Distributed Identity Based Short Linkable Ring Signature

Kasra EdalatNejad

Prof. Bryan Ford
DEcentralized and DIstributed Systems
Goal

- Anonymity
- Accountability
- Usability
Ring Signature

Anonymous
Spontaneous
Linkable Ring Signature

- Event tag
- Accountable
- Linear size
Cryptographic Accumulator

- Make a short representation
- Not a compression
Accumulator

- Accumulate set(X): V
- Generate witness: W
- Check membership: (x, W, V)
Additional properties

- Dynamic
- Authority
Bilinear Pairing (Nguyen)

- Master Secret Key: $s$
  \[ V = \prod_{x \in X} (x + s).P \]
- Publicly computable
  \[(P, sP, s^2P, ..., s^nP)\]
Bilinear Pairing (Nguyen)

- With Authority:
  - Dynamic
  - Authority

- No Authority:
  - Trusted setup
  - Not efficient
Accumulator VS Ring Signature
Short Linkable Ring Signature

- Membership in ring
- Knowing private key
- Correct link tag
Identity Based Cryptography

- Public key is based on name
- No Certificate Authority
- Authority generate private key
- Key escrow
Bilinear pairing SLRS

- Membership: Nguyen’s Accumulator
- Knowledge of private key:
  - Sakai-Kasahara IBC
  - $1/(x + s)\cdot Point$
- Link
Secret Sharing: Direct

- Shamir polynomial
- Distributed key generation
- Compute: $Q \rightarrow sQ$
Secret sharing: inverse

- Compute: \[ Q \rightarrow 1/(x + s)Q \]
- Secure Multiparty Computation
- Online participation for each request
- Not efficient
Distributed IBC

- Use SS inverse
- Distributed trust
Distributed Nguyen’s Acc

● Trusted setup
● Distributed trust
  ○ SS Direct: Week dynamic
  ○ SS Inverse: Fully dynamic
## Distributed Accumulator

<table>
<thead>
<tr>
<th>Operation</th>
<th>None</th>
<th>SS Direct</th>
<th>SS Inverse</th>
</tr>
</thead>
<tbody>
<tr>
<td>Witness generation</td>
<td>$O(n^2)$</td>
<td>$O(n)$</td>
<td>Accumulate: $O(n)$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>No check witness: $O(1)$</td>
</tr>
<tr>
<td>Add member</td>
<td>$O(n^2)$</td>
<td>$O(1)$</td>
<td>$O(1)$</td>
</tr>
<tr>
<td>Remove member</td>
<td>$O(n^2)$</td>
<td>$O(n^2)$</td>
<td>$O(1)$</td>
</tr>
</tbody>
</table>
Idea

- Hierarchical Accumulator
  - Improve efficiency in non-trusted model

- Hierarchical SLRS
  - Different privacy levels
  - Set management
Voting

- Different levels: City, Canton, Country
- Autonomous sets
- Unique identity link across levels
PoP Party

- Merging parties
- Removing parties
- Attribute based parties
- Multiple attributes for a party
- Distinct parties? Same IBC authority?
Challenges

● Efficiency
● Efficiency
● Efficiency
Summary

- Accumulator
- Linkable Ring Signature
- Identity Based Cryptography
- Distributed Authority
- Distributed Identity Based Short Linkable Ring Signature (DIBSLRS)
RSA

- Accumulator
- Short Linkable Ring Signature (SLRS)
- Authority
- Certificate public key