Privacy Enhancing Credential

National Institute of Information and Communications Technology (Japan)

Junji Nakazato
Lihua Wang
Akihiro Yamamura
Motivation

◆ Popularization of the internet services
  ■ Shopping, Bank, Auction…

◆ Using single sign on (SSO) technique
  ■ Ticket type SSO

User -> ticket server
  login -> authentication -> access ticket
  Using ticket

Examples:
- MSN
- eBay
- Qatar airways
Motivation

Disadvantages of SSO

- The same ticket is used for multiple services
- The user’s privacy is obtained by the collusion with services
  - Use frequency of service
  - An order of using service
- The user can transfer ticket to another user

Needs to think about privacy!!
Our goal

- Multiple logins are not needed
  - The user only presents credential of whether he has the right to access service
- User’s privacy is concealed
  - The user can access services with anonymity
- Credential cannot be transferred to anyone
  - No one can transfer correct credential to others
- Authenticated key exchange
  - To provide secure channel between user and service provider

Try to apply “credential system”
Our goal

Authentication & issues **credential**

Presents credential **with anonymity** & **Key establish**

Relationship of **mutual trust**

Service list:
1. Qatar...
2. eBay
3. MSN

Service providers:
- Qatar airways
- eBay
- MSN

User A
Credential system

◆ Previous work
  - “Designated Group Credentials”
  - Ching Yu Ng, Willy Susilo, Yi Mu
  - ASIACCS 2006

- Using pairing technique
- Authority can designate the verifiers
  - Ticket issuer can designate the service providers
- The user authentication is necessary for the outside
- The authority can trace user’s movement
- The user can transfer correct credential to others
## Comparison of requirements

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Unforgeability</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Designated</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Non-transferability</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Anonymity</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Unlinkability</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Technique

- Based on pairing
  - Bilinear: Given any $Q, R$ in $G_1$ and $a, b$ in $\mathbb{Z}_q$, we have $e(aQ, bR) = e(Q, R)^{ab}$
  - Non-degenerate: $e(P, P) \neq 1$
  - Computable: There is an efficient algorithm to compute $e(Q, R)$ for any $Q, R$ in $G_1$

- Non-transferability
  - private key of user is included in the credential

- Unlinkability
  - Randomize credential when he uses it
Our proposed scheme

User A

Computes credentials for each service and randomize them.

((s_1, m_1, a_1, a_2, b_1, b_2, seed_1), (s_2, m_2, a_1, a_2, b_1, b_2, seed_2))

Issues credential (s, i)

Joins services (x, u_a)

Checks the validity of credential

Service list
1. Qatar
2. eBay
3. MSN

Computes credential (s, i)
form x to use services 1 and 3 for user A (designated).

Authenticated key sharing using M(credential)

Service providers

Qatar Airways

eBay

MSN

Check the validity of credential

Including identity (private key)
Conclusion

Propose privacy enhancing credential
- We preserved unlinkability (anonymity).
- We satisfied non-transferability.
- We achieved authenticated key exchange.

We can provide time restriction function
- It can be achieved by a few modification.
- Change generator $F$ to $h(t)$
- $h() : \text{hash function (} h(*) \rightarrow G_1)$
Thanks