A Probably Secure Ring Signature Scheme in Certificateless Cryptography [1]

Yin-Hong Hsu

01 10, 2018

Outline

Preliminaries

Security Model

Analysis of A Generic Construction of CL-Ring

A Concrete CL-Ring Scheme

References

Preliminaries

- certificateless ring signature
  - setup
  - partial-private-key-extract
  - set-secret-value
  - set-private-key
  - set-public-key
  - ring-sign
  - verify

Security Model

- Type I Adverary
  - replace user's public key
- Type II Adverary
  - access to the master key (which be used to be a part of private key)

Security Model

- Game I: Unforgeability of CL-Ring against Type I Adversery
- Game II: Unforgeability of CL-Ring against Type II Adversery

Analysis of A Generic Construction of CL-Ring

- Construction of CL-Ring
  - Detail of 7 functions were mentioned in page 2
- And some security analysis with Game I and II

A Concrete CL-Ring Scheme

- Different algorithm for these 7 functions
- The number of pairing computation is constant and dose not grow with the number of group members

References

[1] L. Zhang, F. Zhang, and W. Wu, “A Provably Secure Ring Signature Scheme in Certificateless Cryptography,” *ArXiv e-prints*, Dec. 2017.

Thanks for Your Attentions