A Distributed Certification System for Structured P2P Networks

François Lesueur, Ludovic Mé, Valérie Viet Triem Tong
firstname.lastname@supelec.fr

Supélec, SSIR Group (EA 4039)

AIMS, July 2008
Bremen, Germany

Main Line of Our Work

Aim

Guarantee Confidentiality, Integrity and Availability in P2P

Specificities of P2P Networks

Dynamic and *Collaborative* networks without *Central Authority*

Approach

1. Admission Control to the Network
2. Security Protocols tolerating a bounded number of attackers

Enforcing Security Properties

Traditional View

- Security is enforced by a central point
- Some *capacities* are proved by certificates issued by CA

Our Proposition: Distributed Certification

- Some capacities are still proved by certificates
- These certificates are signed collaboratively by members

$\Rightarrow$ *Trust that t% of the nodes would not collude*

Applications

Admission Control [COPS '08]

Sybil protection, only genuine members are certified

Misbehaving Nodes Exclusion [I2CS '08]

Nodes are monitored, misbehaviors are detected and excluded

Secure Naming of Resources

- Users in a P2P SIP application obtain unique and provable intelligible names (not $h(P)$)
- P2P DNS system

Outline

Distributed Certification

Certification by a fixed ratio of members

Certification

Access rights, name ownership, . . . materialized by a certificate:

- Contains the public key of the node
- Signed by a unique network secret key S

Certificate generation

Certificates are generated by a fixed ratio of members:

- Fair distribution of the authority
- However, network size is unknown

Fixed Number

[Kong *et al.*, 01]

Certificate generated by a fixed number of peers

[Desmedt, 97], [Rabin, 98]

Generic papers : sign data through the cooperation of t entities among n, t and n fixed at initialization

Mainly suits MANETs

Fixed Ratio with a Server

[Saxena *et al.*, 03]

Certificate generated by a fixed ratio of the peers, but uses a central counter of the network size.

[Frankel *et al.*, 97]

Modification of t and n on the fly:

1. $(t, n) \rightarrow (t, t)$ *(Poly-to-Sum)*
2. $(t, t) \rightarrow (t', n')$ *(Sum-to-Poly)*

Possible corruption if one attacker among the t
How to know the size of the network without a central point ?

Our Proposition: Fixed Ratio without Server

Certification

Certificate generated by a fixed ratio of the peers, without central counter.

Adaptive threshold cryptography

Modification of t and n on the fly to maintain the ratio but without knowing the network size.

Cryptographic Material

Principle

- Network is characterized by a key pair (S, P)
- P is publicly known
- S is shared among the nodes
- Signing a message requires the cooperation of t% of the nodes
- **No node knows S at any moment**

RSA is a homomorphic function

First level sharing

Let $S = (e, m)$ be the network secret key
Let e_0, e_1 be as $e = e_0 + e_1$ (arithmetic $+$)
Then $d^e[m] = d^{e_0+e_1}[m] = (d^{e_0} \times d^{e_1})[m]$

Example

$(e, m) = (19, 187)$
$e_0 = 8, e_1 = 11$ such as $19 = 8 + 11$
$d = 18$
Then $18^{19}[187] = (18^8 \times 18^{11})[187] = 52$

$\Rightarrow$ Shares e_i are distributed in *sharing groups* and this operation is recursively iterated when the network grows

Fixing the Threshold Ratio

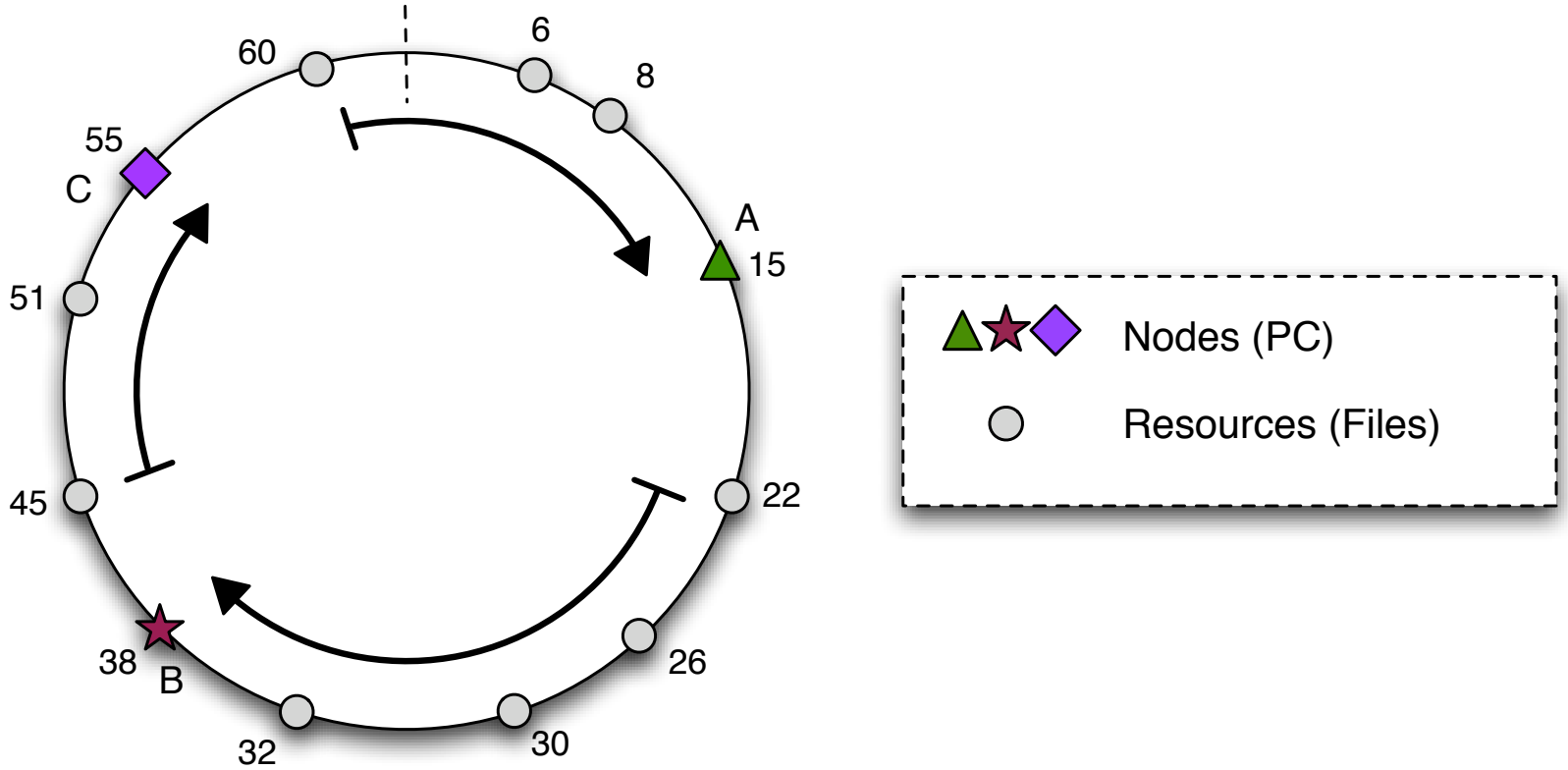
Now that we can locally split a share...

- t is the ratio of nodes needed to sign a certificate
- g_{min} (resp. g_{max}) is the minimal (resp. maximal) size of a sharing group
- $\frac{1}{g_{max}} < t < \frac{1}{g_{min}}$

Remark

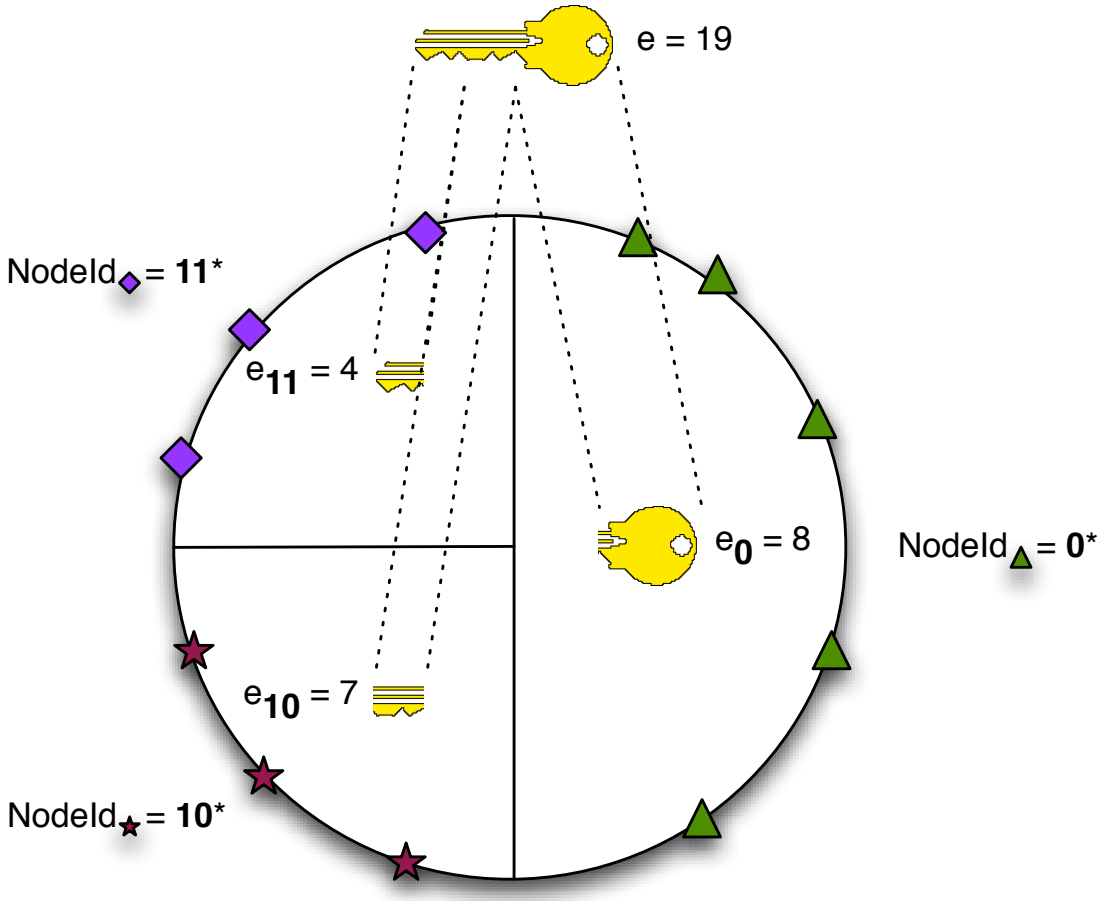
Network size is not needed to enforce t, only local knowledge !

Structured P2P Networks

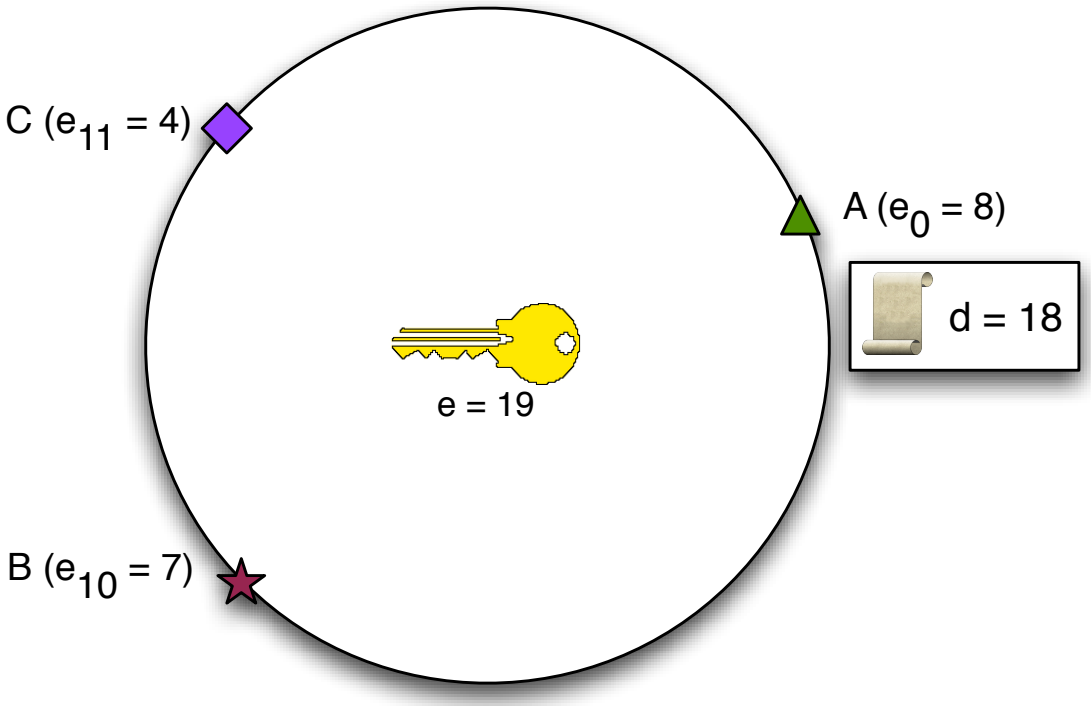


DHT : $key \mapsto value$

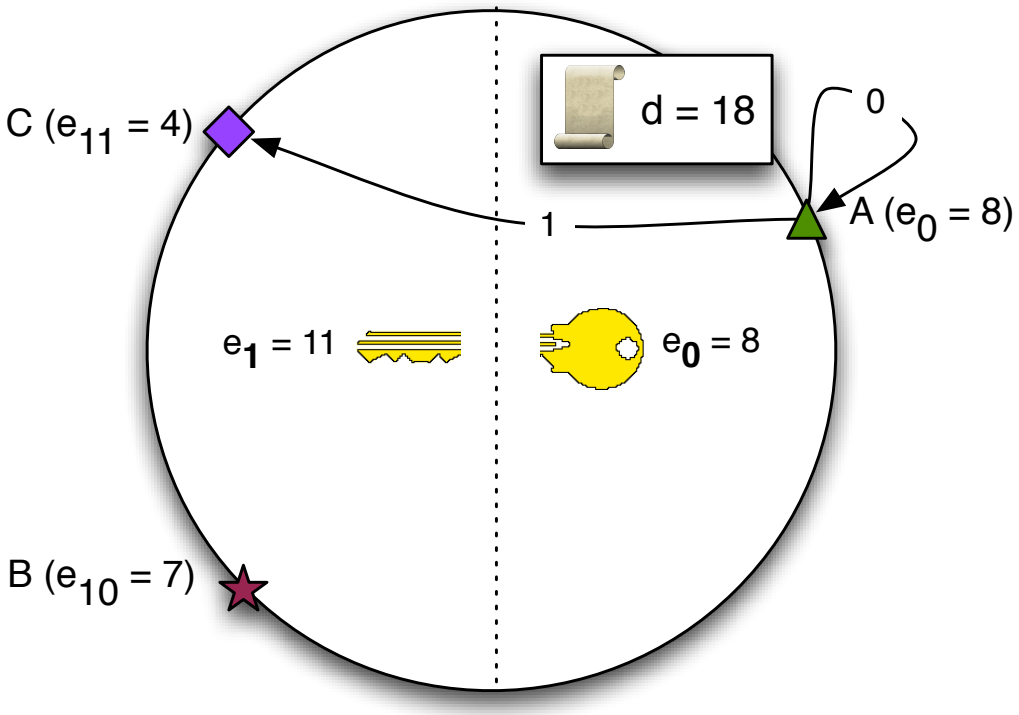
Network Secret Key Sharing



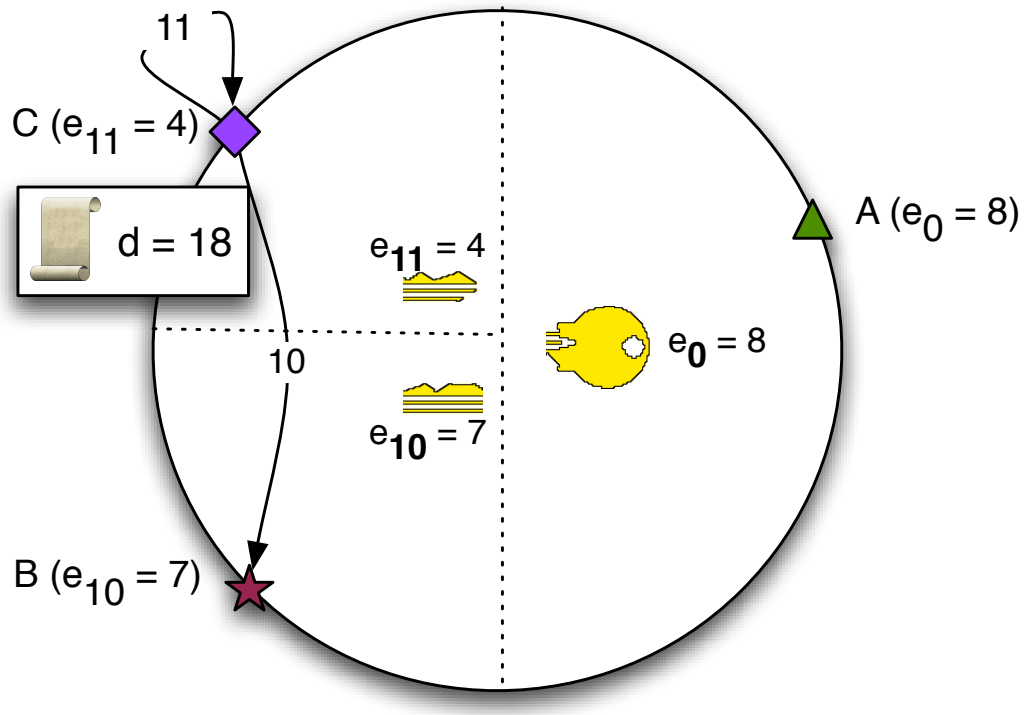
Distributed Certification



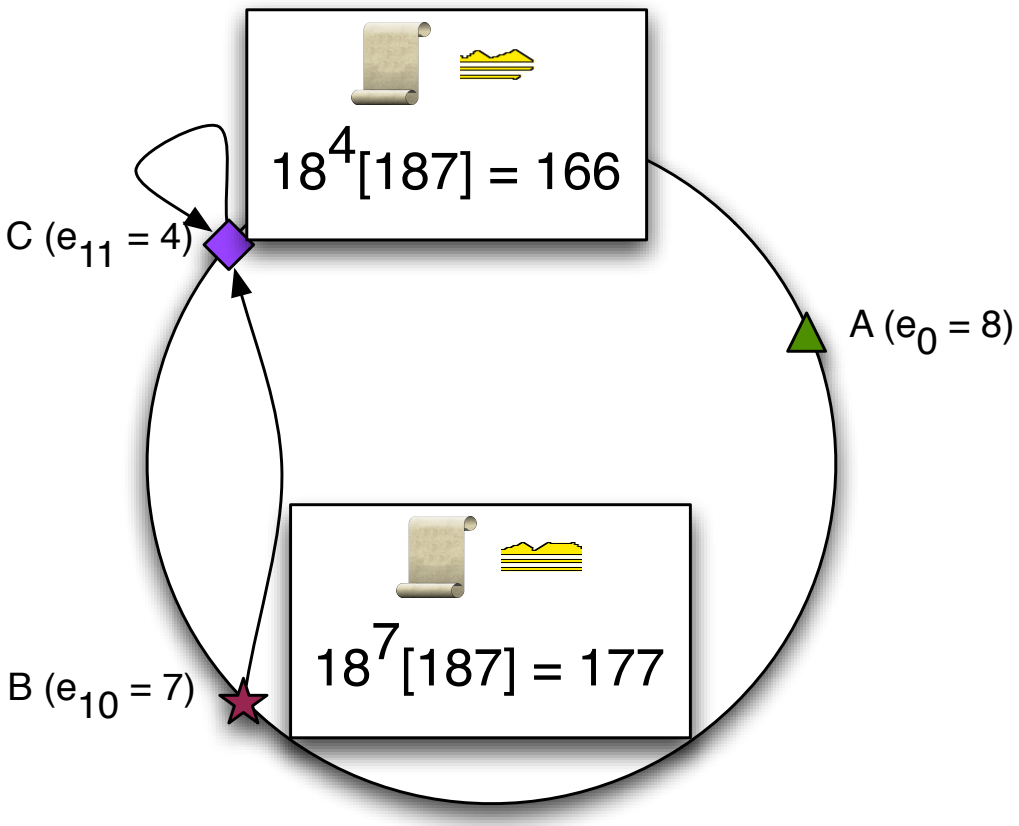
Distributed Certification



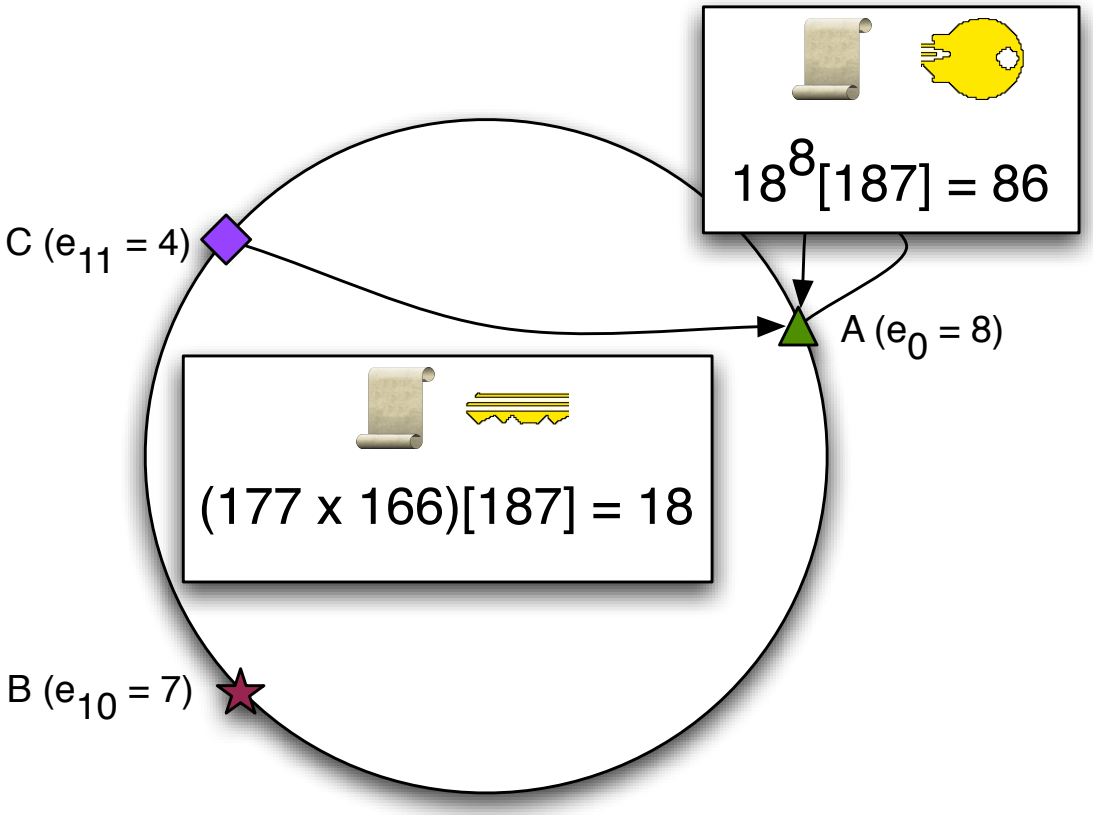
Distributed Certification



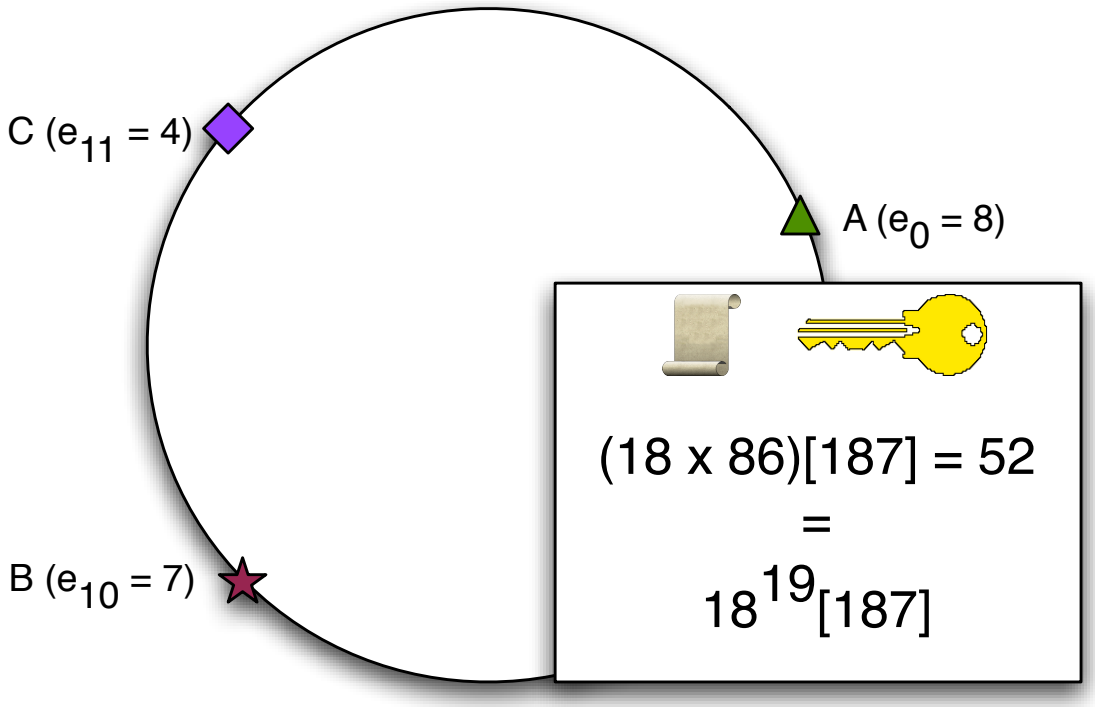
Distributed Certification



Distributed Certification



Distributed Certification



Tolerating Misbehving Nodes

Misbehaving nodes problem

A misbehaving node can:

- Fake the partial signature with his share
- Fake an intermediate multiplication

$\Rightarrow$ Only detected by the initiator node, with P

Solution

- Ask each partial signature to several nodes
- Exclude such nodes !

Maintenance

Maintenance Operations

Verified invariant

1. The sum of shares is the network secret key
2. Each node knows all the members of his sharing group

Three main operations

- Split
- Merge
- Refresh

Splitting a share

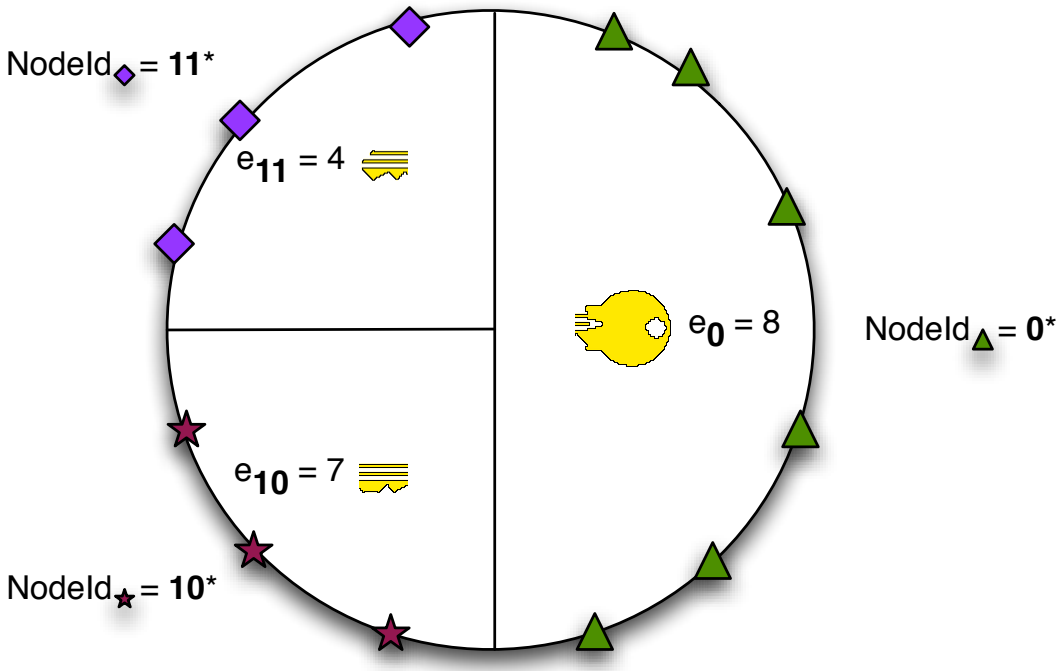
Principle

Splitting a share into two parts when a groups is composed of more than g_{max} members

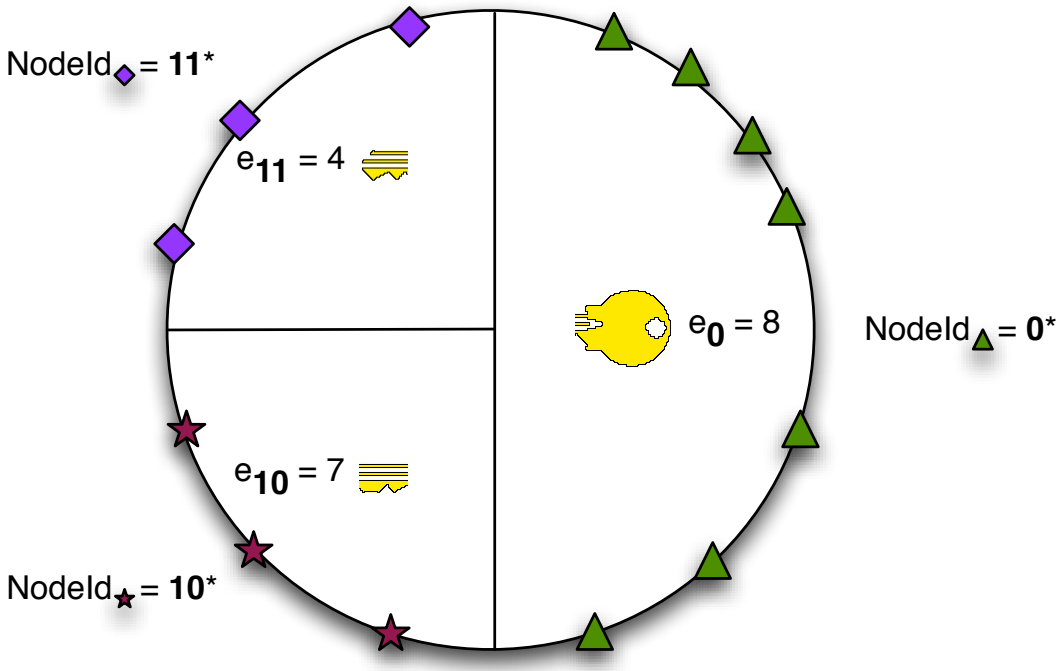
Mechanism

1. Agreement on the value of the new shares ($e_x = e_{x0} + e_{x1}$)
2. Each node migrates to one of the groups
3. Shares are refreshed

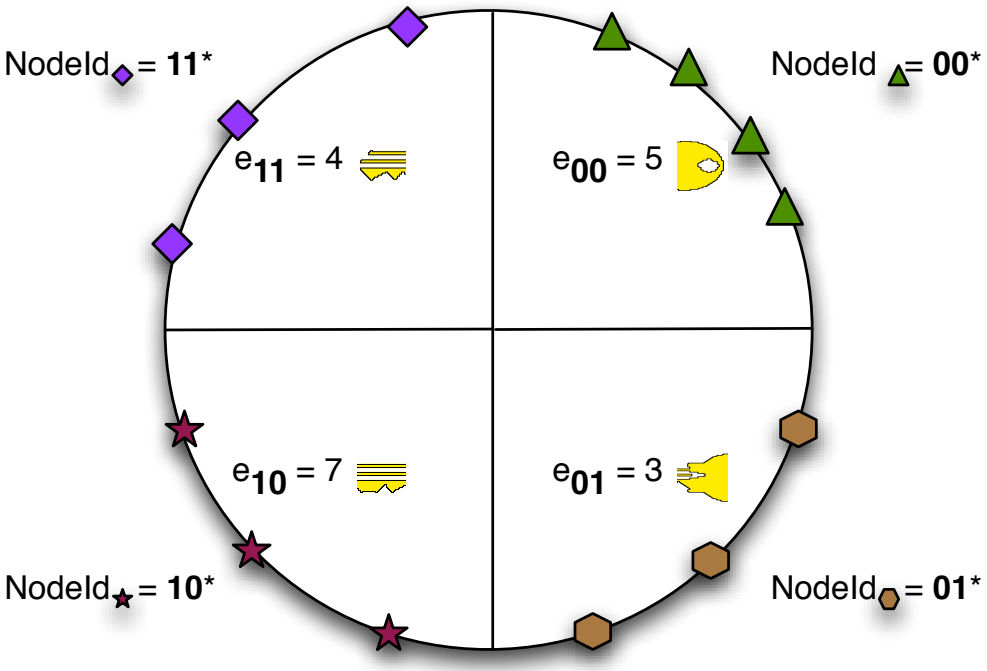
Splitting a share



Splitting a share



Splitting a share

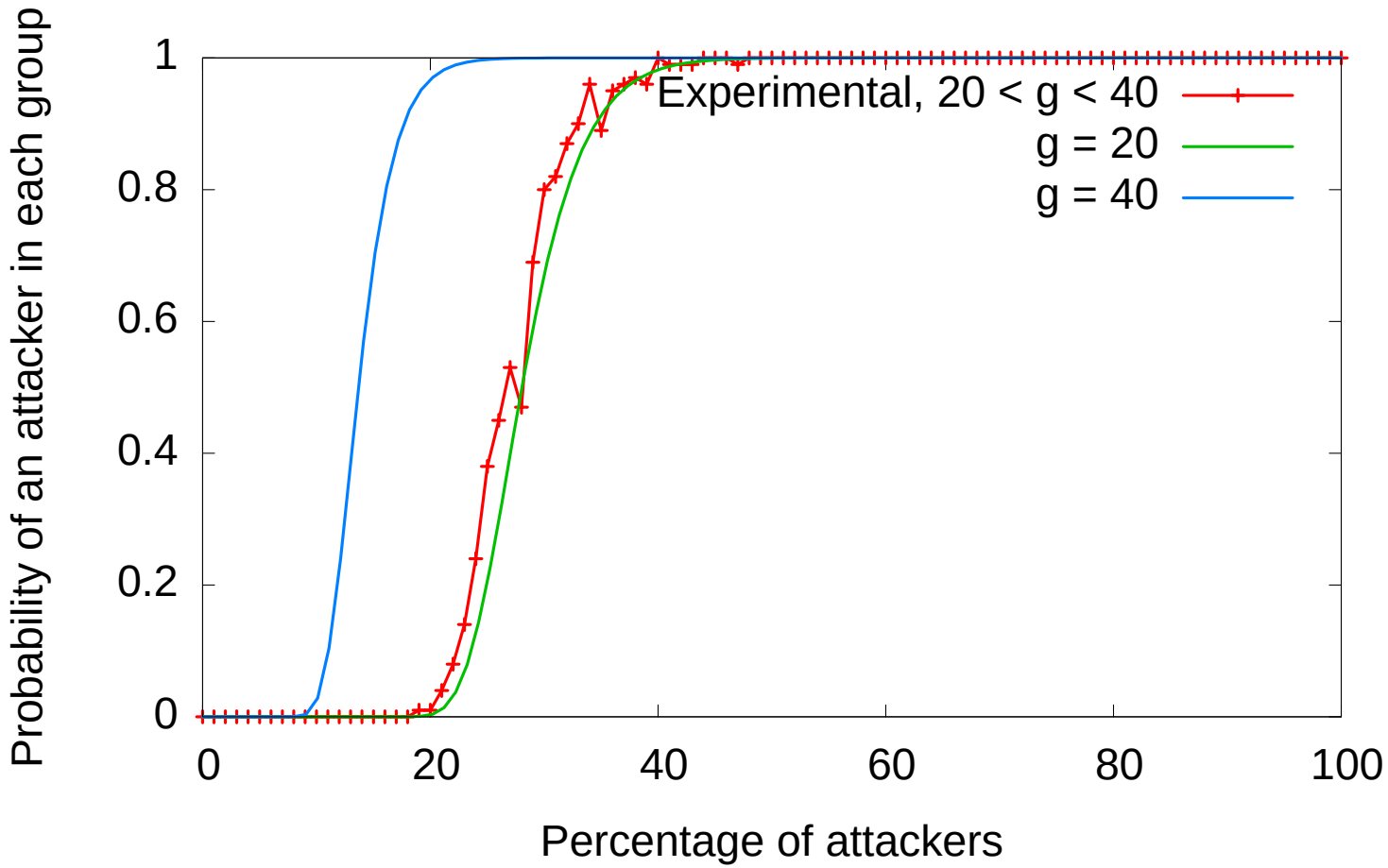


Analysis and Results

How to obtain a fake certificate ?

- Convince $t\%$ of the members
- Insert into each group $\Rightarrow$ Sybil attack
- Collude with many other attackers

Probability for colluding attackers to obtain every share

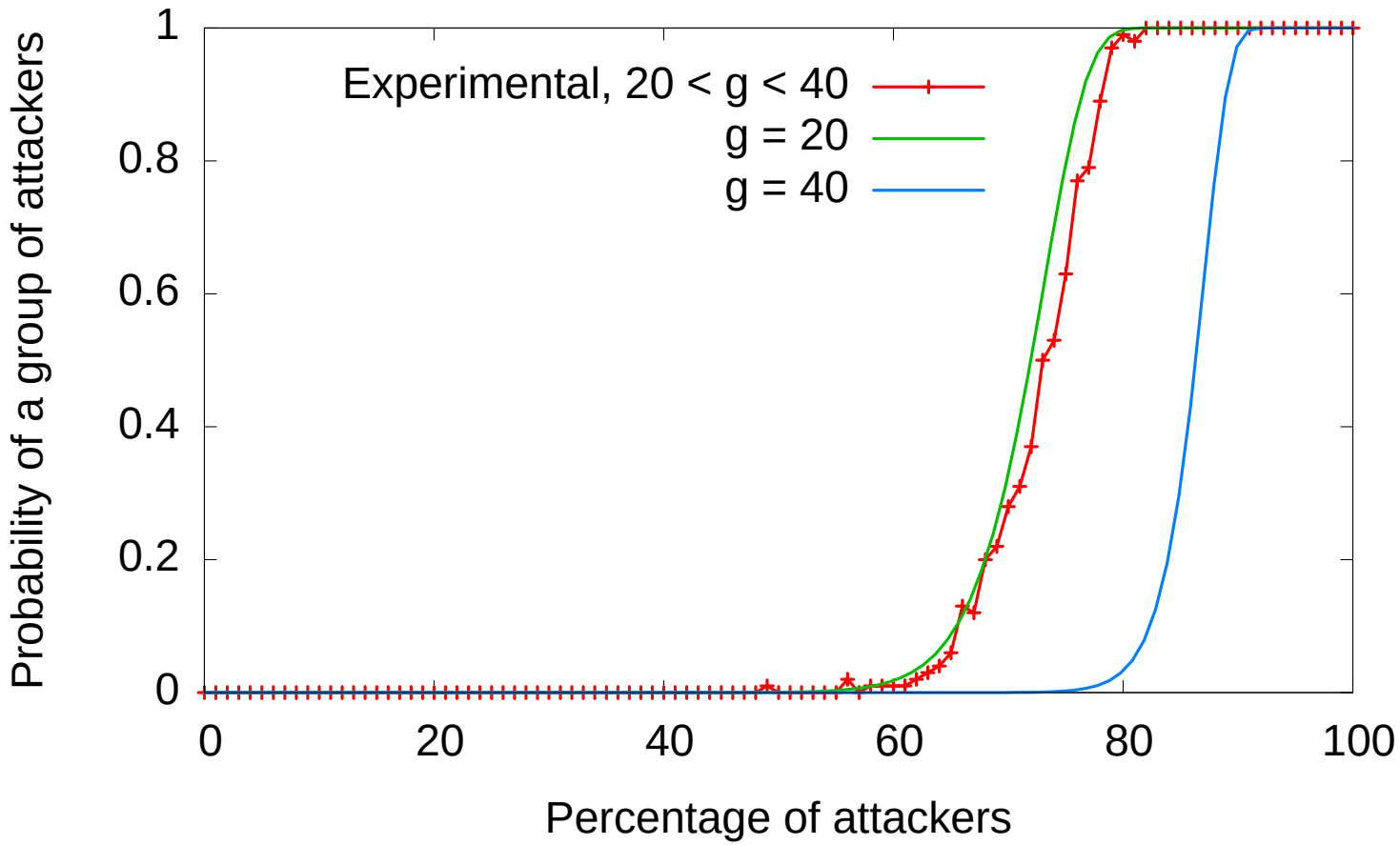


$10,000$ nodes, $2.5\% < t < 5\%$

How to attack an honest certification ?

- Intercept the request
- Own each node in any sharing group $\Rightarrow$ Sybil attack
- Collude with many other attackers

Probability for colluding attackers to control a sharing group



$10,000$ nodes, $2.5\% < t < 5\%$

Distributed Certification

Provided Service

- Cryptographic proof of agreement of a fixed ratio of the nodes
- Resistant to some inside attackers

Applications

- Protecting from Sybil Attack
- Excluding attackers
- Securely naming resources

A Distributed Certification System for Structured P2P Networks

François Lesueur, Ludovic Mé, Valérie Viet Triem Tong
firstname.lastname@supelec.fr

Supélec, SSIR Group (EA 4039)

AIMS, July 2008
Bremen, Germany