Unlinkable Complex Identity Claims
Ruchith Fernando, Bharat Bhargava
Department of Computer Science and CERIAS, Purdue University

Requirements
- Unlinkability
- Multiple Identity Providers
- Multiple Claim Types
- Complex Service Provider Policies

Modified HIBE
- Select a random = \( I_r \)
- \( ID_r = h_1^1 \cdot h_2^2 \cdot h_3^3 I_r \)
- \( ID_r \) is the request

Issuing Claims
- Publish
- HIBE Private Keys generated for each user

Single Claim
- Alice
  - Generate \( ID_r \)
  - Generate \( K_{priv(r)} \)
  - \( K = \text{Decrypt} (\text{Resp}, K_{priv(r)}) \)

Complex Claims
- Service Provider
  - Select \( K \)
  - Key values of the leaves are encrypted using \( ID_r \) and respective parameters

Secure Channel Using \( K \)