RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **CRYP-R07**

Post-Quantum Crypto: Traceable Ring Signatures with Post-quantum Security

Hanwen Feng ; Jianwei Liu; Qianhong Wu; Ya-Nan Li

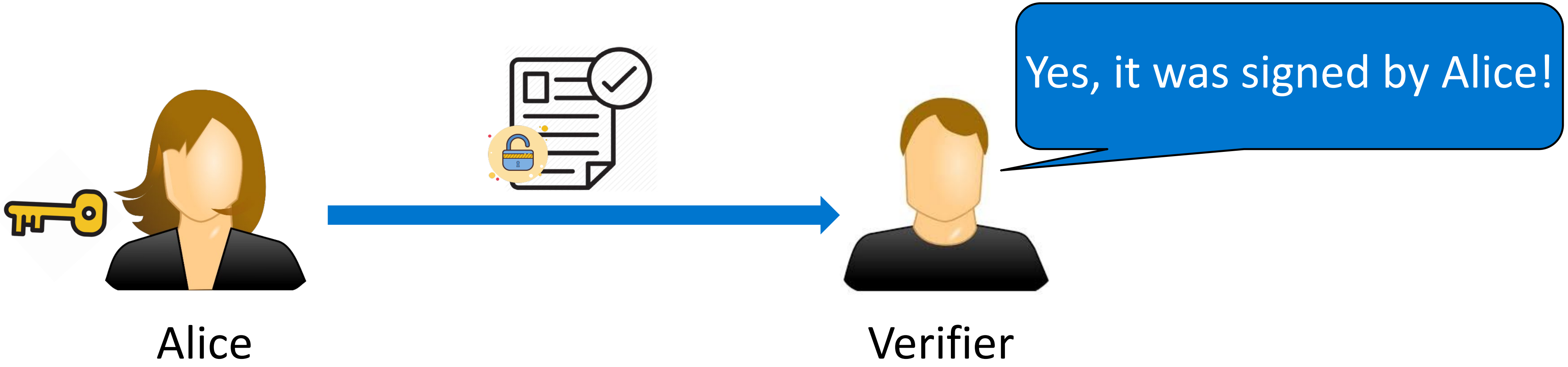
PhD. Candidate
School of Cyber Science and Technology, Beihang University
Email: feng_hanwen@buaa.edu.cn

RSAConference2020

Background and Motivations

Background: Digital Signatures

Alice can use her secret key to sign any message



Yes, it was signed by Alice!

Alice

Verifier

Correctness: Anyone can verify that the message was signed by Alice

Security: Anyone without Alice’s secret key cannot forge a valid signature

Privacy Concern: Digital signature cannot provide privacy protection for signers.

Background: Privacy Demands from Real-World

- A ballot should not reveal the identity of the voter

E-voting

- Transactions should not be traced

E-cash

- The message should not reveal the identity of the TPM

Trusted Platform Module

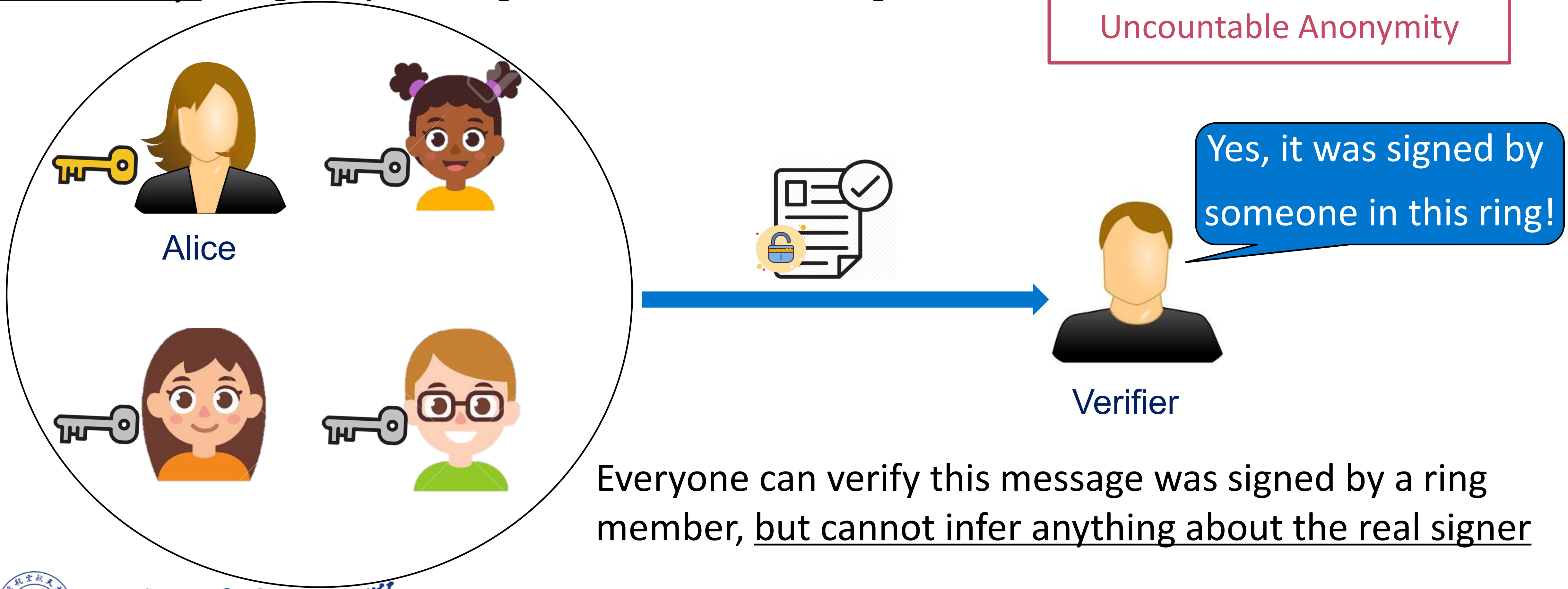
Vehicle Network

- A broadcast message should not reveal the speed or position of a vehicle

Background: Ring Signatures

Ring signature [RST01] allows a ring member to use her/his secret key to sign any message on behalf of this ring

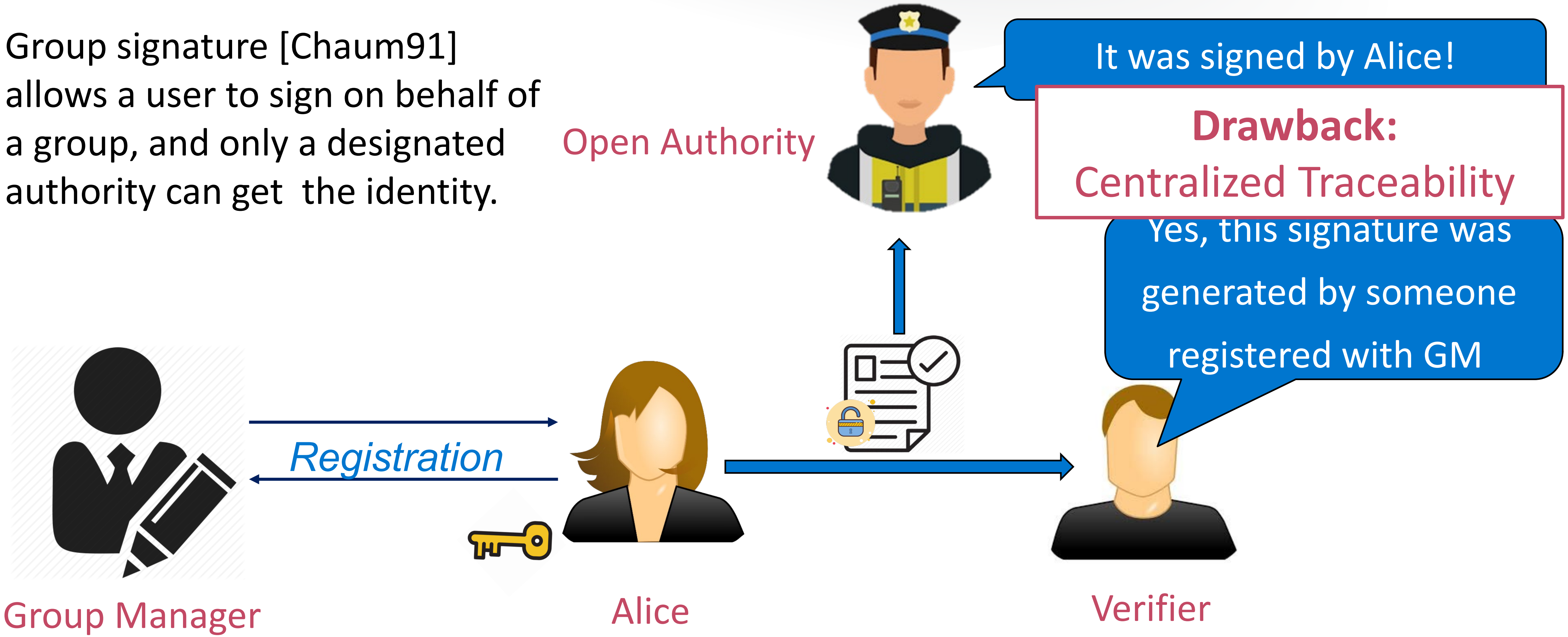
Drawback:
Uncountable Anonymity



Everyone can verify this message was signed by a ring member, but cannot infer anything about the real signer

Background: Group Signatures

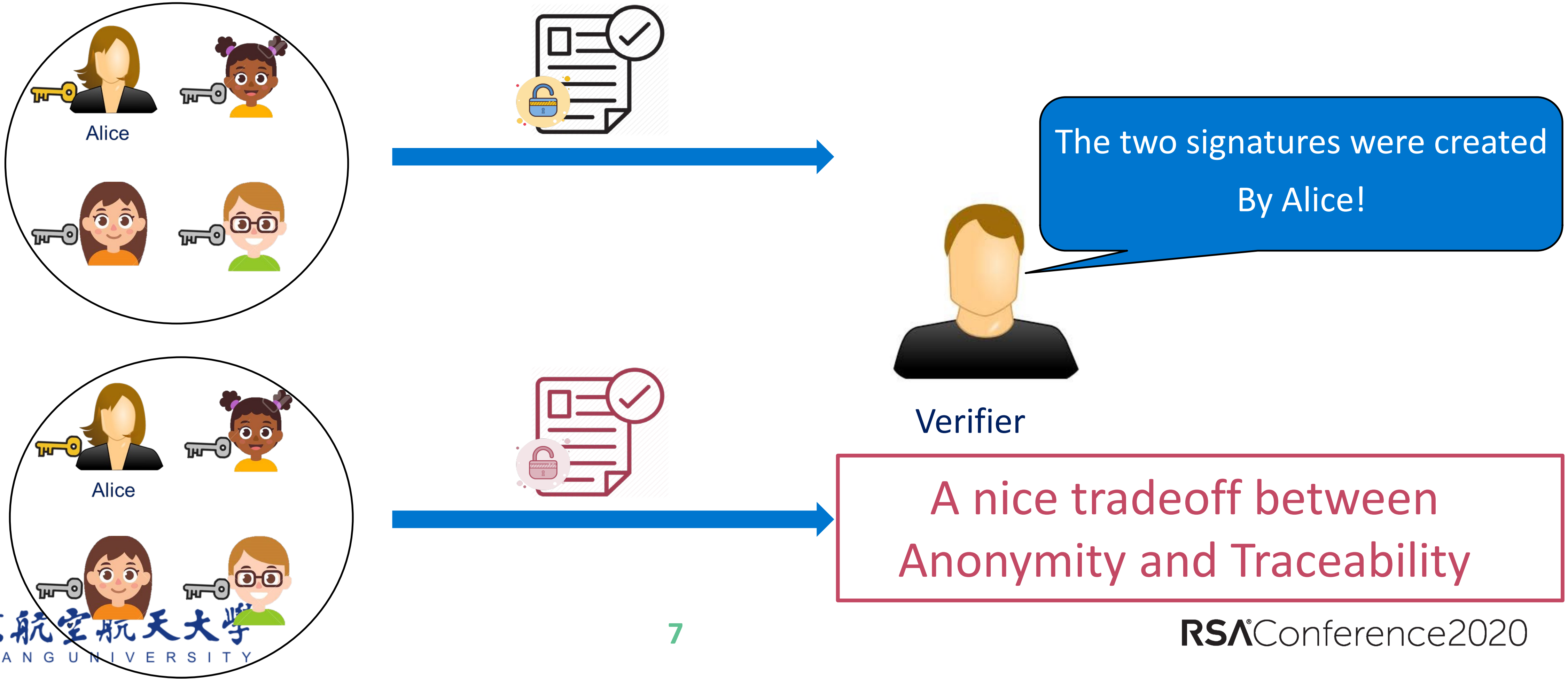
Group signature [Chaum91] allows a user to sign on behalf of a group, and only a designated authority can get the identity.



Drawback:
Centralized Traceability

Background: Traceable Ring Signatures

In ring signature [LWW04], every two signatures w.r.t the same ring, generated by the same signer for different messages, can be publicly traced to the singer



A nice tradeoff between Anonymity and Traceability

Background: Application of Traceable Ring Signatures

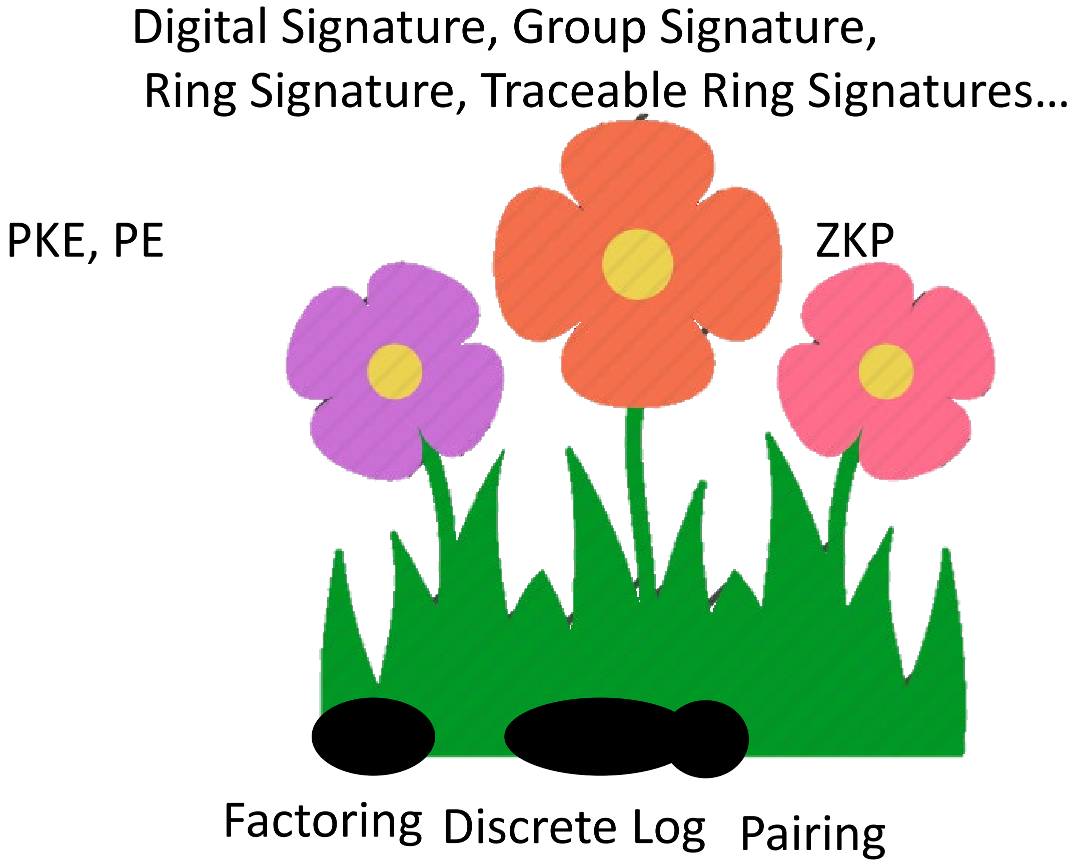
E-voting

- Dishonest voters who vote for two candidates will be identified

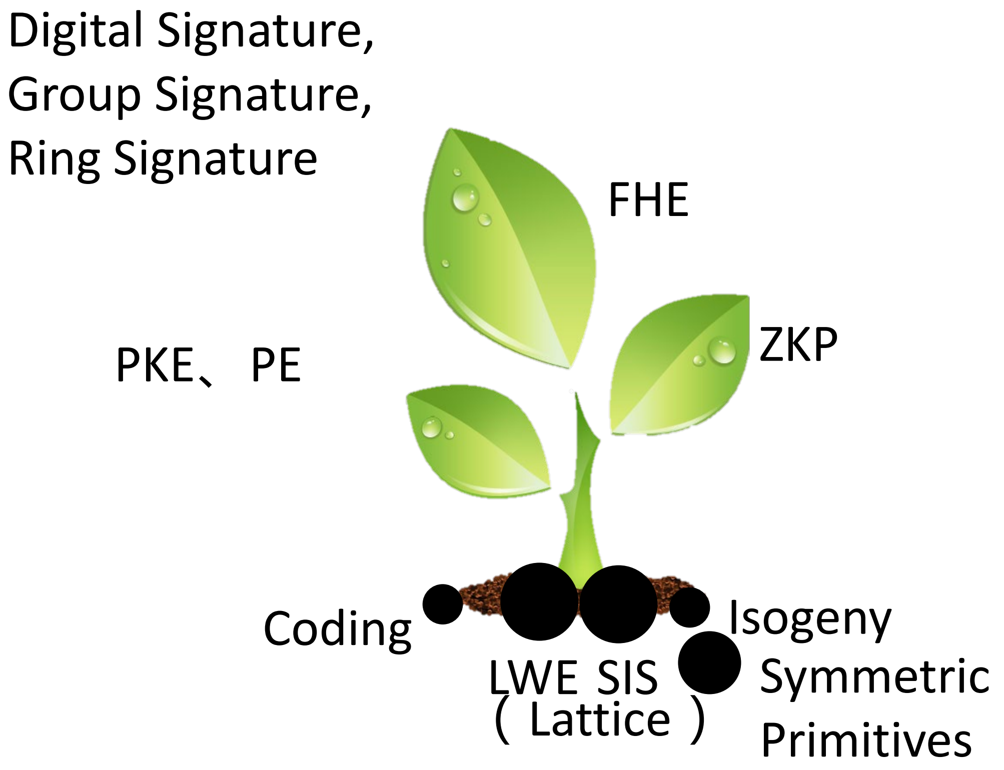
Offline E-cash

- Dishonest users who perform double-spending attacks will be identified

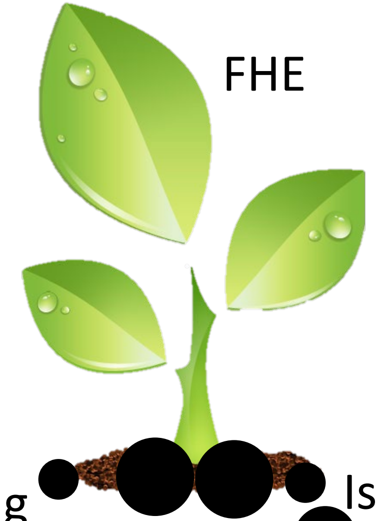
Background: Post-quantum Cryptography


Digital Signature, Group Signature,
Ring Signature, Traceable Ring Signatures…
PKE, PE
ZKP
Factoring
Discrete Log
Pairing

[Shor94]: Algorithms for quantum computation: discrete logarithms and factoring



Motivations



Digital Signature,
Group Signature,
Ring Signature

Traceable Ring Signature

FHE

ZKP

PKE、 PE

Coding

LWE SIS
（Lattice）

Isogeny

Symmetric
Primitives

Building Blocks

Building Blocks: Pseudorandom Function

- $F: K \times X \to Y$ is a family of pseudorandom functions, if for

$k \leftarrow K, f \leftarrow \mathcal{F}[X:Y]$

$$F(k,\cdot) \approx f(\cdot)$$

- Additional Property ---Uniqueness

For $x \in X, k_1 \neq k_2$, we have

$$\Pr[F(k_1,x) \neq F(k_2,x)] \in \mathrm{negl}(\lambda)$$

Building Blocks: Pseudorandom Function

Additional Property ---Intersection-free Range

- The range Y is a vector space of rational numbers
- For every two distinct elements y_1 , y_2, and any polynomial $N(\cdot)$,

$$\Pr[\exists i \leq N(\lambda), y_1 + i\delta_1 = y_2 + i\delta_2 : \delta_1, \delta_2 \hookleftarrow \mathcal{Y}] \in \mathrm{negl}(\lambda)$$

Building Blocks: Pseudorandom Function- Example

Example: PRF in Fujisaki and Suzuki’s construction [FS07]

$$F(k, x) = H(x)^k \in G$$

$G$is a DDH group, and H is a random oracle.

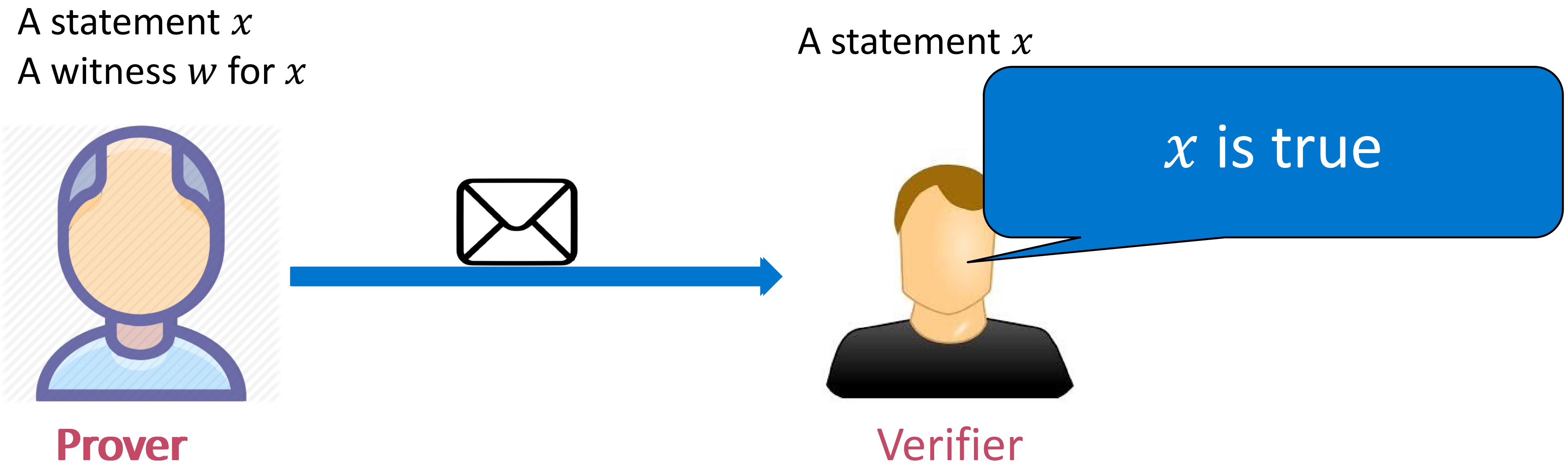
Uniqueness: every $k_1 \neq k_2, H(x)^{k_1} \neq H(x)^{k_2}$

Intersection-free range:

G is a vector space of rational numbers

$$\begin{aligned}&\Pr[\exists i \leq N(\lambda), y_1 \cdot \delta_1^i = y_2 \cdot \delta_2^i : \delta_1, \delta_2 \hookleftarrow \mathbb{G}]\\ &\leq \Pr[\exists i \leq N(\lambda), y_1/y_2 = \delta^i : \delta \hookleftarrow \mathbb{G}] \leq \frac{N(\lambda)}{q(\lambda)} \in \mathrm{negl}(\lambda).\end{aligned}$$

Building Blocks: Non-interactive Zero-knowledge Proof of Knowledge



A statement x
A witness w for x

A statement x

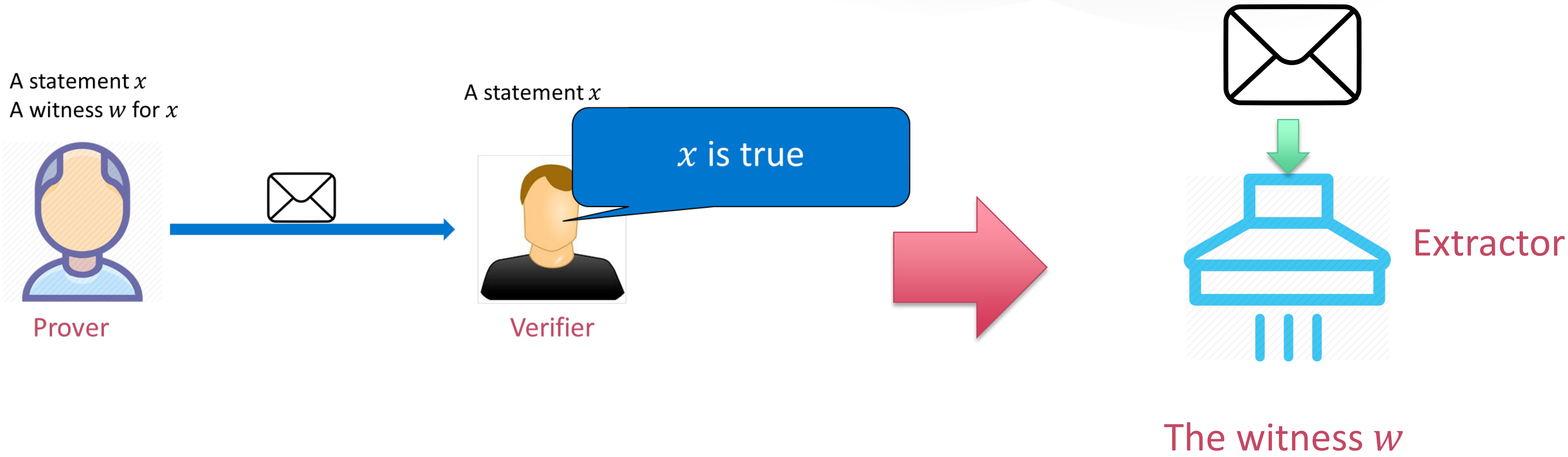
x is true

Prover

Verifier

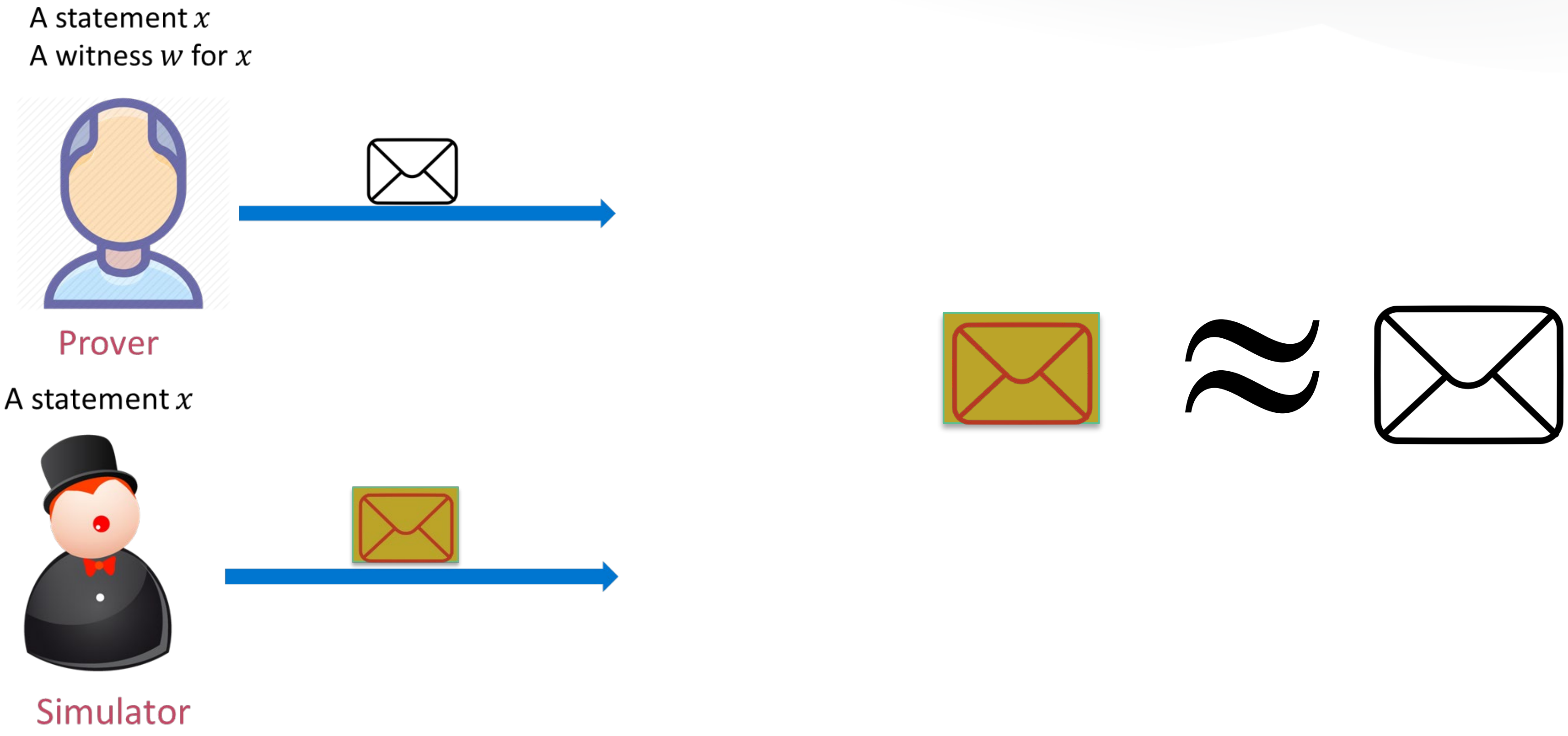
- Completeness: an honestly generated proof for a true statement will always be accepted

Building Blocks: Non-interactive Zero-knowledge Proof of Knowledge



- Proof of knowledge: a witness can be extracted from a valid proof by an extractor

Building Blocks: Non-interactive Zero-knowledge Proof of Knowledge



A statement x
A witness w for x

Prover

A statement x

Simulator

$\approx$

- Zero-knowledge : a valid proof can be simulated without the witness

General Framework of Traceable Ring Signatures

Framework of Unique Ring Signature [FZ12]

- Key Generation:

Choose a key of PRF as the secret key, and take the commitment

of it as the public key.

- Sign: a signature consists of a label and a proof

Label: $l = F(sk, (R, m))$, R is a set of public keys, m is the message

Proof: prove l is correctly generated by some sk whose public key is in R

- Link:

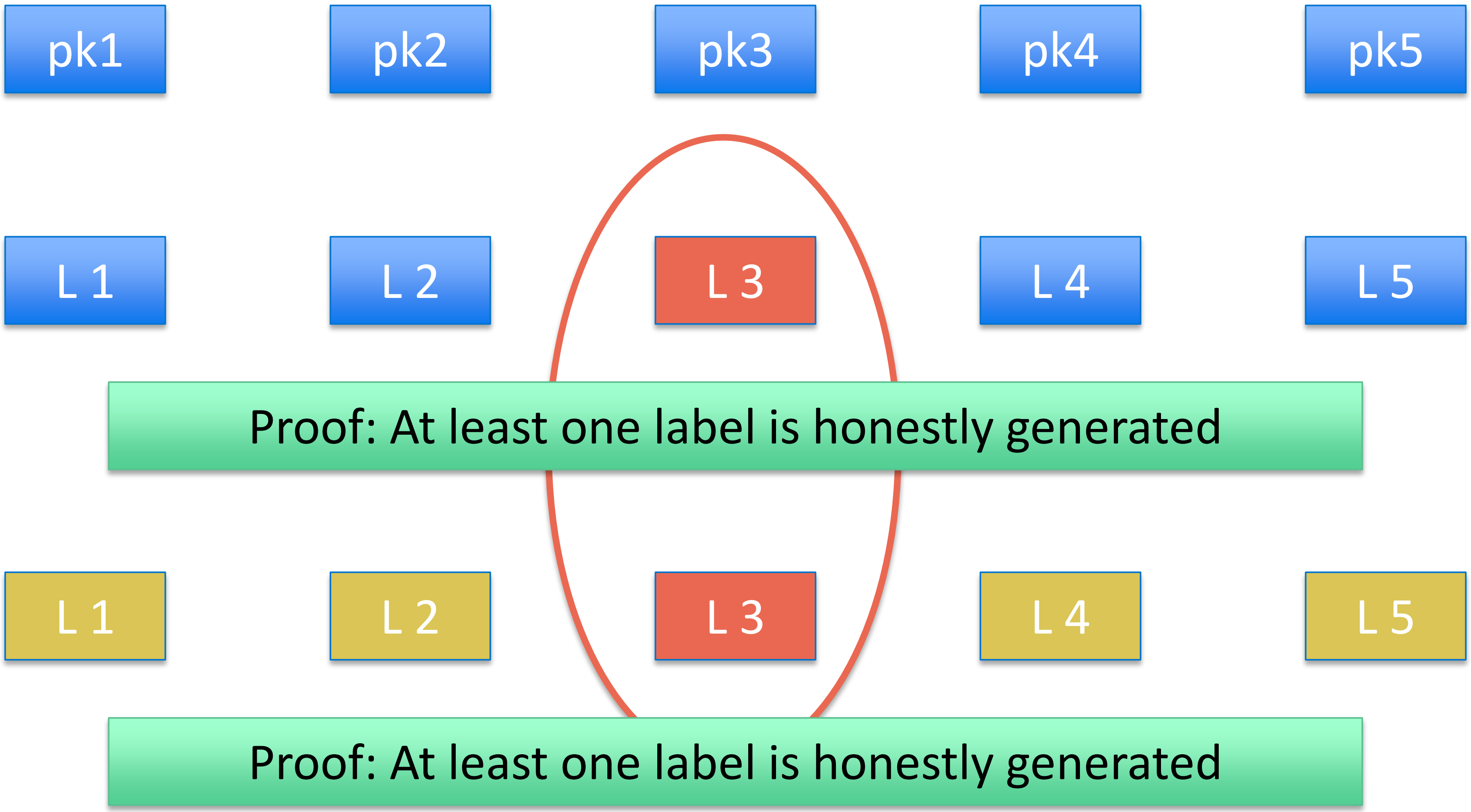
If the two signatures have the same label, they will be linked

Our Framework: Design Principle

- Ring
- Signature 1

  Using sk3
- Signature 2

  Using sk3



pk1 pk2 pk3 pk4 pk5

L 1 L 2 L 3 L 4 L 5

Proof: At least one label is honestly generated

L 1 L 2 L 3 L 4 L 5

Proof: At least one label is honestly generated

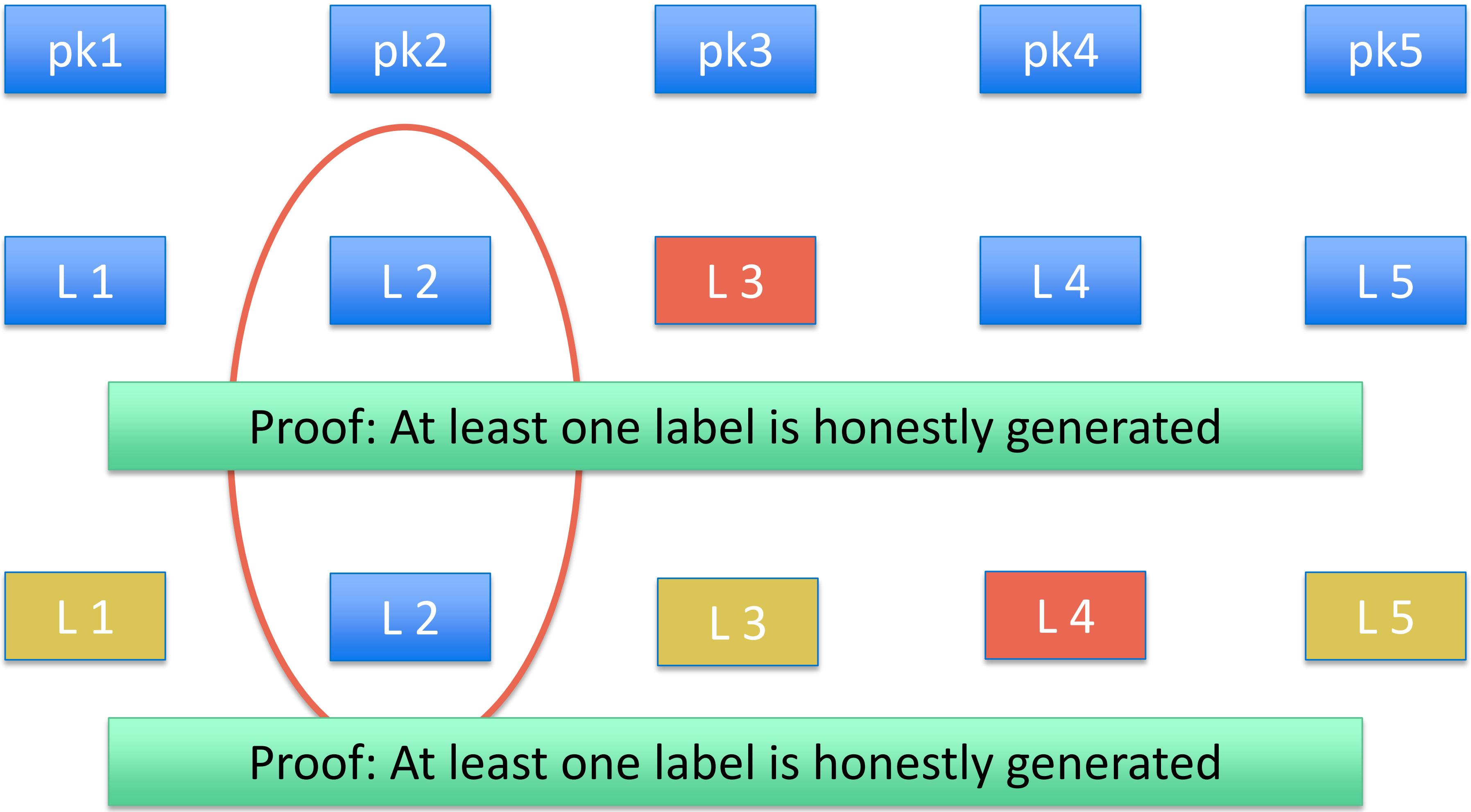
  - L3 in two signatures are identical,
  - We know they are created by someone **whose pk is pk3**

A Possible Attack

- Ring
- Signature 1

  Using sk3
- Signature 2

  Using sk4



pk1 pk2 pk3 pk4 pk5

L 1 L 2 L 3 L 4 L 5

Proof: At least one label is honestly generated

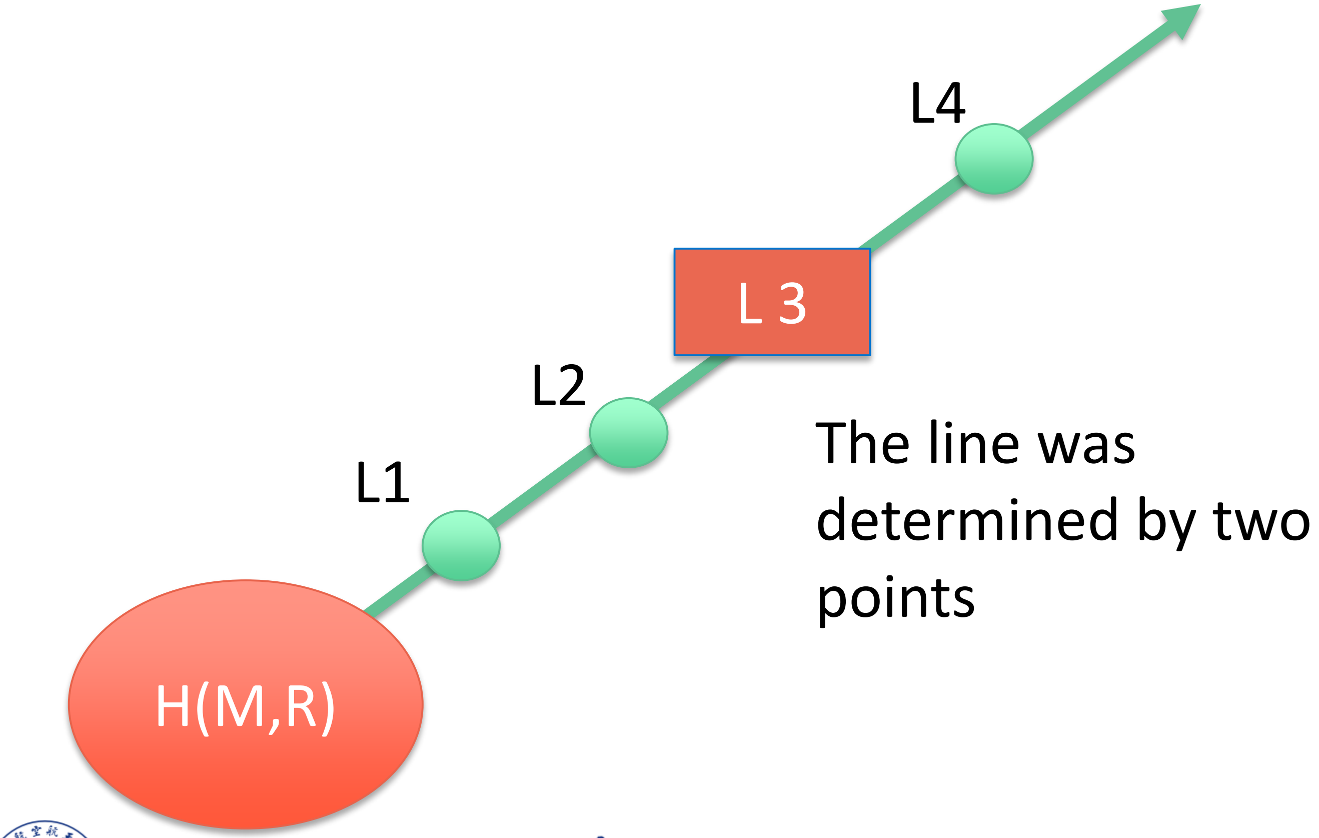
L 1 L 2 L 3 L 4 L 5

Proof: At least one label is honestly generated

  - Signature 2 contains a label L2 that was borrowed from Signature 1
  - The two signatures will be wrongly traced to PK2!

Our Framework: More Details

- To prevent malicious users from framing honest users, we need to ensure that other labels are uniquely determined by the honest label and the message.



The line was determined by two points

$$\delta = \frac{L3 - H(M,R)}{3}$$

$$L_i = H(M,R) + i\delta$$

L3 is an evaluation of PRF. We need to perform ADD and Scalar Multiplication Operations on L3.

Our Framework: Security analysis

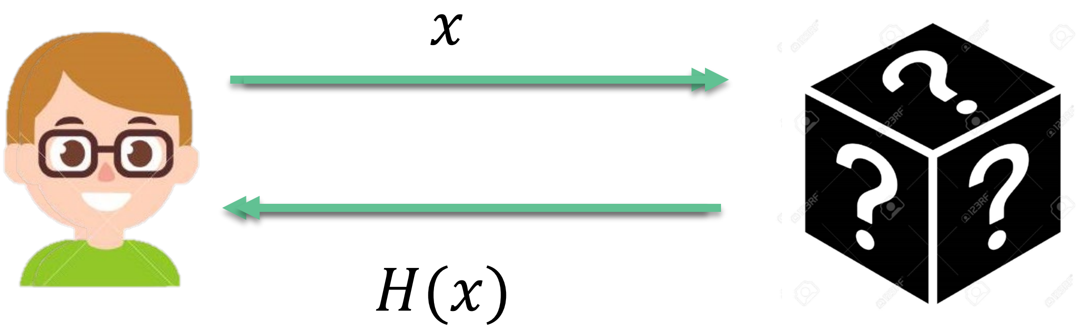
- Tag-Linkability: the total number of unlinked signatures with one tag cannot exceed the total number of ring members
- From the simulation-extractability of the NIZK proof system, and the uniqueness of PRF.
- Anonymity: when a signature is signed by either of two signers, an attacker cannot infer anything as to by whom this signature is signed
- From the zero knowledgeness of the NIZK proof system, and the pseudorandomness of the PRF.
- Exculpability : an honest signer cannot be accused of being dishonest by breaking the rule, even if every ring memeber except him is corrupted.
- From the simulation-extractability of the NIZK proof system, and the pseudorandomness of PRF.

RSAConference2020

Efficient Traceable Ring Signatures in Quantum Random Oracle Model

What is the Quantum Random Oracle Model

To get the output of a hash function H

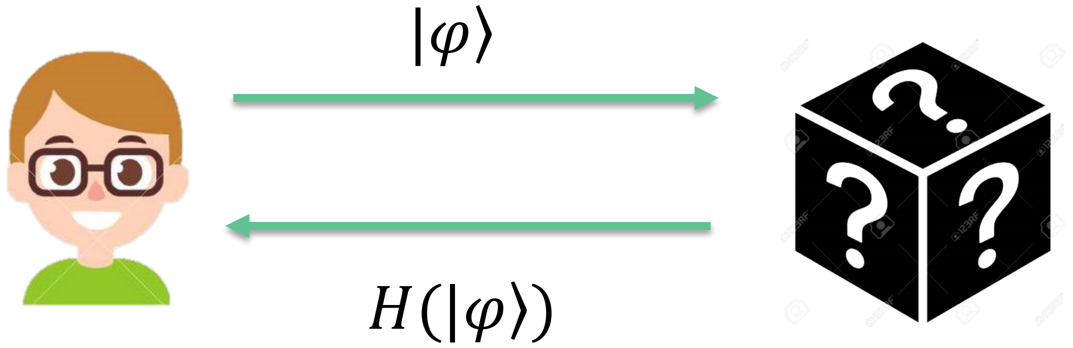


x

$H(x)$

Random Oracle Model

Superposition queries are allowed



$|\varphi\rangle$

$H(|\varphi\rangle)$

Quantum Random Oracle Model

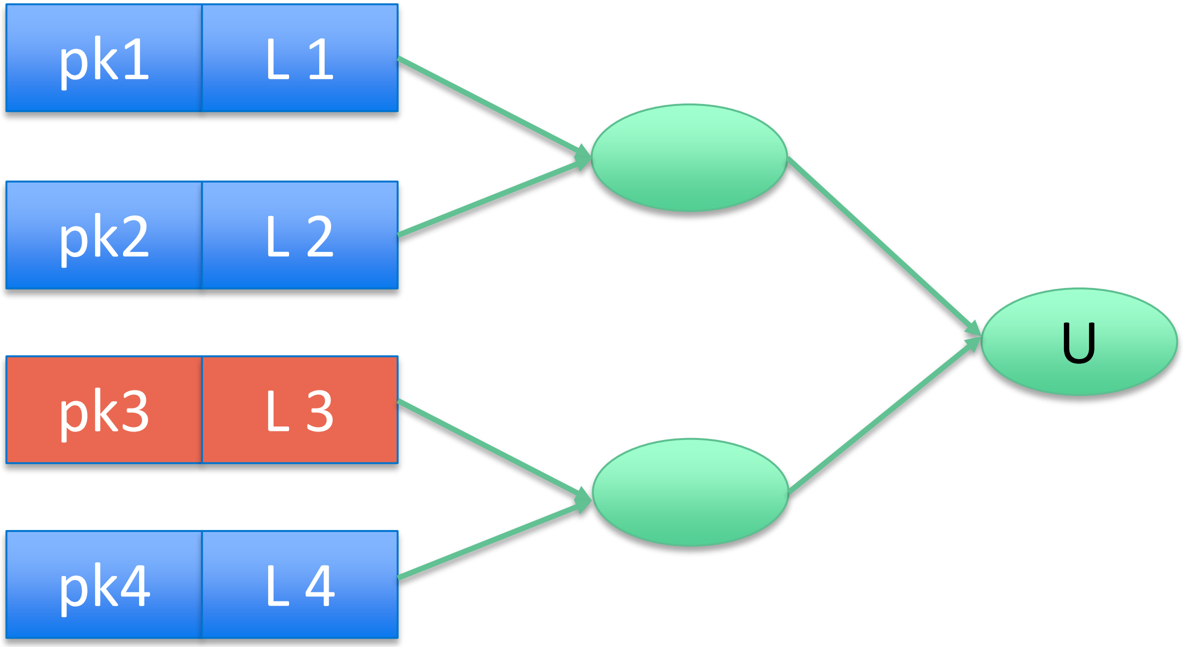
An Efficient PRF in QROM

$$F^H : \mathbb{Z}_q^n \times \{0,1\}^* \to \mathbb{Z}_p^m \text{ with } F^H(T,\mathbf{s}) = \lfloor H(T)\cdot\mathbf{s}\rceil_p$$

- H is modeled as a quantum random oracle
- The pseudorandomness can be reduced from LWE assumption

We prove the pseudorandomness in QROM, by using Zhandry's programming technique [Zhandry 12]

A Sigma Protocol for Our Construction



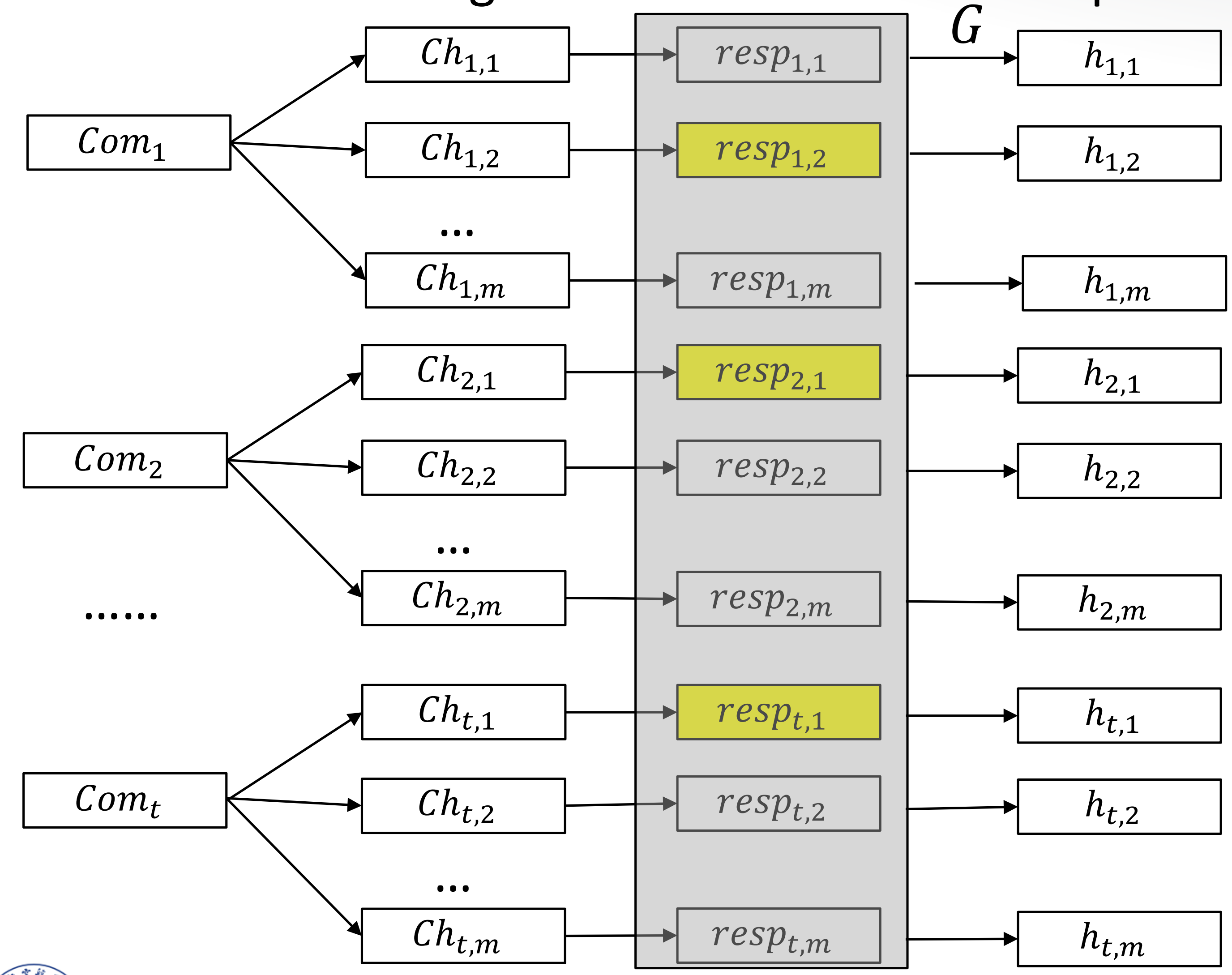
Merkle Tree-based Accumulator

We design a Stern-like protocol to prove :

- There is an honestly generated node that was accumulated to U

Obtain a secure NIZKPoK in QROM: Unruh Transform

Hash all of them to get the selection what to open



▨ Hidden by a random function

Idea

- Make the random function invertible (for extractor)
- All needed information to extract the witness is already contained in the proof.

Apply What You Have Learned Today

- In this paper, we give a general framework of traceable ring signatures from PRF and NIZKPoK
- We also provide a concrete construction by instantiating our framework with lattice-based components, and prove its security in the quantum random oracle model
- You can obtain your traceable ring signatures by instantiating our framework with other possible components
- You may improve our framework in efficiency or security

Thanks for your listening