

Threshold Ring Signatures and Applications to Ad-hoc Groups

Emmanuel Bresson (ÉNS, France)
Jacques Stern (ÉNS, France)
Michael Szydlo (RSA Labs, USA)

1

Crypto '02 -- Santa Barbara, CA, USA -- August 18-22, 2002

Outline

- Introduction
- Improved scheme [RST01]
 - ◆ Simplified proof
- Ad-hoc / threshold ring signatures
 - ◆ Formalization
- New scheme
 - ◆ Description of a threshold scheme
 - ◆ Provable security
- Conclusion

2

Crypto '02 -- Santa Barbara, CA, USA -- August 18-22, 2002

Motivation

- Anonymity is frequently required
 - ◆ Electronic voting, e-cash applications
 - ◆ Group signatures/authentication
 - ◆ Medical, private data processing
- Ad-hoc groups are a specific target
 - ◆ Temporary membership scenarios
 - ◆ Grow-up of wireless lan applications
- Both concepts are worthy being combined

Related work

- Group signatures (appears in [CvH91])
 - ◆ Definition of group anonymity
 - ◆ Improved schemes in [CS97, ACJT00]
- Anonymity designing methods
 - ◆ Proving anonymous « OR » statements [CDS94]
- Rivest, Shamir, Tauman [RST01]
 - ◆ Formalization of ring signatures
 - ◆ Secure scheme in the ideal-cipher model

Definitions

- **Group signatures**
 - ◆ A group of members is predefined and members sign on behalf of the group
- **Ring signatures**
 - ◆ A user specifies an arbitrary set which he belongs to and then signs on behalf of this group
- **Threshold signatures**
 - ◆ The secret key is shared and a minimal number of servers is required to sign

Our contributions

- **Improved security proof**
 - ◆ We simplify the security proof provided in [RST01] and additionally prove security relative to weaker assumptions
- **Ad-hoc group formalization**
 - ◆ We generalize ring signatures by defining ad-hoc groups together with a security model
- **Threshold ring signatures**
 - ◆ We propose a new scheme combining ring anonymity and threshold features

The basic construction

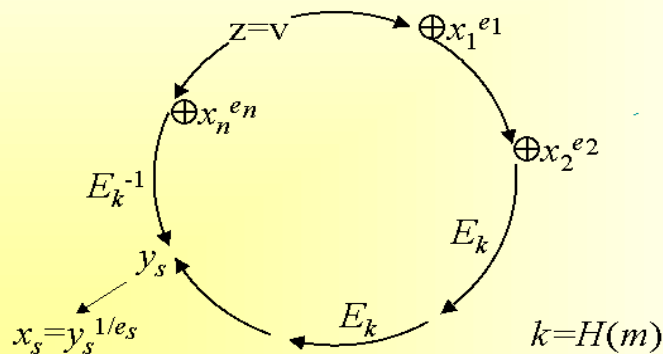
- Basic scheme for ring signatures
 - ◆ How to prove that 1 out of n users actually signed
- Combining functions
 - ◆ One needs a function C that, when given n values y_1, \dots, y_n , can output a single one, such that:
 - ◆ For any s , any fixed $y_{i \neq s}$, $y_s \rightarrow C(y_i)$ is one-to-one and efficiently computable
- Ring signature scheme
 - ◆ Choose all $y_{i \neq s}$ as $f(x_i)$, compute y_s s.t. $C(y_i) = 0$
 - ◆ Use a trapdoor one-way permutation $x_s = f^{-1}(y_s)$

7

Crypto '02 -- Santa Barbara, CA, USA -- August 18-22, 2002

Ring signatures based on RSA

- Combining functions
 - ◆ Combine RSA permutations through « encrypt-and-xor » mechanism:



Signature:

$$\sigma = (v, x_1, \dots, x_n)$$

Verification:

$$C(x_i^{e_i}) = ? 0$$

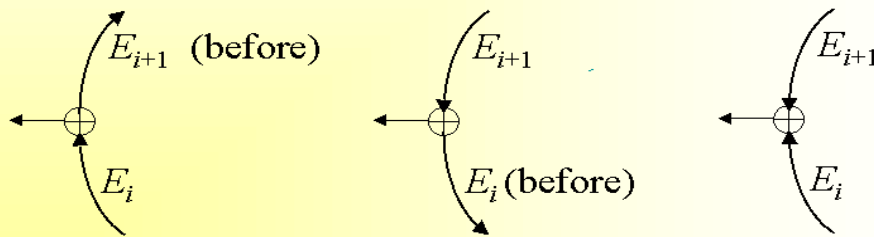
8

Crypto '02 -- Santa Barbara, CA, USA -- August 18-22, 2002

Security: the « ring lemma »

■ The lemma

- ◆ In a forgery, there must be an index i along the ring such that ...



Security: the proof

■ Reduction to the RSA inversion problem

- ◆ Given n , y and e , compute $x = y^{1/e} \pmod n$

■ Security proof for [RST01]

- ◆ Guess the index and the two related queries
- ◆ Slip a challenge RSA value
- ◆ Use the forgery to get the e -th root

■ Computational model

- ◆ The encryption function is an ideal oracle

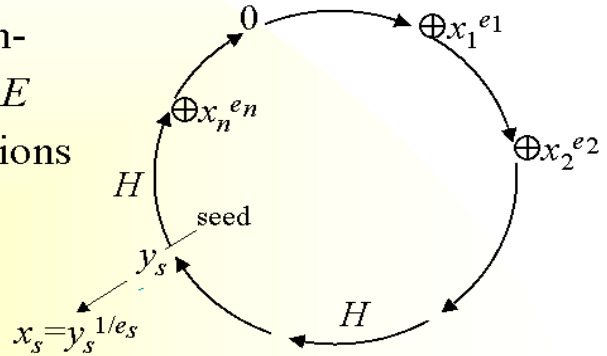
Improved proof

■ Simplified scheme

- ◆ One does not need the symmetric encryption scheme E to combine RSA permutations
- ◆ Just hash-and-xor ring

■ Weaker assumptions

- ◆ Using Random Oracles instead of Ideal-Ciphers
- ◆ Same security bound



Ad-hoc groups

■ Ad-hoc networks

- ◆ Intensively used through mobile devices
- ◆ Dynamic structure
- ◆ Involve « ad-hoc groups » (without registration or authority)

■ Ad-hoc groups

- ◆ List of users, with certified public keys
- ◆ An arbitrary monotone access structure (list of *acceptable* subsets)

Ad-hoc ring signatures

■ Definitions

- ◆ Σ -sign algorithm: an acceptable subset of users generates a signature on a message m
- ◆ Σ -verification algorithm: outputs 1 or 0 depending on the validity.

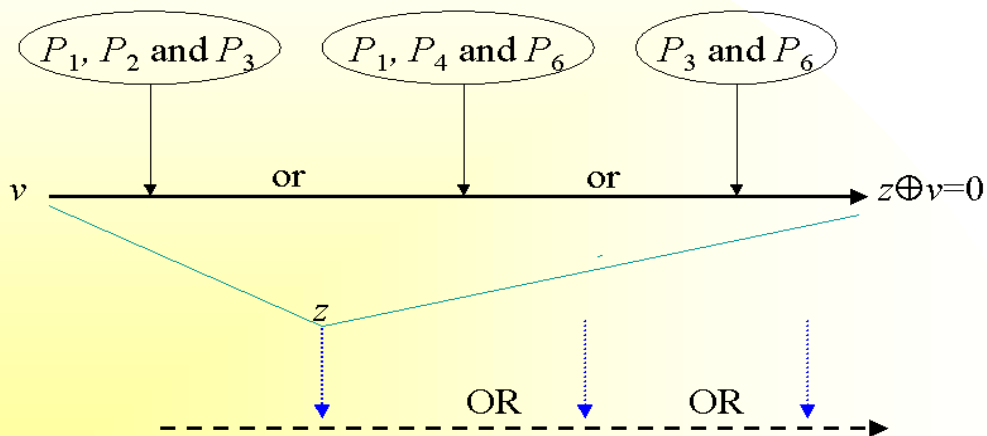
■ Threshold ring signature

- ◆ Σ is just a threshold access structure over the ring

13

Crypto '02 -- Santa Barbara, CA, USA -- August 18-22, 2002

Ad-hoc groups: combinations



14

Crypto '02 -- Santa Barbara, CA, USA -- August 18-22, 2002

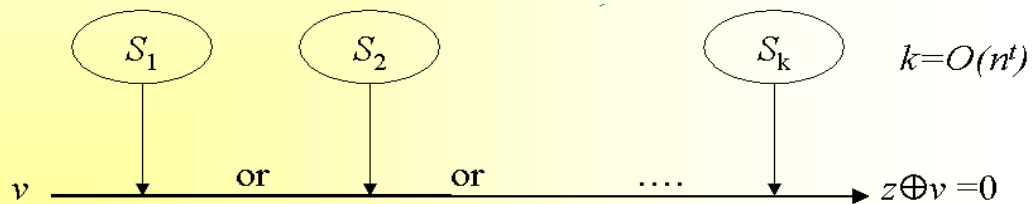
Threshold ring signatures

■ Definitions

- ◆ At least t out of the n ring members cooperatively produced the signature

■ Naive way

- ◆ List all the subsets of cardinality t : inefficient



15

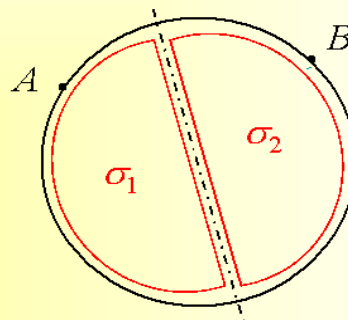
Crypto '02 -- Santa Barbara, CA, USA -- August 18-22, 2002

An efficient scheme

■ Introduction: case $t=2$

- ◆ To prove that 2 signers A and B have cooperated, each of them solves a part of the ring

Split the ring R into R_1, R_2 , in such a way that $A \in R_1$ and $B \in R_2$



$$\sigma = (\sigma_1, \sigma_2)$$

16

Crypto '02 -- Santa Barbara, CA, USA -- August 18-22, 2002

Fair partitions of a ring

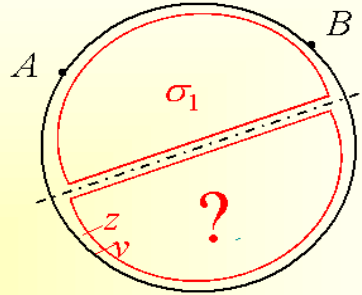
- Preserve anonymity
 - ◆ A single split reveals partial information (namely $A \in R_1$ and $B \in R_2$)
 - ◆ Anonymity is « restored » by providing many splits
- Combinatorics [AYZ95]
 - ◆ There exists a family of $2^t \log n$ splits such that for any subset I of cardinality t , there exists a partition π :
$$\#(R_j \cap I) = 1 \text{ for all subrings } R_j$$

Our new scheme (1)

- General idea
 - ◆ To prove that t signers cooperate, choose a fair partition π for this set of signers
 - ◆ Compute t sub-ring-signatures (since each sub ring contains one signer)
 - ◆ Embed these signatures among the collection of signatures on the « unfair » partitions to ensure anonymity
 - ◆ Prove that at least one partition has been correctly solved (meta-ring mechanism)
 - Needs to simulate sub-rings for « unfair » partitions !

How to simulate a ring ?

- For an « unfair » partition, at least one sub-ring cannot be solved (we do not have enough private keys)



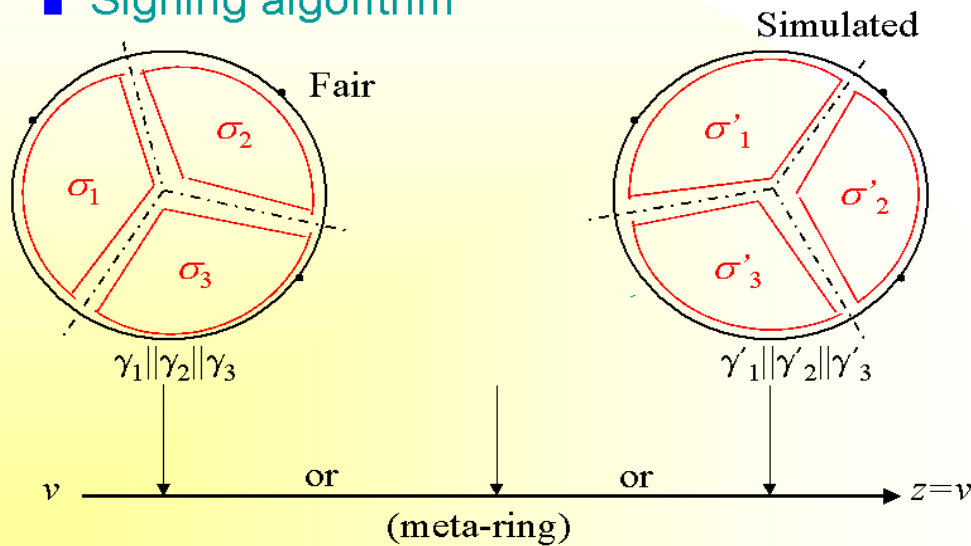
- Free the gap values
 - ◆ The gap $\gamma = z \oplus v$ is not fixed in advance
 - ◆ Simulation becomes easy

19

Crypto '02 -- Santa Barbara, CA, USA -- August 18-22, 2002

Our new scheme (2)

- Signing algorithm

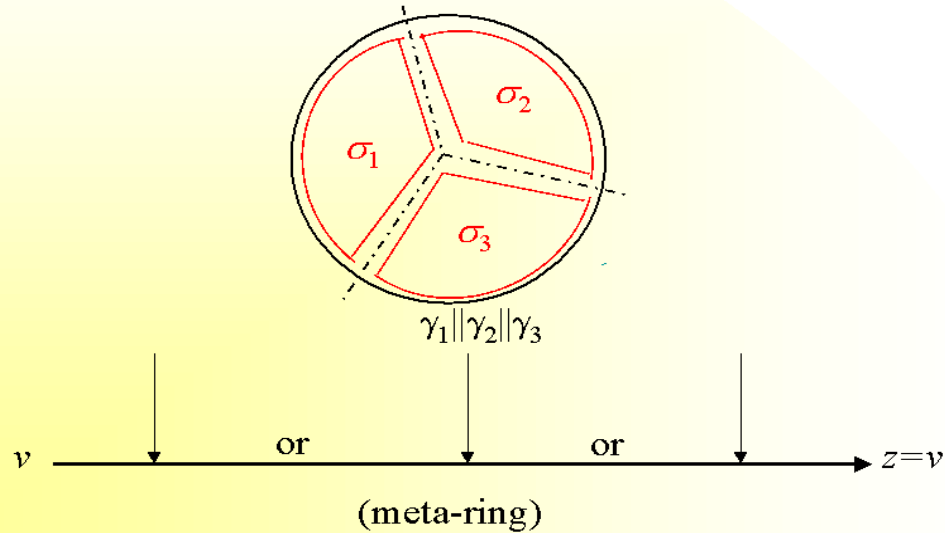


20

Crypto '02 -- Santa Barbara, CA, USA -- August 18-22, 2002

Our new scheme (3)

- Verification algorithm



21

Crypto '02 -- Santa Barbara, CA, USA -- August 18-22, 2002

Security result

- Security theorem

- ◆ The scheme is secure under the RSA assumption, in the random oracle model.
- ◆ The scheme ensures perfect anonymity

22

Crypto '02 -- Santa Barbara, CA, USA -- August 18-22, 2002

Conclusions

■ Contributions

- ◆ Simplified scheme for basic ring signatures
- ◆ Extension to ad-hoc and threshold structures
- ◆ New, provably secure scheme

■ Future work

- ◆ Improve reduction
- ◆ Improve the model (standard model)