RSA®Conference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID:CRYP-F03

Accountable Tracing Signatures from Lattices

San Ling, Khoa Nguyen, Huaxiong Wang, Yanhong Xu

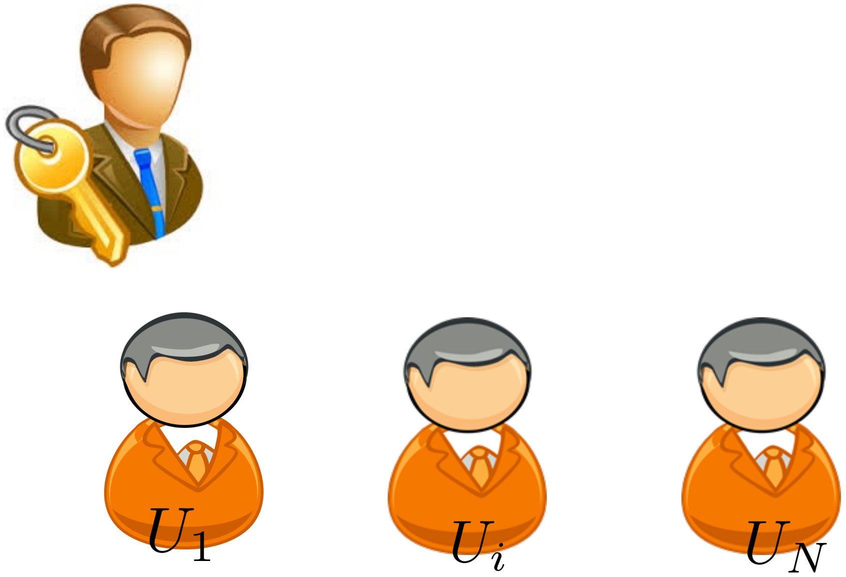
Nanyang Technological University, Singapore

#RSAC

Introduction

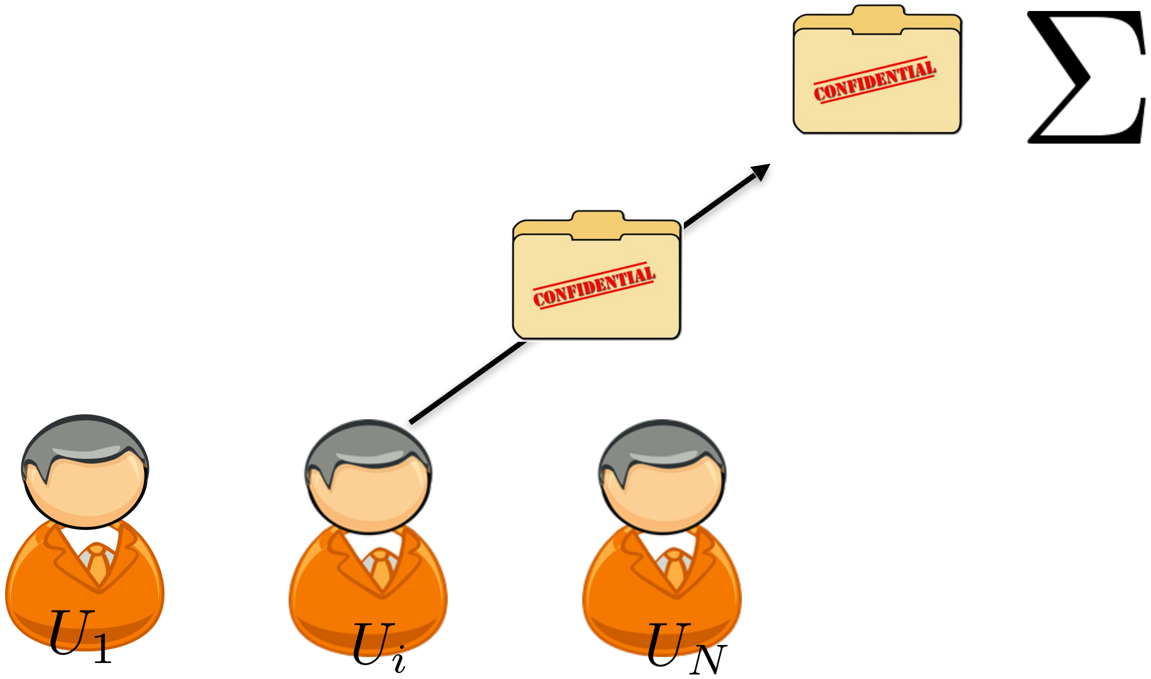
- Group Signatures
- Motivation

Group Signatures [Chaum, van Heyst, EC'91]



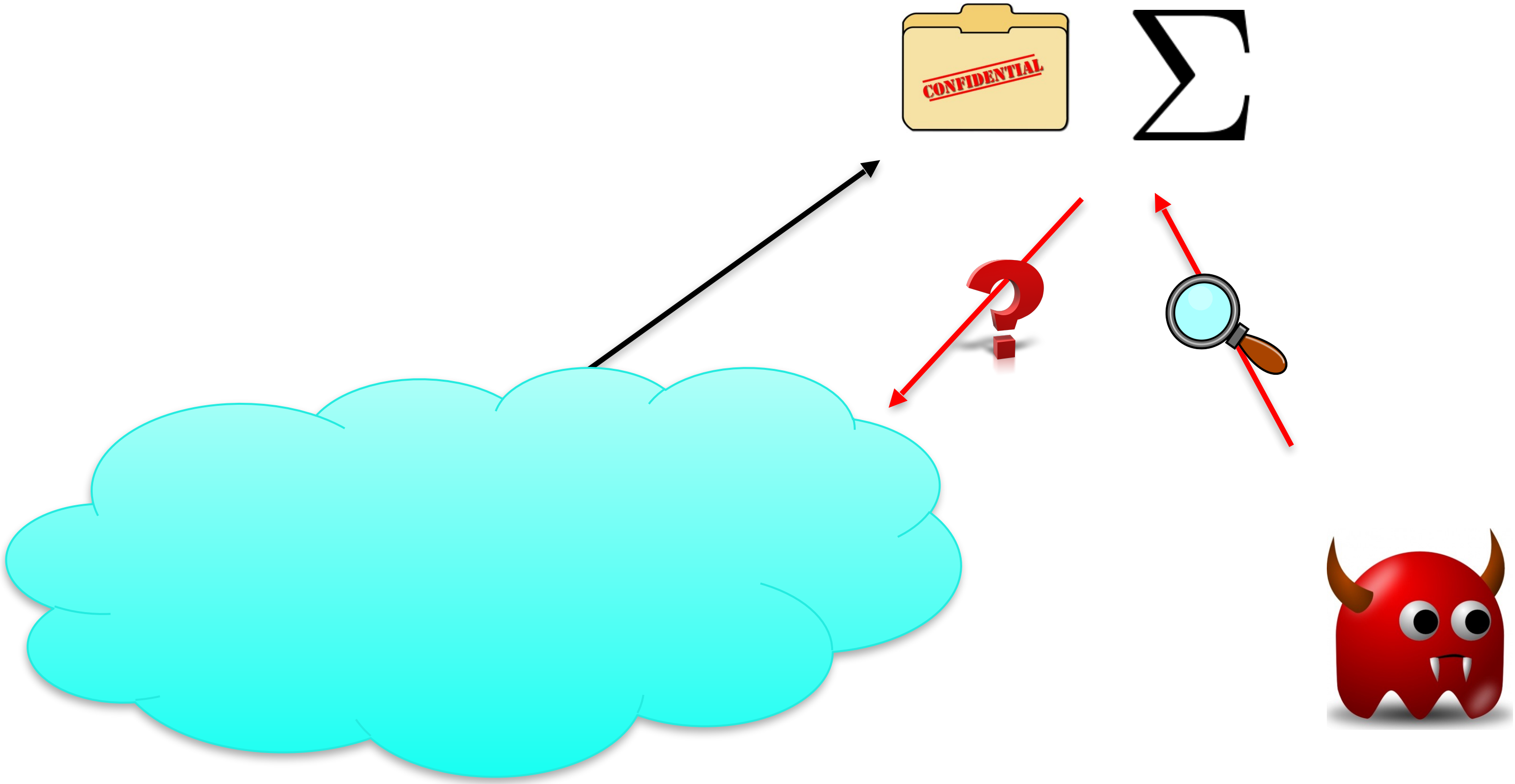
Group manager (GM) manages a set of users.

Group Signatures [Chaum, van Heyst, EC'91]



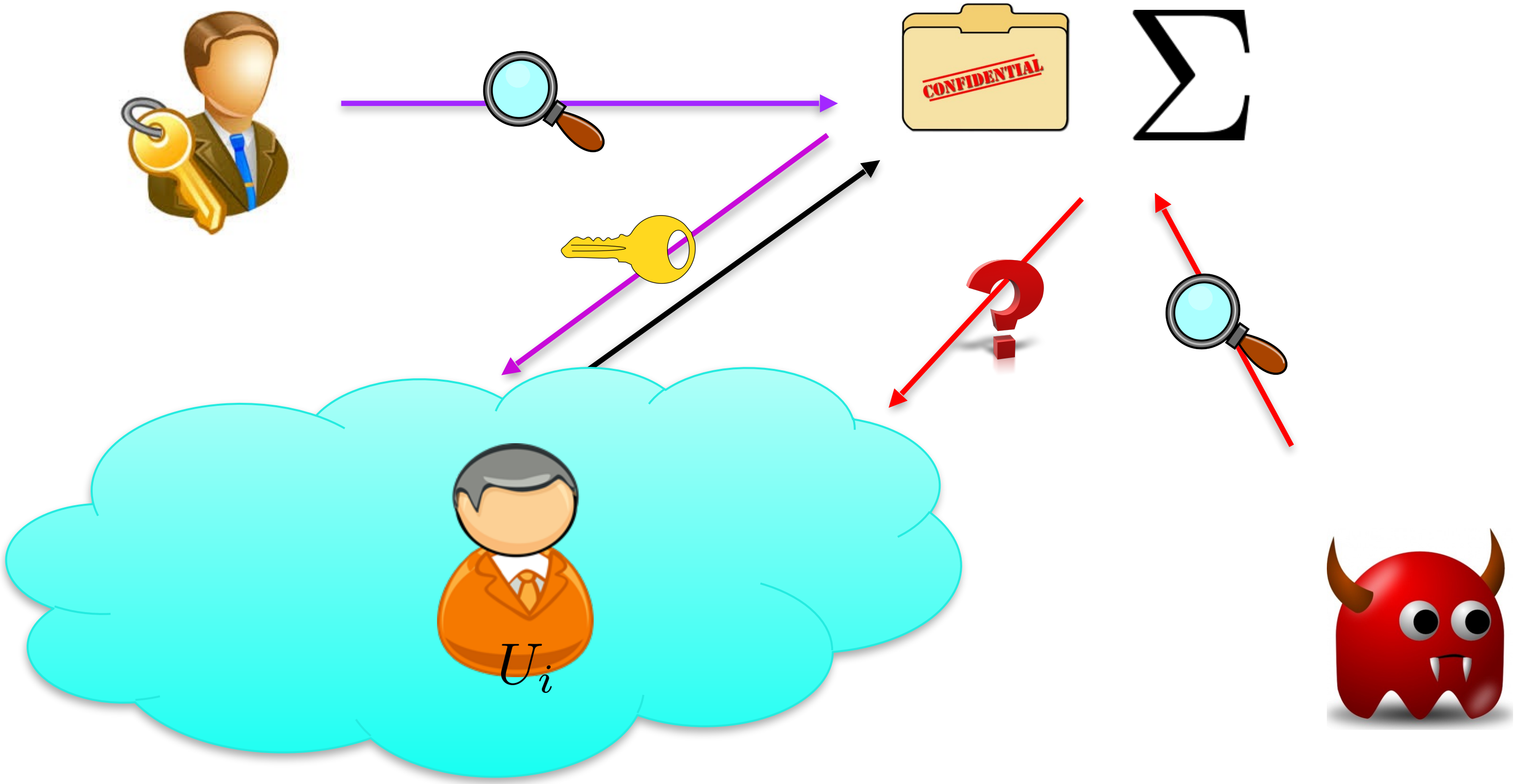
Each user is able to sign messages on behalf of the group.

Group Signatures [Chaum, van Heyst, EC'91]



- Anonymity.

Group Signatures [Chaum, van Heyst, EC’91]



- Traceability.

Why Group Signatures (GS)

- Potential applications in practice:
  - Anonymous public transportation,
  - Electronic auction,
  - Online bidding, …
- Theoretical interests. It requires a sophisticated combination of
  - Digital signature,
  - Encryption,
  - Zero-Knowledge (ZK) proof.
- The techniques apply to:
  - Anonymous credentials,
  - E-cash,
  - Adaptive oblivious transfers, …

Observations

- Opening authority (OA) can open all signatures.
  - No way to verify his accountability.
- One attempt to restrict the power of OA:
  - GS with Message Dependent Opening (MDO).
  - Only open signatures of message approved by an additional authority-admitter.
    - Can open signatures of all users, including innocent ones, who ever signed a specific message that was approved by admitter.
    - Can open all signatures by colluding with admitter.

Accountable Tracing Signatures [Kohlweiss, Miers, PoPETs'15]

- GM/OA.
- Traceable users and non-traceable ones.
  - Traceable users: anonymity can be broken by GM/OA.
  - Non-traceable users: anonymous throughout the scheme.
- When a user join the group:
  - First, GM/OA determines traceable or non-traceable.
  - Then, it issues a traceable or non-traceable certificate.
  - Later, it reveals his choices to enforce his accountability.

Surveillance Controls of some Entrance

Security

Privacy

- Implement using an accountable tracing signature(ATS) scheme.
- Suspected users vs non-suspected ones.

Surveillance Controls of some Entrance

Security

Privacy

- A standard group signature (e.g., [Bellare, Micciancio, Warinschi, EC’03]?
- A traceable signatures [Kiayias, Tsiounis, Yung, EC’04]?

Motivation of this Work

- Kohlweiss and Miers' work: based on number-theoretic assumptions.
  - Vulnerable against quantum computer.
  - Can we have post quantum instantiation such as: lattice-based constructions?

Lattice-Based Group Signatures

- [Gordon, Katz, Vaikuntanathan, AC'10]: the first lattice-based one.
- 12 other schemes.
  - Group signature with MDO.
- Still open of making OA accountable in the lattice setting.

- Lattice-based ATS?

Our Results

Our Results

- The first lattice-based ATS scheme.
- Security model: [Kohlweiss, Miers, PoPETS’15].
  - Ring Short Integer Solution (RSIS) and Ring Learning with Errors (RLWE).
  - Random oracle.
- Main building blocks:
  - Key-oblivious encryption (KOE) scheme from lattices.
  - Zero-Knowledge (ZK) protocol for quadratic relations in the ring setting.

RSA®Conference2019

Our Techniques

Generic Construction [Kohlweiss, Miers, PoPETS'15]

Ordinary Group Signature

- When signing messages,
  - Each user first encrypts **id** under **pk**, in which GM knows **sk**.
  - It then proves the well-formedness of the ciphertext.

Accountable Tracing Signature

- When signing messages,
  - Traceable user encrypts **id** under **pk**, in which GM knows **sk**.
  - Non-traceable user encrypts **id** under **pk'** in which no one knows **sk'**.

- Randomize pk to epk so that it is infeasible to determine the relation.
  - Key-oblivious encryption (KOE) scheme.
  - ElGamal cryptosystem [Gamal, C'84].

Generic Construction [Kohlweiss, Miers, PoPETS'15]

Ordinary Group Signature

- When signing messages,
  - Each user first encrypts id under pk, in which GM knows sk.
  - It then proves the well-formedness of the ciphertext.

Accountable Tracing Signature

- When signing messages,
  - Traceable user encrypts id under his own epk, in which GM knows sk.
  - Non-traceable user encrypt id under his own epk in which no one knows sk'.

- Key-oblivious encryption (KOE) scheme.
- ZK protocol for honest encryption.

Our Technique-KOE

- Kohlweiss and Miers built their KOE from ElGamal cryptosystem [Gamal, C'84].
- A candidate: [Lyubashevsky, Peikert, Regev, J.ACM'13] (ring-based) encryption scheme.
- Noise in lattice based encryption.
  - Set the parameters to control the noise growth.
  - Follow Kohlweiss-Miers technique.

Our Technique-ZK Protocol for Quadratic Relation

- The user needs to prove id encrypted under epk.
- Reduces to proving knowledge of a and x such that y=a x over the ring.
- Two lines of ZK protocol from lattices.
  - Rejection sampling technique, compact: linear equations.
    - ○ Prove knowledge of x such that y= A x mod q.
  - Decomp/Extension/Permutation, less practical: quadratic relation.
    - ○ Stern-like protocols.
    - ○ Prove knowledge of A and x such that y= A x mod q.

Our Technique-Lattice-Based Ordinary Group Signatures

- LB ordinary GS: [Ling, Nguyen, Wang, Xu, PKC’18].
  - LPR encryption, Stern-like ZK, Ducas-Micciancio Signature.
- Byproduct: Constant-size signatures.
  - The sizes of signatures: independent of N.
  - Larger: treatment of quadratic relations.

Accounting Algorithm

- GM/OA reveals his choice and randomness.
  - Traceable users: epk = Rand (pk, r).
  - Non-traceable users: epk = Rand (pk', r).
- User then checks whether his epk was computed as claimed.
- GM/OA is required to sign epk when user joins the group.
  - GM/OA: Non-repudiation of epk.

Summary

Summary

- The first lattice-based ATS scheme.
- Far from being practical.
  - Efficient ZK protocol?
- Accountable forward tracing
  - Backward tracing?

Thank you for your attention!