Attribute-based Authentication

Huihui Yang
Supervisor: Vladimir Oleshchuk
University of Agder, Norway
Outline

- Background and motivation
- ABA properties
- ABA workflow
- ABA construction
- ABA applications
- Some open problems
- Conclusions
Authentication is very important for Internet communication.
Traditional Public key authentication
ABA

- Based on users’ attributes: age, gender
- A group of users share the same public attribute key
Background and Motivation

Advantages of ABA

- More flexibility: multi-organization cooperation
- More privacy: anonymity, selective disclosure
ABA Properties

- Anonymity
- Unforgeability
- Unlinkability
- Coalition resistance
- Traceability
ABA Workflow

Authorities: divided by functions

- Central authority: generate basic parameters, users’ keys
- Attribute authority: generate private/public key pairs, users’ private attribute keys
- Revocation authority: revoke users or their attribute keys
- Opener: reveal the signer’s identity given a signature
ABA Workflow
ABA Construction

Examples: based on group signatures, ring signatures
  ◦ Group signature: traceability
  ◦ Ring signature: no traceability

Reference:
  ◦ ...
ABA Applications

Part of attribute-based access control (ABAC)
ABA Applications

- Multi-organization cooperation
ABA Applications

- Data outsourcing and cloud computing
Open Problems

- ABA schemes are usually very complicated.
  - Complicated algorithms, lots of computations
  - Gap between theory and application

- Revocation
  - User-based
  - Attribute-based
Conclusions

- ABA introduction
- Workflow
- Construction
- Applications
- Open problems
THANK YOU!