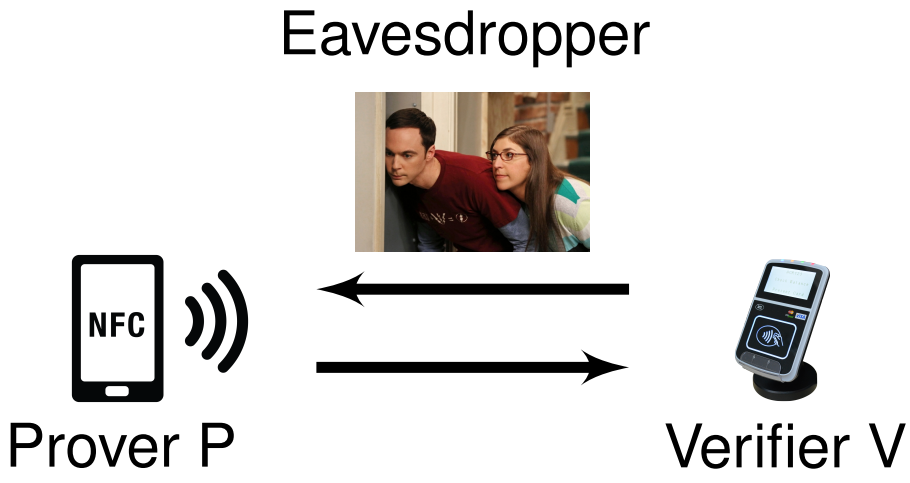
Proximity Devices Everywhere

What security do we want?

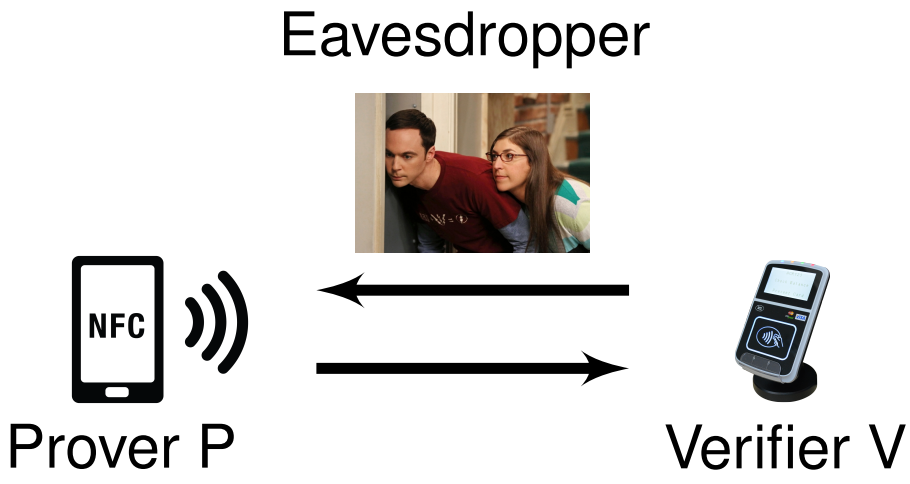
“Wormhole Attack”

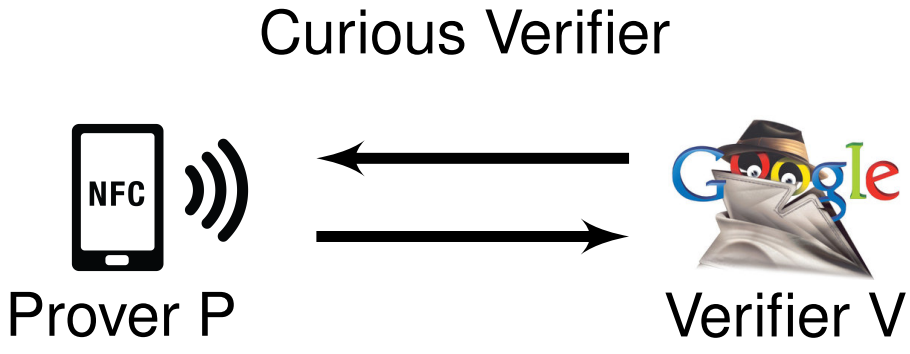


Intruder: Eavesdropper VS Curious Verifier



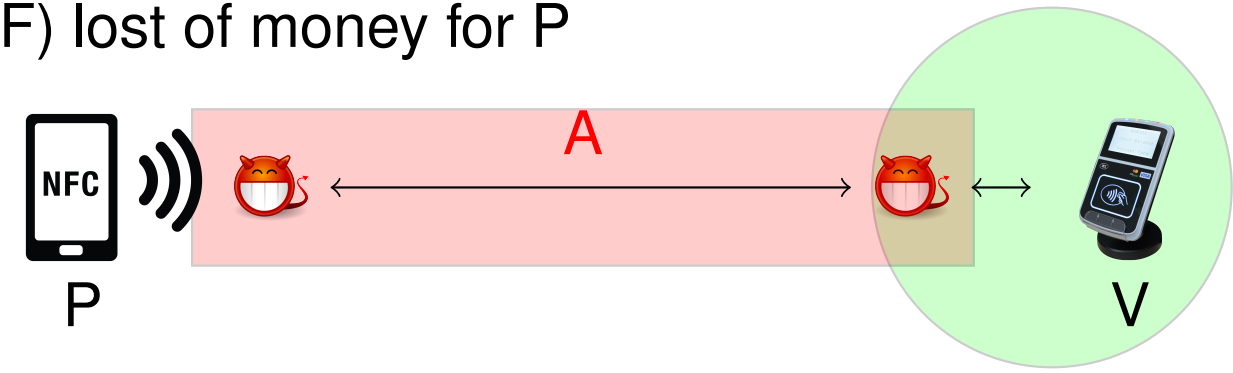
Intruder: Eavesdropper VS Curious Verifier





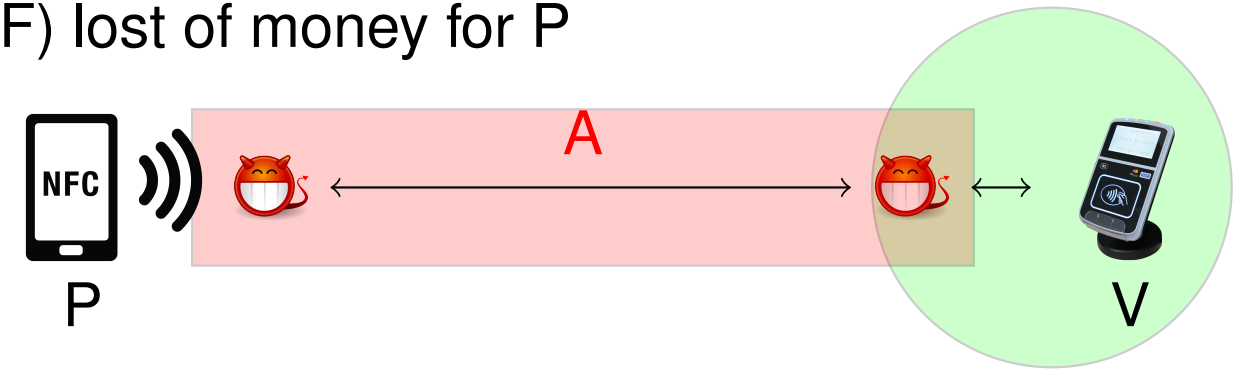
Properties: Threats against honest provers

Mafia Fraud (MF) lost of money for P



Properties: Threats against honest provers

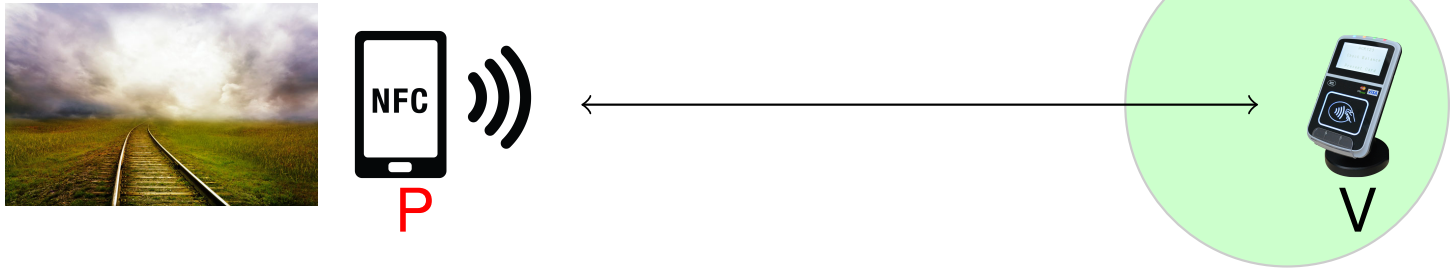
Mafia Fraud (MF) lost of money for P



User tracking

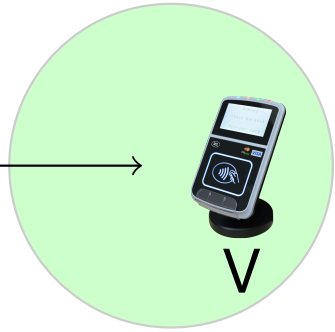
Properties: Threats with malicious Provers

Distance Fraud (DF) location usurpation

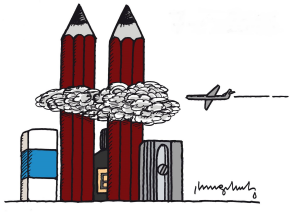


Properties: Threats with malicious Provers

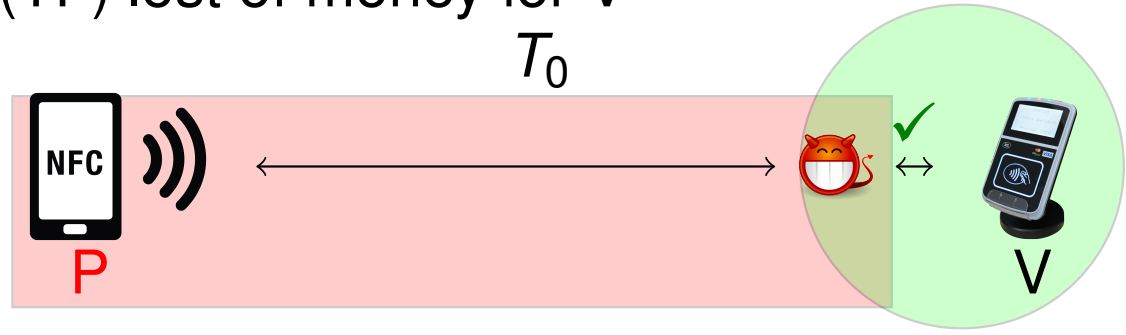
Distance Fraud (DF) location usurpation



Terrorist Fraud(TF) lost of money for V

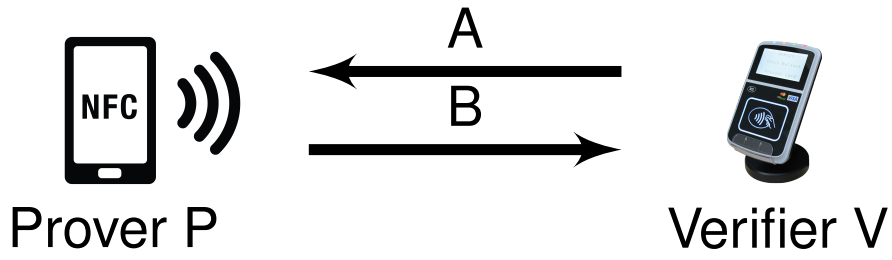


T_0

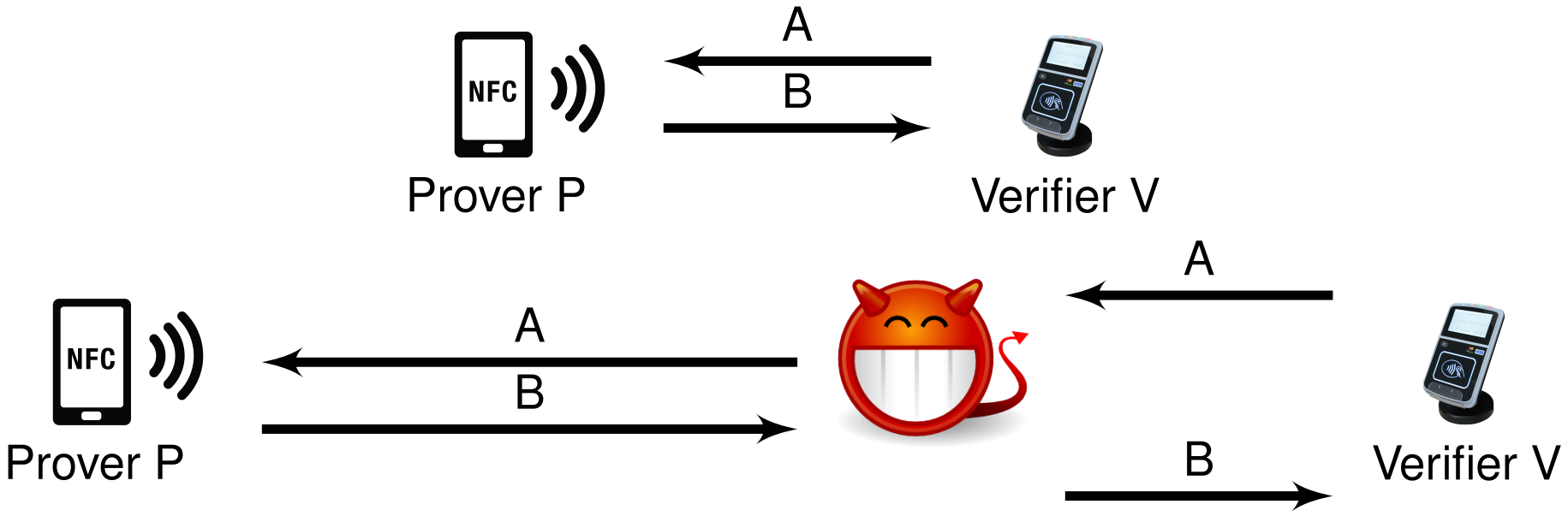


T_1

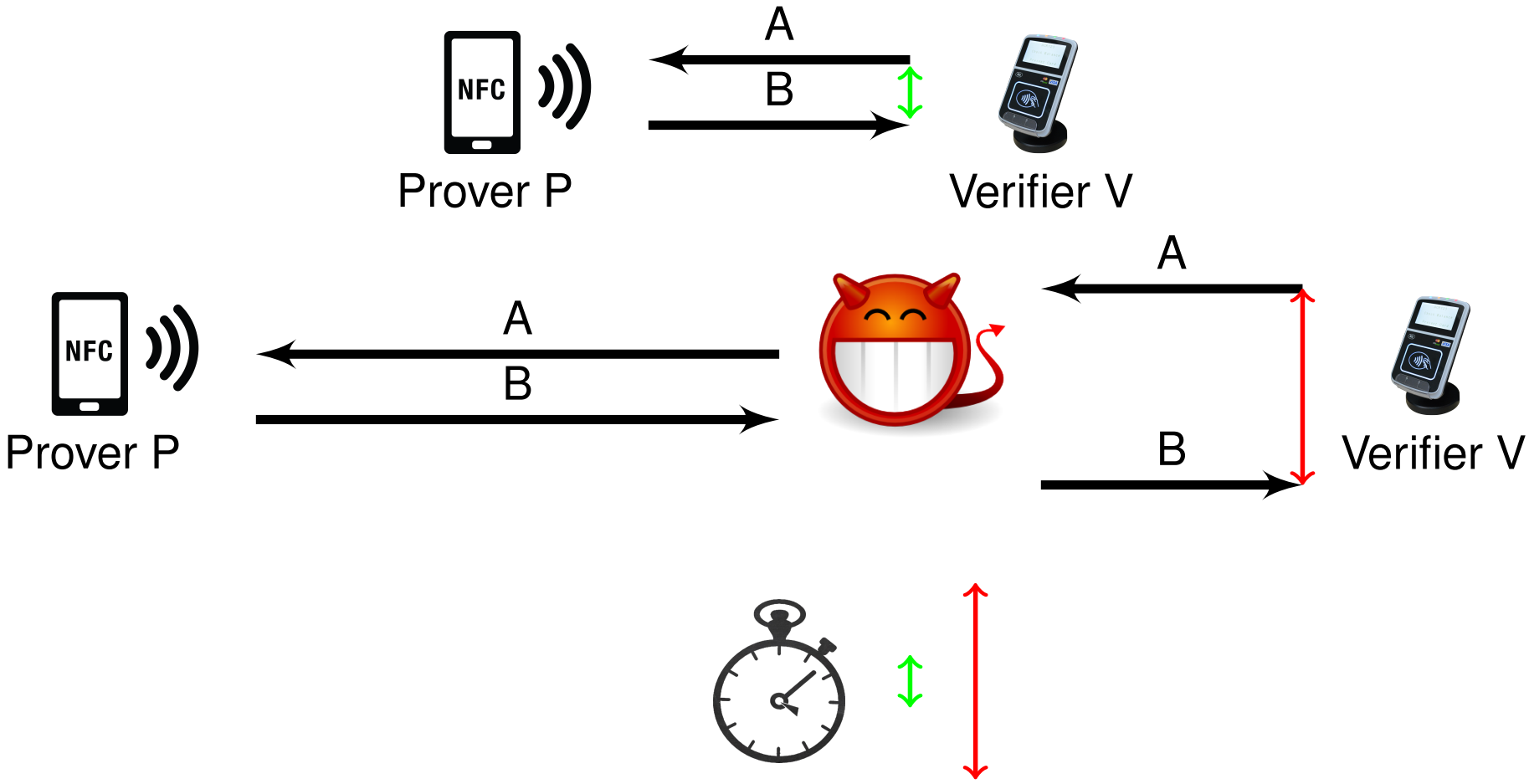
Distance Bounding Idea



Distance Bounding Idea

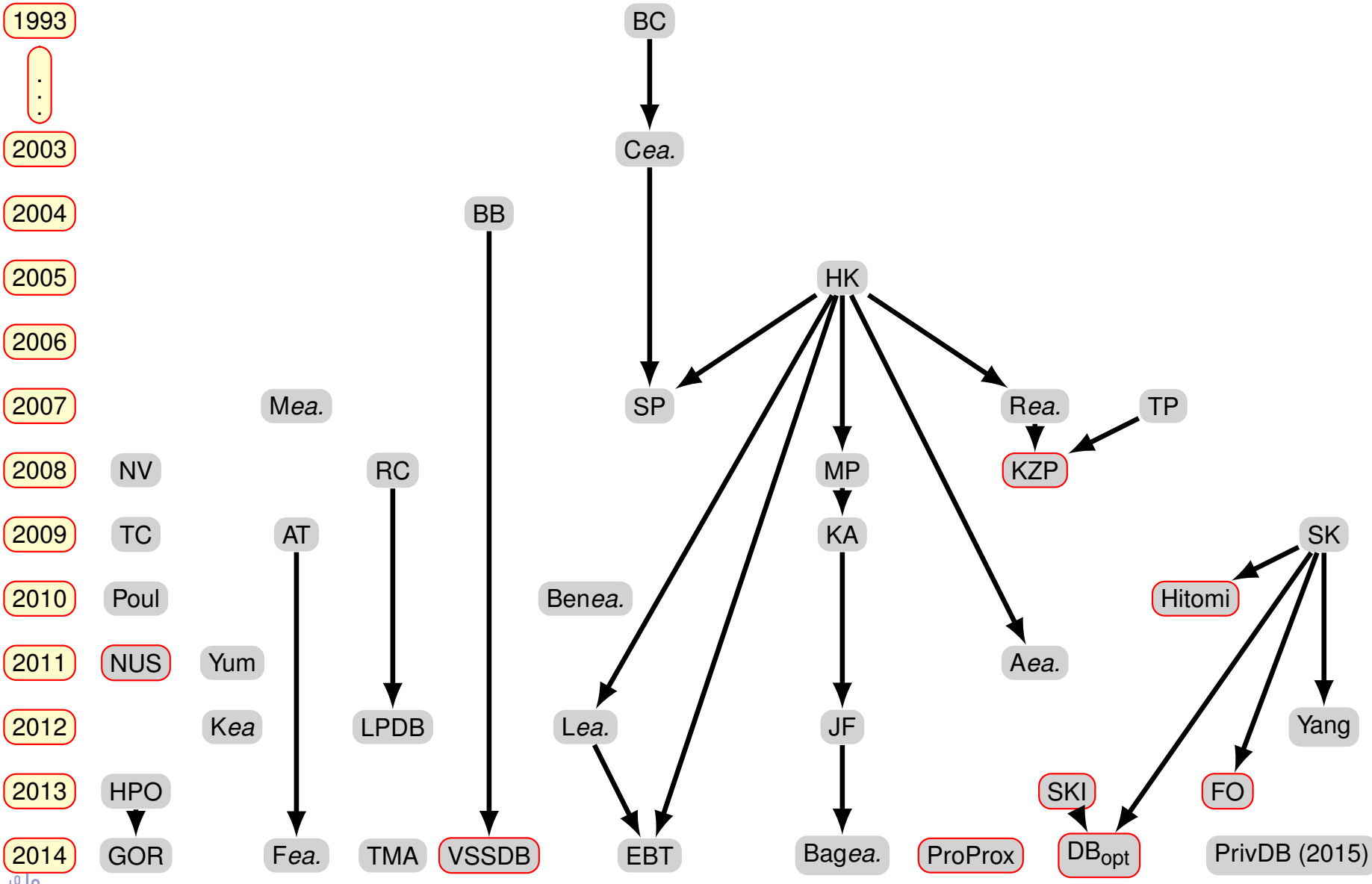


Distance Bounding Idea



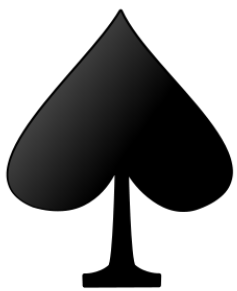
Solution against MF: Distance Bounding (Brands and Chaum, 1991)

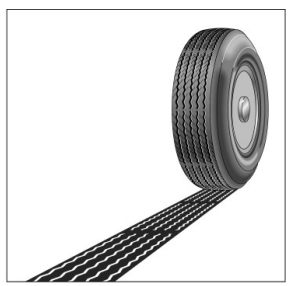
Survey : 42 protocols from 1993 to 2015.



LIMOS Contributions

- Designing secure IoT is difficult
- Distance Bounding can help to improve security
- SPADE and TREAD: 2 secure DB protocols





Outline

IOT and Security : Distance Bounding

Secure Matrix Multiplication with MapReduce

Ktimes Traceable Ring Signatures

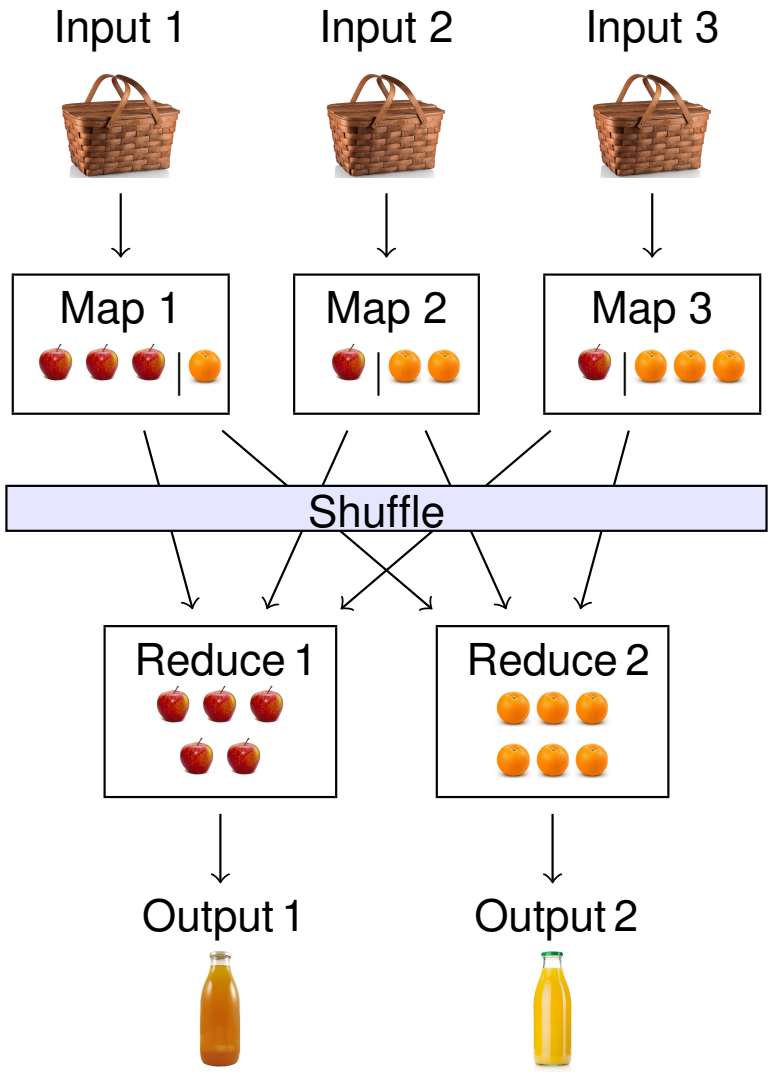
Challenges

MapReduce

- Partitioning input data
- Scheduling program execution on machines
- Performing the shuffle
- Handling machine failures

Programmer specifies:

- Map and Reduce functions
- Input files



Matrix Multiplication

$$M_{a,b} \cdot N_{b,c} = P_{a,c}$$

Matrix Multiplication

$$M_{a,b} \cdot N_{b,c} = P_{a,c}$$

$$N_{2,3} = \begin{bmatrix} 0 & 2 & 3 \\ 1 & 0 & 6 \end{bmatrix}$$

$$M_{2,2} = \begin{bmatrix} 1 & 2 \\ 0 & 5 \end{bmatrix} \quad P_{2,3} = \begin{bmatrix} 1\cdot 0+2\cdot 1=2 & 1\cdot 2+2\cdot 0=2 & 1\cdot 3+2\cdot 6=15 \\ 0\cdot 0+5\cdot 1=5 & 0\cdot 2+5\cdot 0=0 & 0\cdot 3+5\cdot 6=30 \end{bmatrix}$$

Matrix Multiplication

$$M_{a,b} \cdot N_{b,c} = P_{a,c}$$

$$N_{2,3} = \begin{bmatrix} 0 & 2 & 3 \\ 1 & 0 & 6 \end{bmatrix}$$

$$M_{2,2} = \begin{bmatrix} 1 & 2 \\ 0 & 5 \end{bmatrix} \quad P_{2,3} = \begin{bmatrix} 1\cdot 0+2\cdot 1=2 & 1\cdot 2+2\cdot 0=2 & 1\cdot 3+2\cdot 6=15 \\ 0\cdot 0+5\cdot 1=5 & 0\cdot 2+5\cdot 0=0 & 0\cdot 3+5\cdot 6=30 \end{bmatrix}$$

M

i	j	m_{ij}
1	1	1
1	2	2
2	1	0
2	2	5

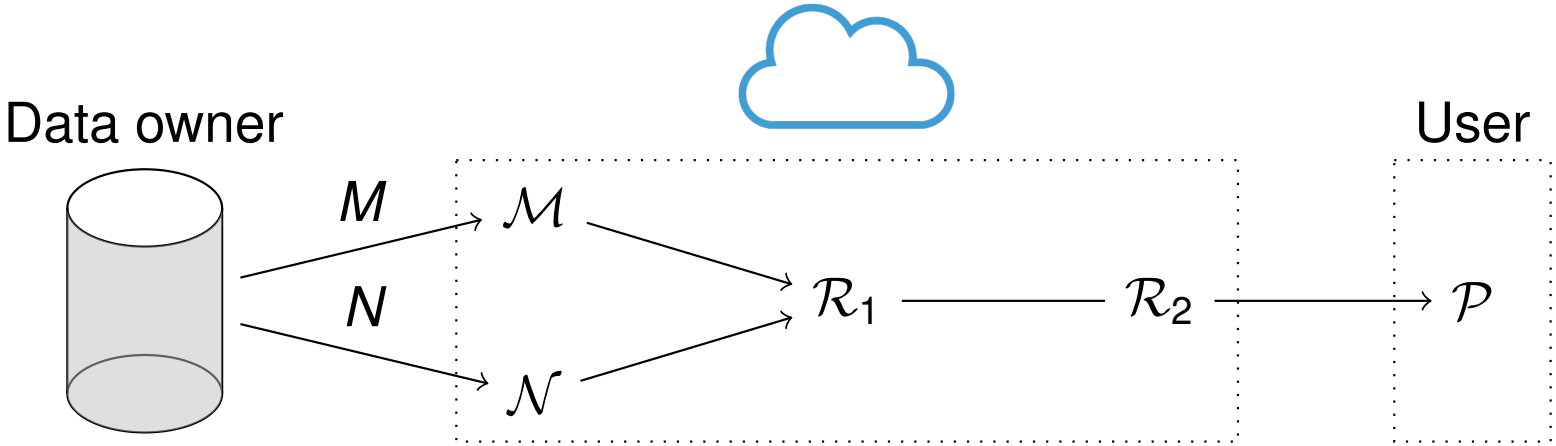
N

j	k	n_{jk}
1	1	0
1	2	2
1	3	3
2	1	1
2	2	0
2	3	6

P

i	k	p_{ik}
1	1	2
1	2	2
1	3	15
2	1	5
2	2	0
2	3	30

Matrix Multiplication with 2 Rounds



Round 1

Map:

- $\mathcal{M} \to \mathcal{R}_1$: $\{(j, (M, i, m_{ij}))\}_{1 \le i \le a, 1 \le j \le b}$
- $\mathcal{N} \to \mathcal{R}_1$: $\{(j, (N, k, n_{jk}))\}_{1 \le j \le b, 1 \le k \le c}$

Reduce: $\mathcal{R}_1 \to \mathcal{R}_2$: $\{((i, k), m_{ij} \cdot n_{jk})\}_{1 \le i \le a, 1 \le j \le b, 1 \le k \le c}$

Round 2

Map: identity $functionf(x) = x$

Reduce: $\mathcal{R}_2 \to \mathcal{P}$: $\{(i, k), p_{ik} = \sum_{j=1}^{b} m_{ij} \cdot n_{jk}\}_{1 \le i \le a, 1 \le k \le c}$

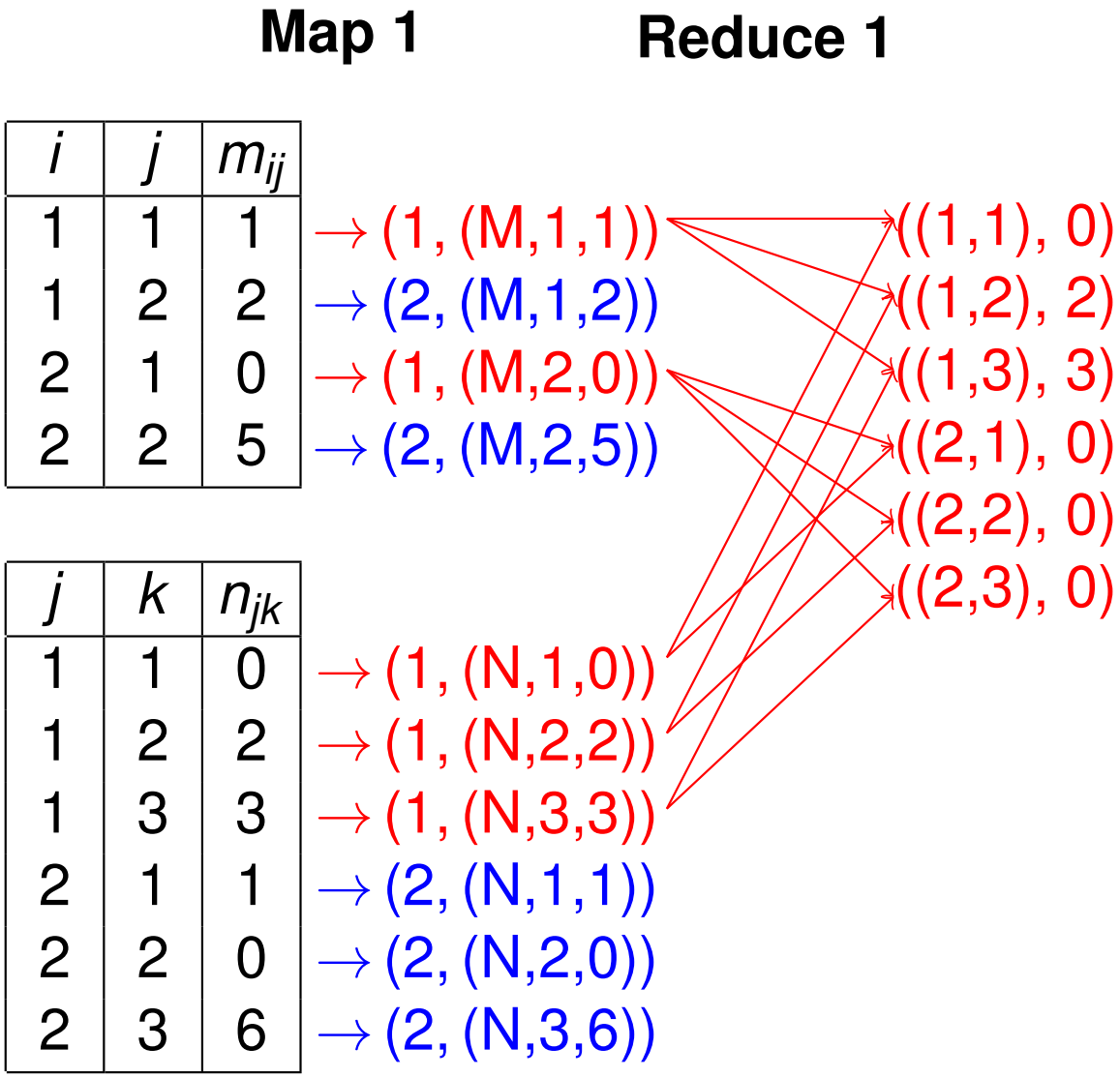
Example

Map 1

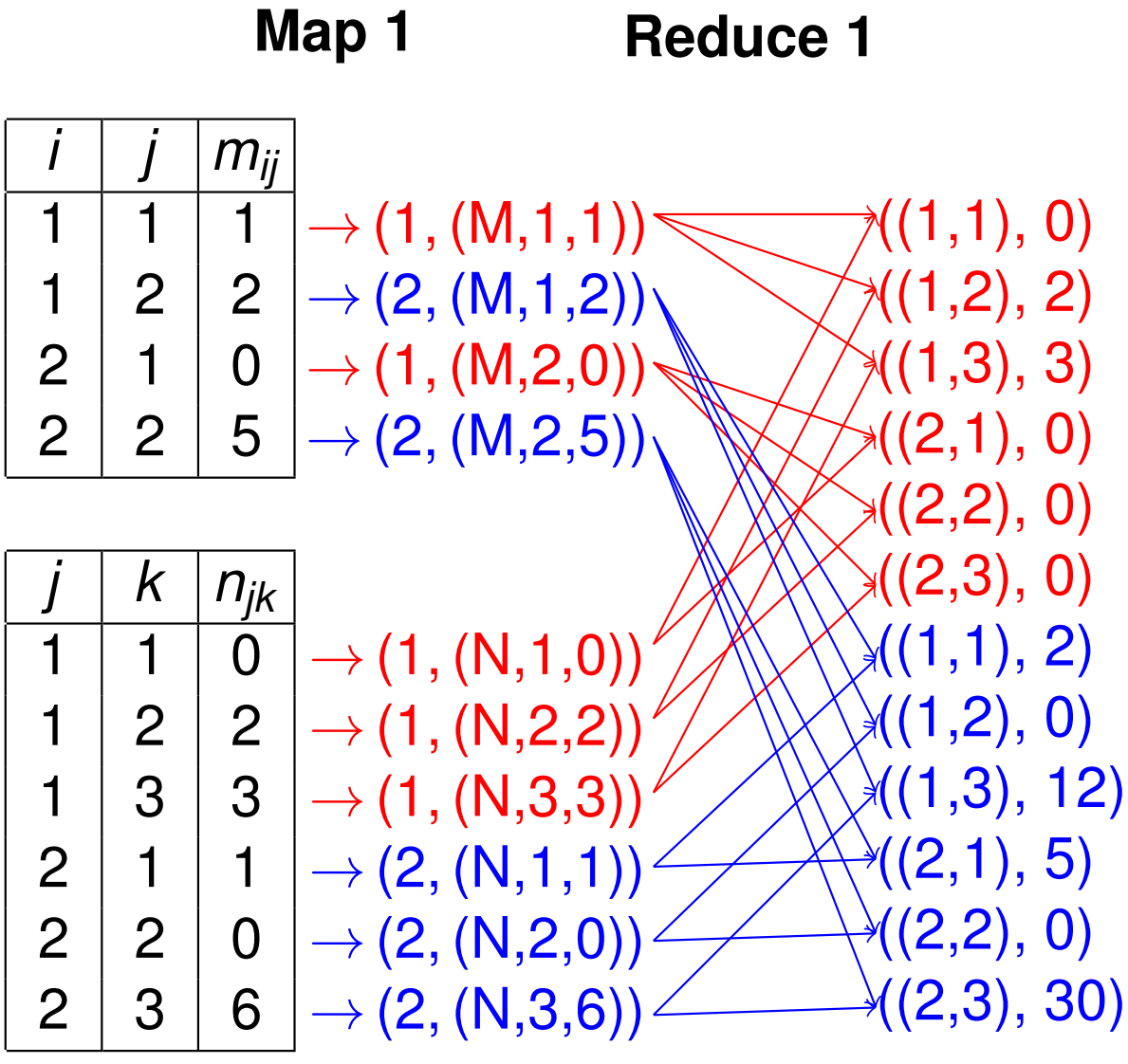
i	j	m_{ij}	
1	1	1	$\rightarrow$ (1, (M,1,1))
1	2	2	$\rightarrow$ (2, (M,1,2))
2	1	0	$\rightarrow$ (1, (M,2,0))
2	2	5	$\rightarrow$ (2, (M,2,5))

j	k	n_{jk}	
1	1	0	$\rightarrow$ (1, (N,1,0))
1	2	2	$\rightarrow$ (1, (N,2,2))
1	3	3	$\rightarrow$ (1, (N,3,3))
2	1	1	$\rightarrow$ (2, (N,1,1))
2	2	0	$\rightarrow$ (2, (N,2,0))
2	3	6	$\rightarrow$ (2, (N,3,6))

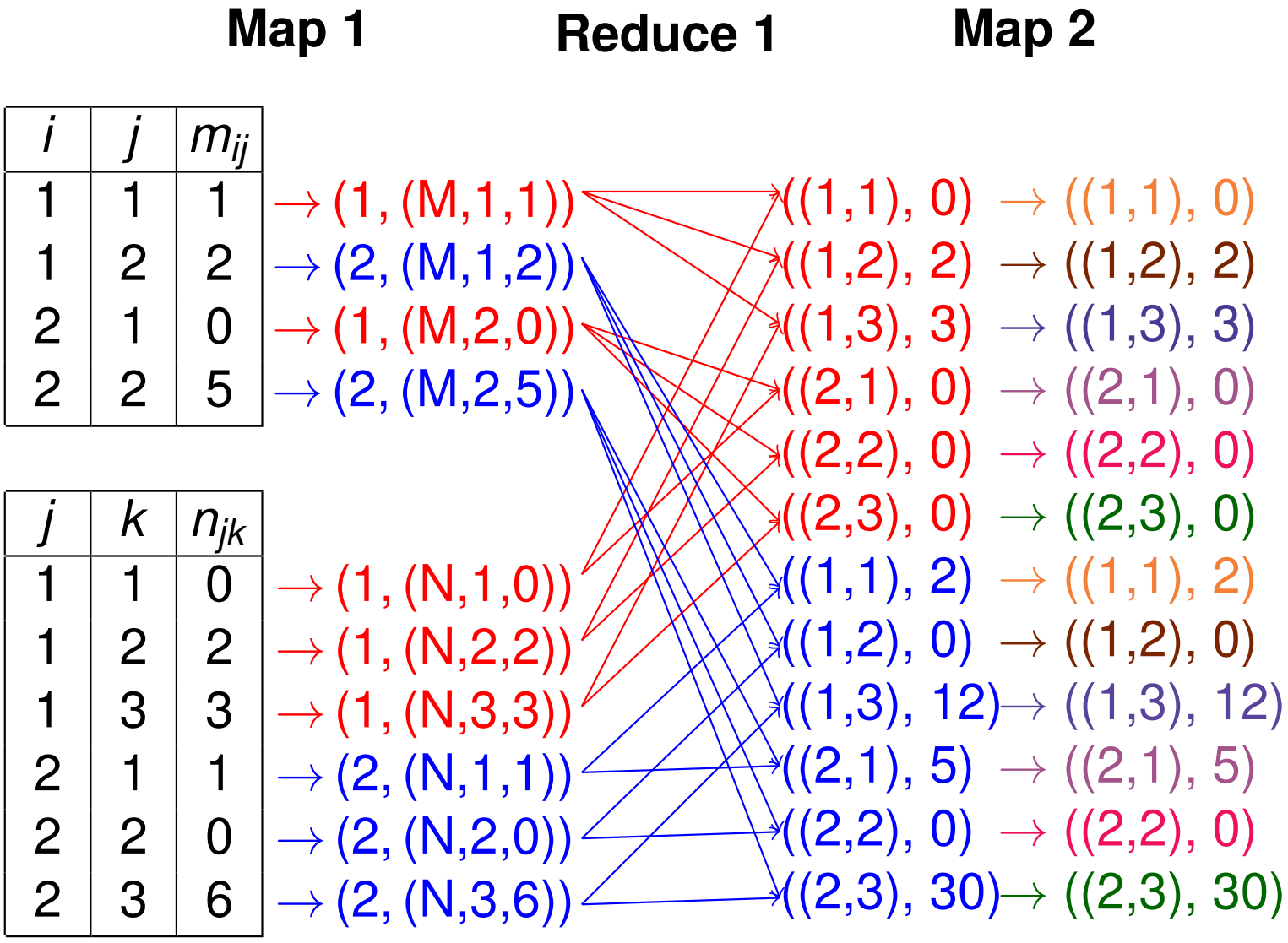
Example


Map 1
Reduce 1
i j m_{ij}
1 1 1
1 2 2
2 1 0
2 2 5
j k n_{jk}
1 1 0
1 2 2
1 3 3
2 1 1
2 2 0
2 3 6
→ (1, (M,1,1))
→ (2, (M,1,2))
→ (1, (M,2,0))
→ (2, (M,2,5))
→ (1, (N,1,0))
→ (1, (N,2,2))
→ (1, (N,3,3))
→ (2, (N,1,1))
→ (2, (N,2,0))
→ (2, (N,3,6))
((1,1), 0)
((1,2), 2)
((1,3), 3)
((2,1), 0)
((2,2), 0)
((2,3), 0)

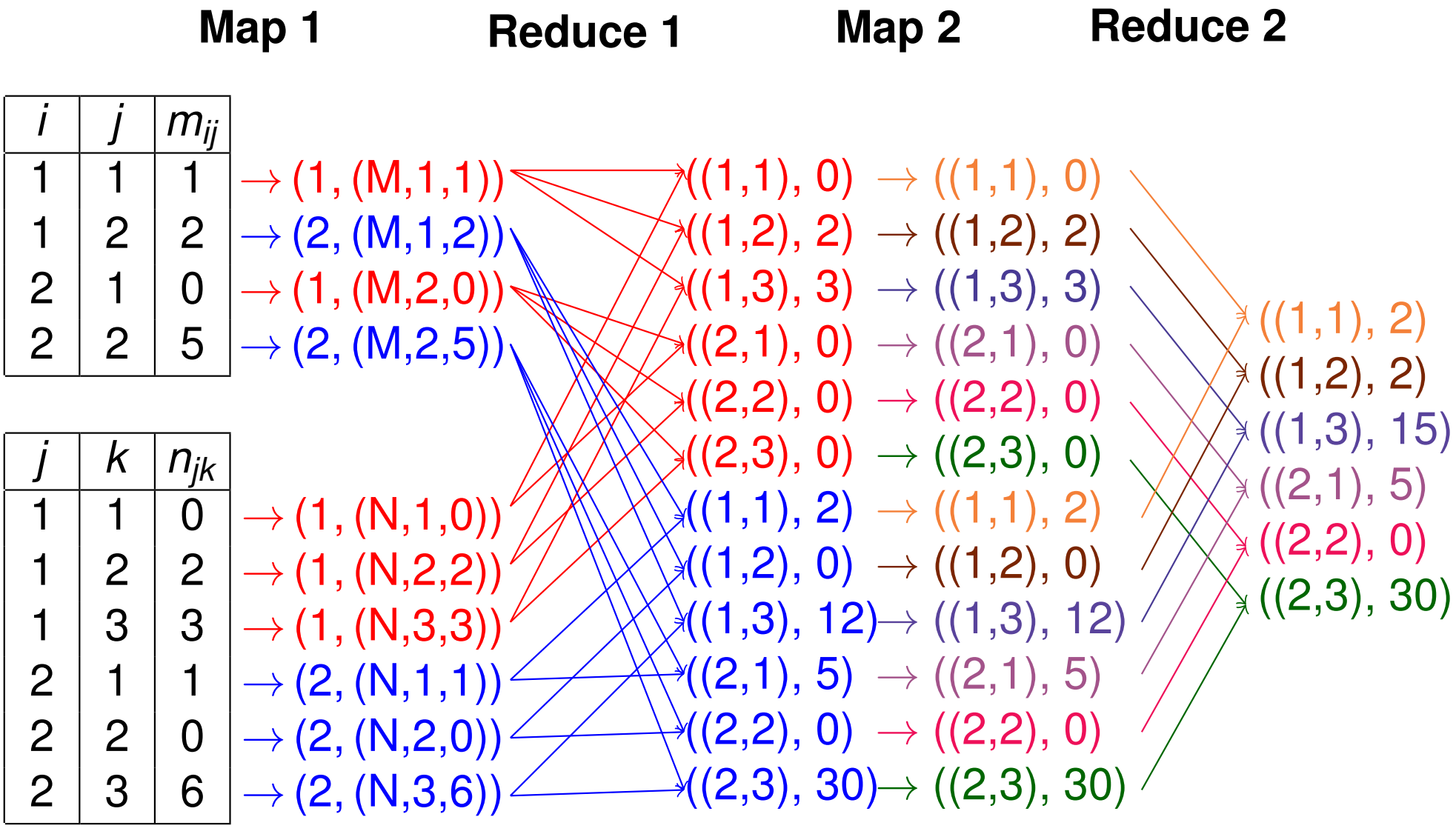
Example


Map 1
Reduce 1
i j m_{ij}
1 1 1
1 2 2
2 1 0
2 2 5
j k n_{jk}
1 1 0
1 2 2
1 3 3
2 1 1
2 2 0
2 3 6
→ (1, (M,1,1))
→ (2, (M,1,2))
→ (1, (M,2,0))
→ (2, (M,2,5))
→ (1, (N,1,0))
→ (1, (N,2,2))
→ (1, (N,3,3))
→ (2, (N,1,1))
→ (2, (N,2,0))
→ (2, (N,3,6))
((1,1), 0)
((1,2), 2)
((1,3), 3)
((2,1), 0)
((2,2), 0)
((2,3), 0)
((1,1), 2)
((1,2), 0)
((1,3), 12)
((2,1), 5)
((2,2), 0)
((2,3), 30)

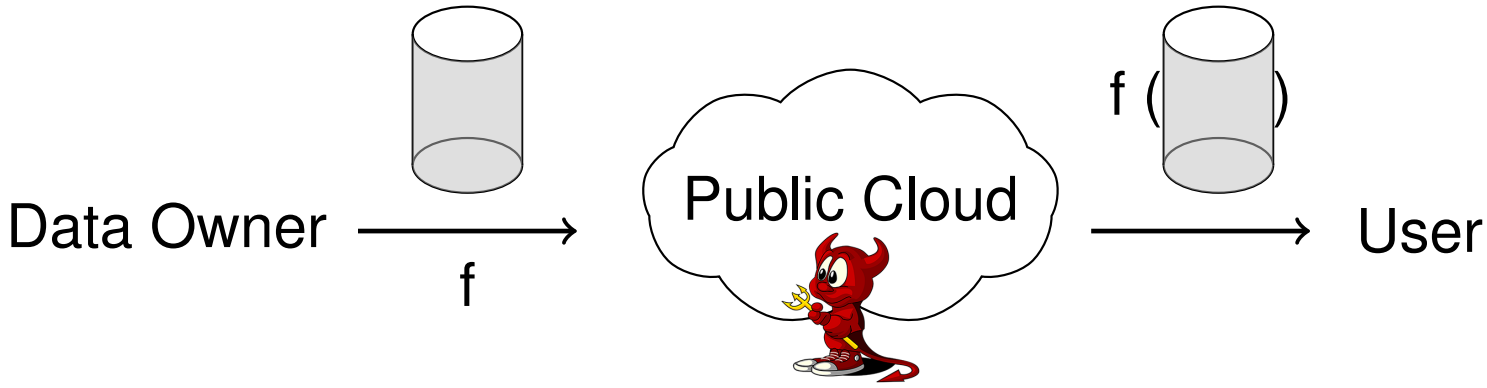
Example


Map 1
Reduce 1
Map 2
i j m_{ij}
1 1 1
1 2 2
2 1 0
2 2 5
j k n_{jk}
1 1 0
1 2 2
1 3 3
2 1 1
2 2 0
2 3 6
→ (1, (M,1,1))
→ (2, (M,1,2))
→ (1, (M,2,0))
→ (2, (M,2,5))
→ (1, (N,1,0))
→ (1, (N,2,2))
→ (1, (N,3,3))
→ (2, (N,1,1))
→ (2, (N,2,0))
→ (2, (N,3,6))
((1,1), 0)
((1,2), 2)
((1,3), 3)
((2,1), 0)
((2,2), 0)
((2,3), 0)
((1,1), 2)
((1,2), 0)
((1,3), 12)
((2,1), 5)
((2,2), 0)
((2,3), 30)
→ ((1,1), 0)
→ ((1,2), 2)
→ ((1,3), 3)
→ ((2,1), 0)
→ ((2,2), 0)
→ ((2,3), 0)
→ ((1,1), 2)
→ ((1,2), 0)
→ ((1,3), 12)
→ ((2,1), 5)
→ ((2,2), 0)
→ ((2,3), 30)

Example


Map 1
Reduce 1
Map 2
Reduce 2
i j m_{ij}
1 1 1
1 2 2
2 1 0
2 2 5
j k n_{jk}
1 1 0
1 2 2
1 3 3
2 1 1
2 2 0
2 3 6
→ (1, (M,1,1))
→ (2, (M,1,2))
→ (1, (M,2,0))
→ (2, (M,2,5))
→ (1, (N,1,0))
→ (1, (N,2,2))
→ (1, (N,3,3))
→ (2, (N,1,1))
→ (2, (N,2,0))
→ (2, (N,3,6))
((1,1), 0)
((1,2), 2)
((1,3), 3)
((2,1), 0)
((2,2), 0)
((2,3), 0)
((1,1), 2)
((1,2), 0)
((1,3), 12)
((2,1), 5)
((2,2), 0)
((2,3), 30)
→ ((1,1), 0)
→ ((1,2), 2)
→ ((1,3), 3)
→ ((2,1), 0)
→ ((2,2), 0)
→ ((2,3), 0)
→ ((1,1), 2)
→ ((1,2), 0)
→ ((1,3), 12)
→ ((2,1), 5)
→ ((2,2), 0)
→ ((2,3), 30)
((1,1), 2)
((1,2), 2)
((1,3), 15)
((2,1), 5)
((2,2), 0)
((2,3), 30)

Secure Computations with MapReduce



Assumption

- The cloud is honest-but-curious

Security properties

- Cloud nodes can learn neither  nor f()
- User is allowed to query f() but cannot learn 

Contributions

Secure approaches for **2-rounds MapReduce matrix multiplication**

- Secure-Private (SP) – assumes no collusions between cloud nodes
- Collusion-Resistant-Secure-Private (CRSP) – resists to collusions but needs user interactions

Similar results for **1-round MapReduce matrix multiplication**

Outline

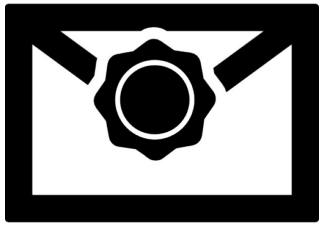
IOT and Security : Distance Bounding

Secure Matrix Multiplication with MapReduce

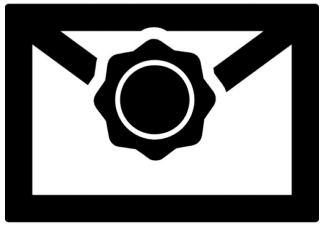
Ktimes Traceable Ring Signatures

Challenges

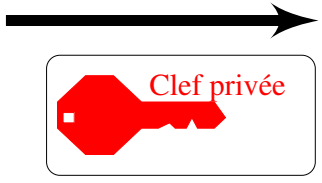
Signature



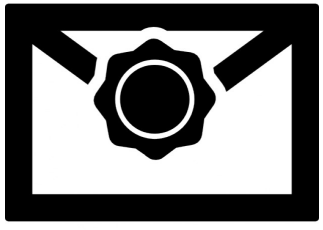
Signature



Signature



Secrete key

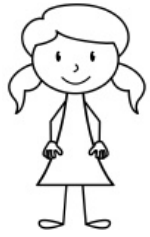


Verification

Public key

1977, RSA: $m^d \mod n$

Ring Signature (Rivest et al., 2001)

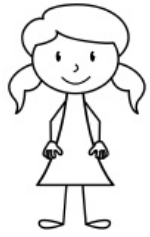
Alice  (m_1, σ_1) (m_2, σ_2) (m_3, σ_3)	Bob  (m_4, σ_4)
Carol  (m_5, σ_5) (m_6, σ_6)	David  (m_7, σ_7)

Observer

σ_1, σ_2, σ_3, σ_4, σ_5, σ_6 and σ_7 come from **Alice or Bob or Carol or David**

$\rightarrow$ Anonymous signatures

Linkable Signature (Liu et al., 2004)

Alice  (m_1, σ_1) (m_2, σ_2) (m_3, σ_3)	Bob  (m_4, σ_4)
Carol  (m_5, σ_5) (m_6, σ_6)	David  (m_7, σ_7)

Observer

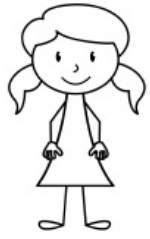
σ_1, σ_2 and σ_3 come from **the same user**

σ_5 and σ_6 come from **the same user**

No information about σ_4 and σ_7 signer

$\rightarrow$ Anonymous but Linkable

1-time Traceable Sig. (Canard et al., 2006)

Alice  (m_1, σ_1) (m_2, σ_2) (m_3, σ_3)	Bob  (m_4, σ_4)
Carol  (m_5, σ_5) (m_6, σ_6)	David  (m_7, σ_7)

Observer

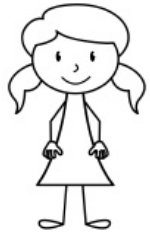
σ_1, σ_2 and σ_3 comes from **Alice**

σ_5 and σ_6 comes from **Carol**

σ_4 and σ_7 are **anonymous**

$\rightarrow$ Only 1 anonymous signature per group member

2-times Traceable Sig. (Au et al., 2006)

Alice  (m_1, σ_1) (m_2, σ_2) (m_3, σ_3)	Bob  (m_4, σ_4)
Carol  (m_5, σ_5) (m_6, σ_6)	David  (m_7, σ_7)

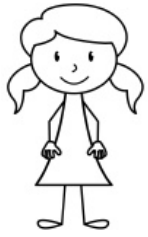
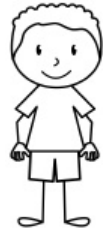
Observer

σ_1 and σ_3 comes from **Alice**

σ_2, σ_4, σ_5, σ_6 and σ_7 are **anonymous**

$\rightarrow$ Only 2 anonymous signature

2-times Traceable Sig. (Au et al., 2006)

Alice  (m_1, σ_1) $\boxed{(m_2, \sigma_2)}$ (m_3, σ_3)	Bob  (m_4, σ_4)
Carol  (m_5, σ_5) (m_6, σ_6)	David  (m_7, σ_7)

Observer

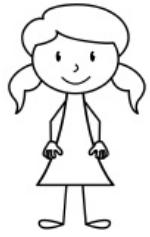
σ_1 and σ_3 comes from **Alice**

$\boxed{\sigma_2}$, σ_4, σ_5, σ_6 and σ_7 are **anonymous**

$\rightarrow$ Only 2 anonymous signature

$\boxed{\sigma_2 \text{ is anonymous} \rightarrow \text{not full traceable}}$

Our contribution: k-times Full Traceable Sig.

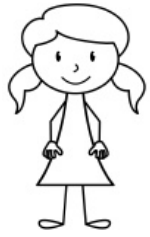
Alice  (m_1, σ_1) (m_2, σ_2) (m_3, σ_3)	Bob  (m_4, σ_4)
Carol  (m_5, σ_5) (m_6, σ_6)	David  (m_7, σ_7)

Observer

σ_1, σ_2 and σ_3 comes from **Alice**

σ_4, σ_5, σ_6 and σ_7 are **anonymous**

Our contribution: k-times Full Traceable Sig.

Alice  (m_1, σ_1) (m_2, σ_2) (m_3, σ_3)	Bob  (m_4, σ_4)
Carol  (m_5, σ_5) (m_6, σ_6)	David  (m_7, σ_7)

Observer

σ_1, σ_2 and σ_3 comes from **Alice**

σ_4, σ_5, σ_6 and σ_7 are **anonymous**

$\rightarrow$ k anonymous signature per users

$\rightarrow$ Trace all cheater's signatures

Our contributions

k-times Full Traceable Signature

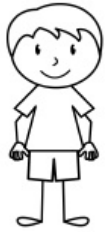
- Generalize traceable signatures
- Ring signature (ad-hoc group)
- Event oriented
- Fine-grained k
- Anonymous (less than k)
- Full public linkability (more than k)
- Full public traceability (more than k)

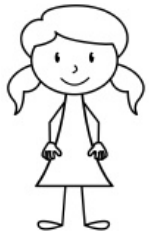
Applications:

1. proxy voting
2. k-times veto

Application in k-times Veto for CARS'16


Alice


Bob


Carol


David

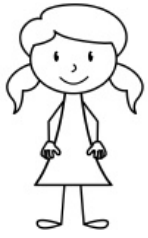
Conference on Anonymous Ring Signatures

- **List of *candidates*** for the Program Commitee (PC): Albert, Bernard, Cedric, Donald, Edward, Fabien, Gaston, Hercul, Ivan, Jim, Karl
- Each member of Steering Commitee (SC) can **exclude** *k* **names** of the list
- Vetos are **anonymous**
- Members who exceed this limitation are **excluded** and their vetos are discarded

Application: k-times Veto

PC= Albert, Bernard, Cedric, Donald, Edward, Fabien, Gaston, Hercul, Ivan, Jim, Karl

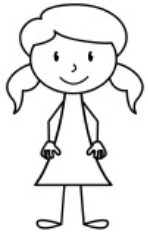
Veto using 2-times traceable signature:

Alice  (Donald, σ(Donald)) (Jim, σ(Jim)) (Edward, σ(Edward))	Bob  (Edward, σ(Edward))
Carol  (Albert, σ(*Albert*)) (Gaston, σ(Gaston))	David  (Gaston, σ(Gaston))

Application: k-times Veto

PC= Albert, Bernard, Cedric, Donald, Edward, Fabien, Gaston, Hercul, Ivan, Jim, Karl

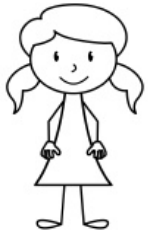
Veto using 2-times traceable signature:

~~Alice~~  ~~(Donald, σ(Donald))~~ (Jim, σ(Jim)) ~~(Edward, σ(Edward))~~	Bob  (Edward, σ(Edward))
Carol  (Albert, σ(*Albert*)) (Gaston, σ(Gaston))	David  (Gaston, σ(Gaston))

Application: k-times Veto

PC= Albert, Bernard, Cedric, Donald, Edward, Fabien, Gaston, Hercul, Ivan, Jim, Karl

Veto using 2-times full traceable signature:

~~Alice~~  ~~(Donald, σ(Donald))~~ ~~(Jim, σ(Jim))~~ ~~(Edward, σ(Edward))~~	Bob  (Edward, σ(Edward))
Carol  (Albert, σ(*Albert*)) (Gaston, σ(Gaston))	David  (Gaston, σ(Gaston))

Outline

IOT and Security : Distance Bounding

Secure Matrix Multiplication with MapReduce

Ktimes Traceable Ring Signatures

Challenges

Security and IOT

LIMOS
LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

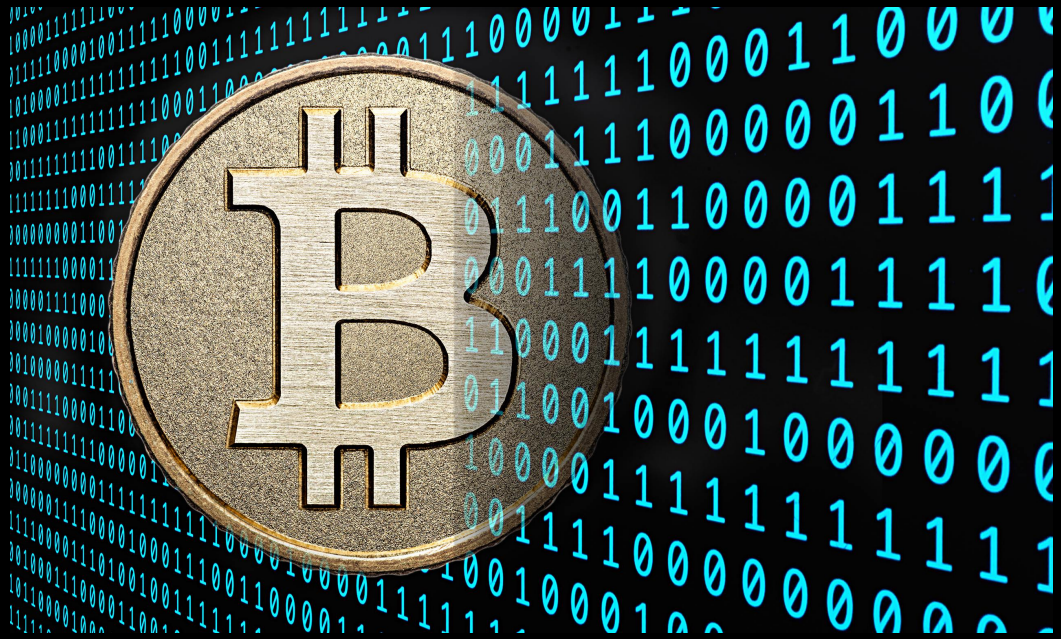
Security

LIMOS
LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

RGPD

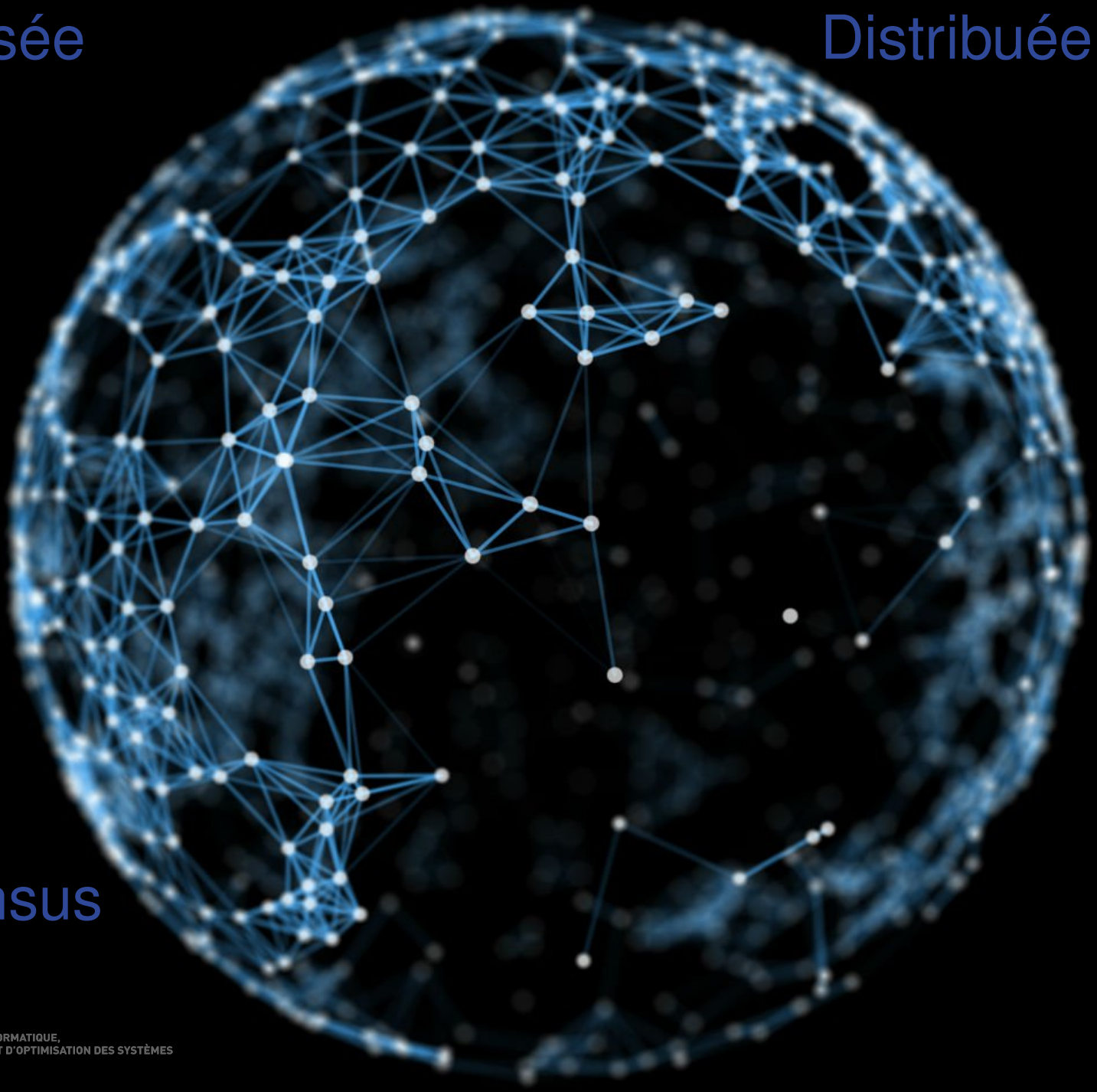
LIMOS
LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

La révolution Bitcoin 2009



Décentralisée

Distribuée

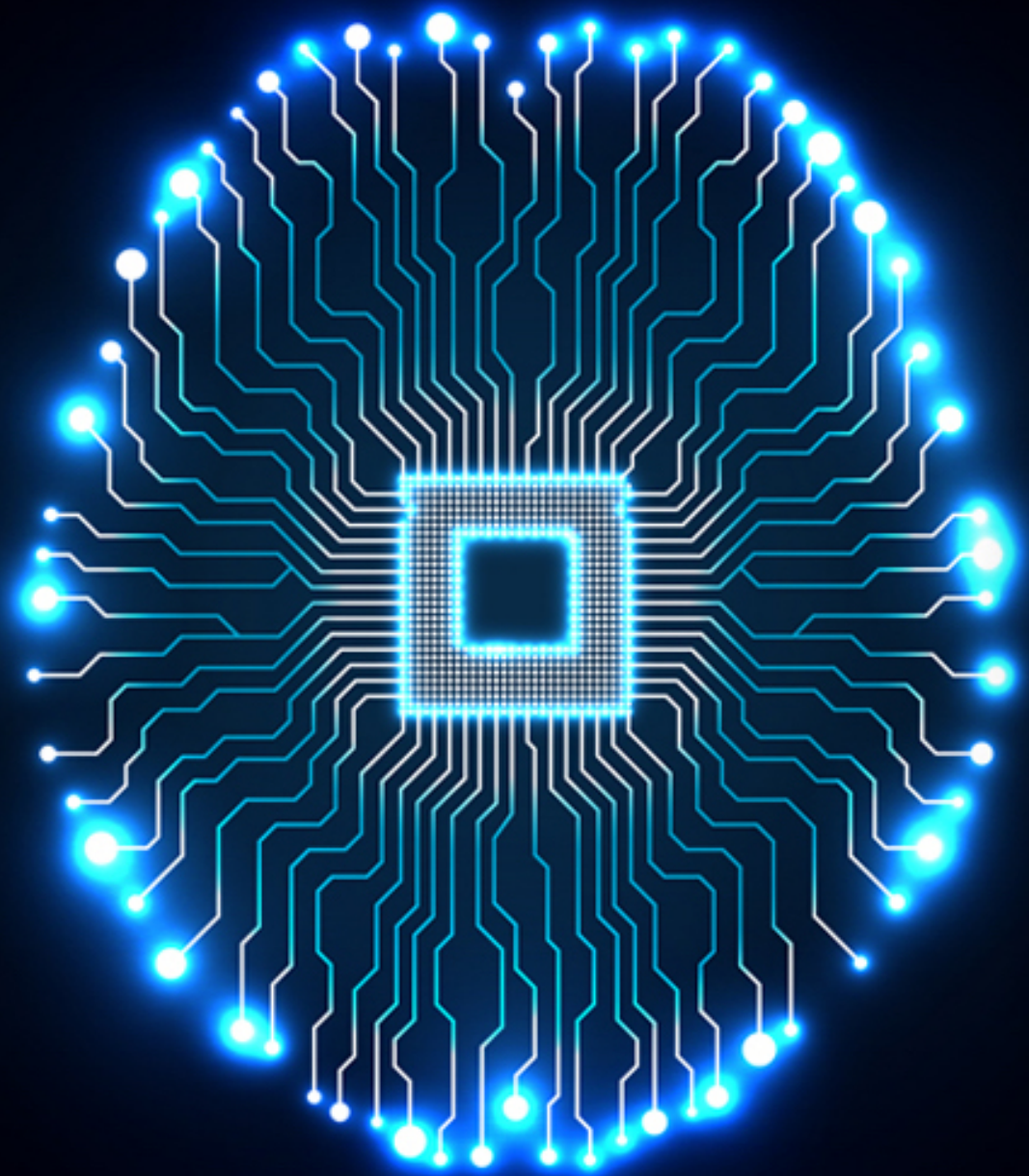


Consensus

LIMOS

LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

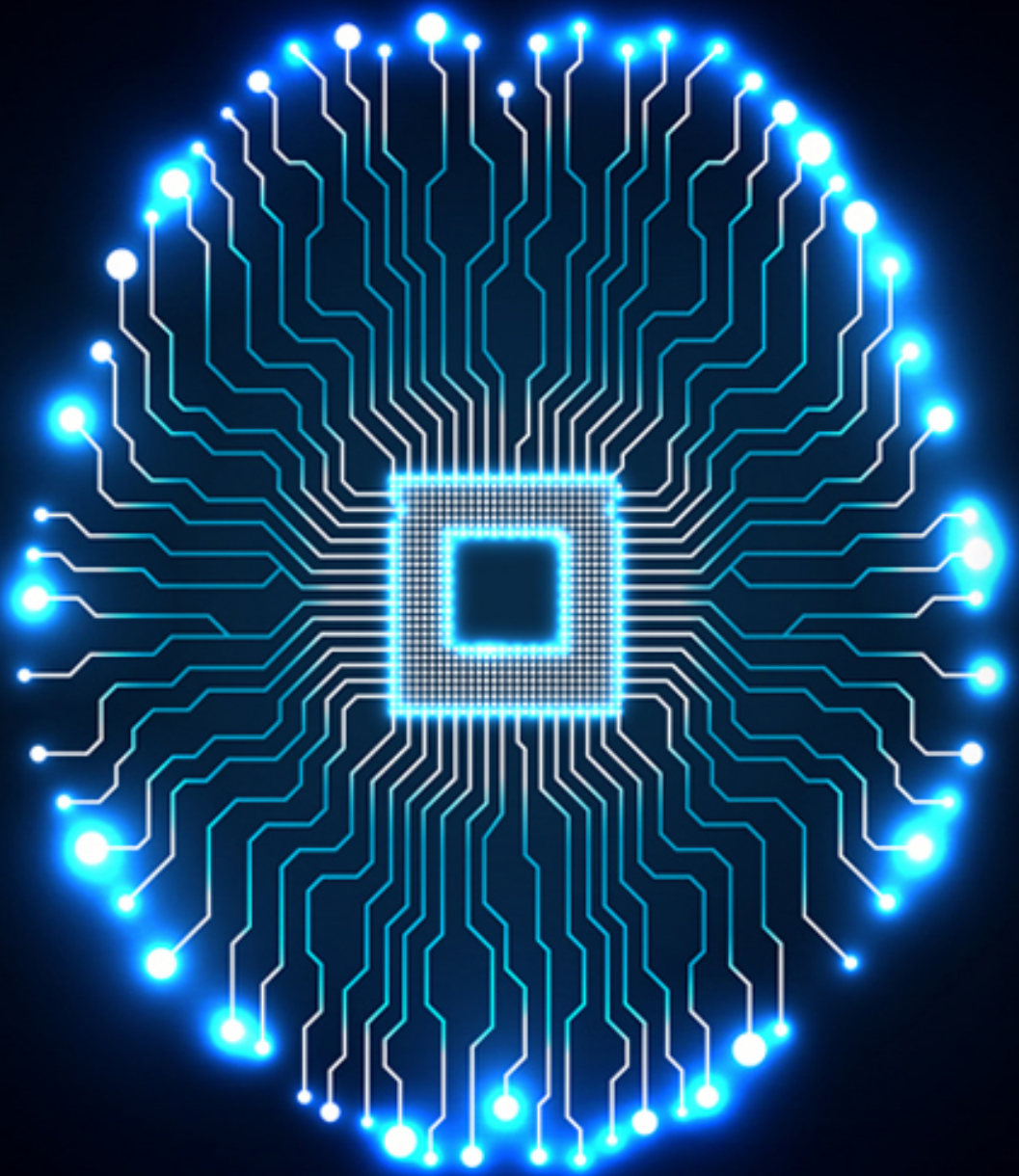
AI & Security



LIMOS

LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

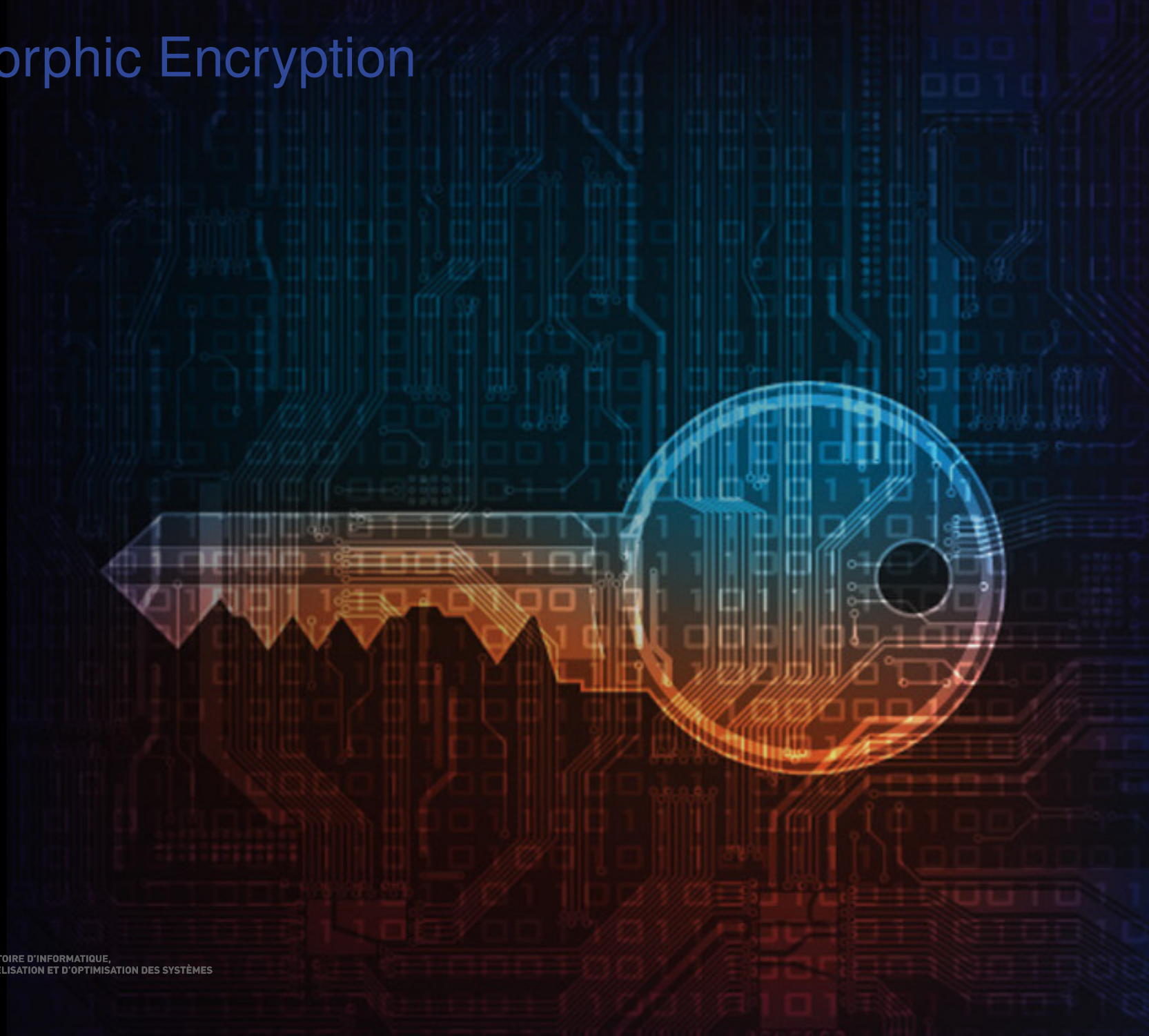
AI & Security



LIMOS

LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Homomorphic Encryption



LIMOS
LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

New Functionalities & Properties

LIMOS
LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Mass Surveillance

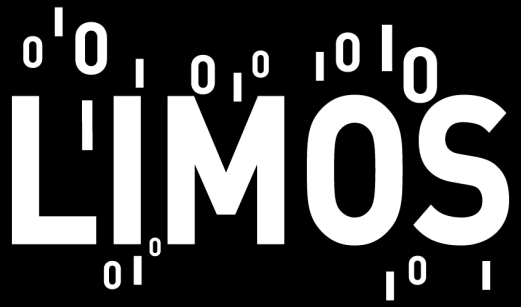
LIMOS
LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Conclusion

DEMOS:

- How to sign and encrypt your emails
- Matrix Multiplication
- Symmetric Searchable Encryption

Thank you for your attention!



Questions?

pascal.lafourcade@uca.fr