CPK: Bounded Identity Based Encryption

James Hughes
Guan Zhi

Identity Based Encryption

- Private matrix to the domain
- Private key to the user
- Public matrix
- Originally described as ECC based system
  - Equally valid in discrete log
- Does not require a bilinear map
- Patented
  - Publication Number WO/2006/074611
    - NAN, XiangHao
    - CHEN, Zhong

System Parameters

- Diffie Hellman group with values (g, p)
- A matrix size (m, n)
- A selection of row values are calculated from identity
  - $h_{1...m} = f(Identity)$
  - Public function
  - SHA-256 or known encryption

Secret Matrix

$$S = \begin{bmatrix} s_{1,1} & \cdots & s_{1,m} \\ \vdots & \ddots & \vdots \\ s_{n,1} & \cdots & s_{n,m} \end{bmatrix}$$

Private to domain

Secret Key

$$S = \begin{bmatrix} s_{1,1} & \cdots & s_{1,m} \\ \vdots & \ddots & \vdots \\ s_{n,1} & \cdots & s_{n,m} \end{bmatrix}$$

Private to domain

$$S_A = \sum_{i=1}^{m} s_{h(i),i} \mod p-1$$

Private to user

Public Matrix

$$S = \begin{bmatrix} s_{1,1} & \cdots & s_{1,m} \\ \vdots & \ddots & \vdots \\ s_{n,1} & \cdots & s_{n,m} \end{bmatrix}$$

Private to domain

$$S_A = \sum_{i=1}^{m} s_{h(i),i} \mod p-1$$

Private to user

$$p_{i,j} = g^{s_{i,j}} \mod p$$

$$P = \begin{bmatrix} p_{1,1} & \cdots & p_{1,m} \\ \vdots & \ddots & \vdots \\ p_{n,1} & \cdots & p_{n,m} \end{bmatrix}$$

Public to domain

Public Key

$$S = \begin{bmatrix} s_{1,1} & \cdots & s_{1,m} \\ \vdots & \ddots & \vdots \\ s_{n,1} & \cdots & s_{n,m} \end{bmatrix}$$

Private to domain

$$S_A = \sum_{i=1}^{m} s_{h(i),i} \mod p-1$$

Private to user

$$p_{i,j} = g^{s_{i,j}} \mod p$$

$$P = \begin{bmatrix} p_{1,1} & \cdots & p_{1,m} \\ \vdots & \ddots & \vdots \\ p_{n,1} & \cdots & p_{n,m} \end{bmatrix}$$

$$P_A = \prod_{i=1}^{m} P_{h(i),i} \mod p$$

Public to domain

Questions

- Secure?
  - Public matrix reduces to the DDH
- Collisions?
  - 32x32 then h is 32x5 or 160 bits
  - Birthday after 2^{80} accounts
- Collusion
  - of near collision (one column different) provides difference
  - 32x32 requires ~1300 private keys.

Collusion Environment

- Without the threat of Collusion
  - Verification and not signature
  - Small matrix
- Without the threat of large scale collusion
  - Non personal equipment
  - Medium Matrix
- With the threat of large scale collusion
  - Authentication module (Chip card, USB token, TPM)
  - Large matrix
- Special Situations
  - One to ten million collusion partners
  - Ultra Large Matrix

- Is this novel?
  - Boneh Franklin
  - Murakami
  - Cocks
  - Heng, Kurosawa, CR-RSA 2004
  - Dodis, Katz, Xu, Yung, EC 2002
- Contact Jim or Guan later....