Zero-pole cancellation for identity-based aggregators: a constant-size designated verifier-set signature

E CHEN, Yan ZHU, Changlu LIN, Kewei LV

Frontiers of Computer Science, DOI: 10.1007/s11704-019-8320-0

Problems & Ideas

- Problems :
  - The existing schemes only support one verifier or multiple verifiers that must cooperate to verify the validity of signature.
  - How to compress a designated set of arbitrary size into a constant-size element.
  - All existing schemes only deal with static and fixed number of verifiers.
- Ideas:
  - Our scheme allows to designate many verifiers, each of whom is able to verify the validity of the signature by himself.
  - Find a compression process to prevent the adversary from tampering with the designated verifier-set.
  - Construct the first designated verifier-set signature for arbitrary dynamic verifiers from a large number of users.

Main Contributions

1. **We propose two identity-based aggregators (IBA) that compress a designated set of verifier's identities to a constant-size random string .**
2. **By using the IBA, we propose the first designated verifier-set signature (DVSS) scheme constructed from the Zero-Pole Cancellation method which can eliminate the same elements between zeros-based aggregator and poles-based aggregator.**
3. **The generated signature with short and constant length can be independently verified by multiple verifiers.**
4. **Our DVSS scheme is proved to be secure into the sense of unforgeability and exclusivity, respectively.**