北京航空航天大學
Beihang University

A Tree-based CP-ABE Scheme with Hidden Policy Supporting Secure Data Sharing in Cloud Computing

Runhua Xu

13 Dec, 2013

Background

- The importance of data self-protection capability

Integrity & Confidentiality

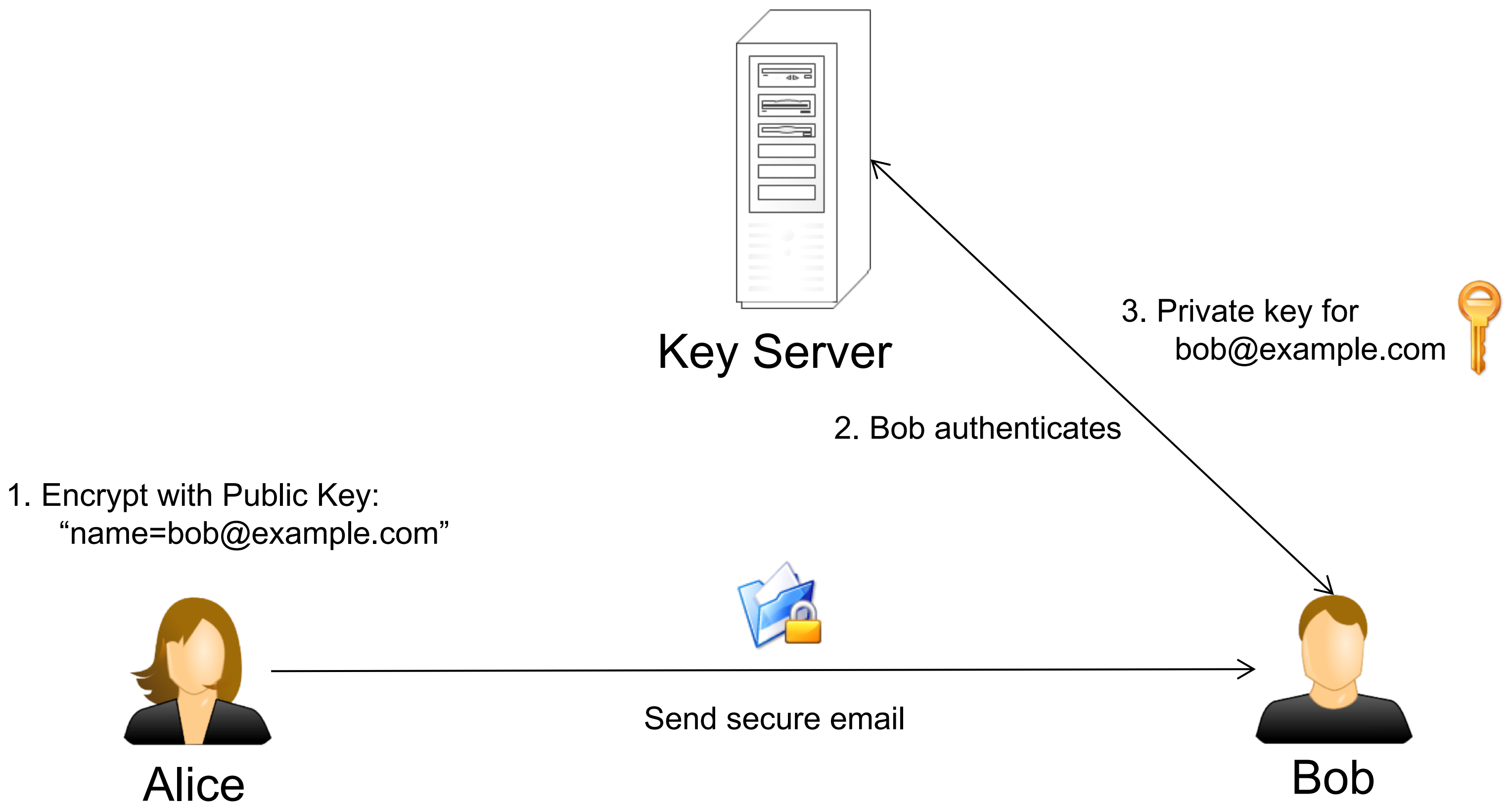
Access Control & encryption

Reliable ?

State Key Laboratory of Software Development Environment
xurunhua@nlsde.buaa.edu.cn

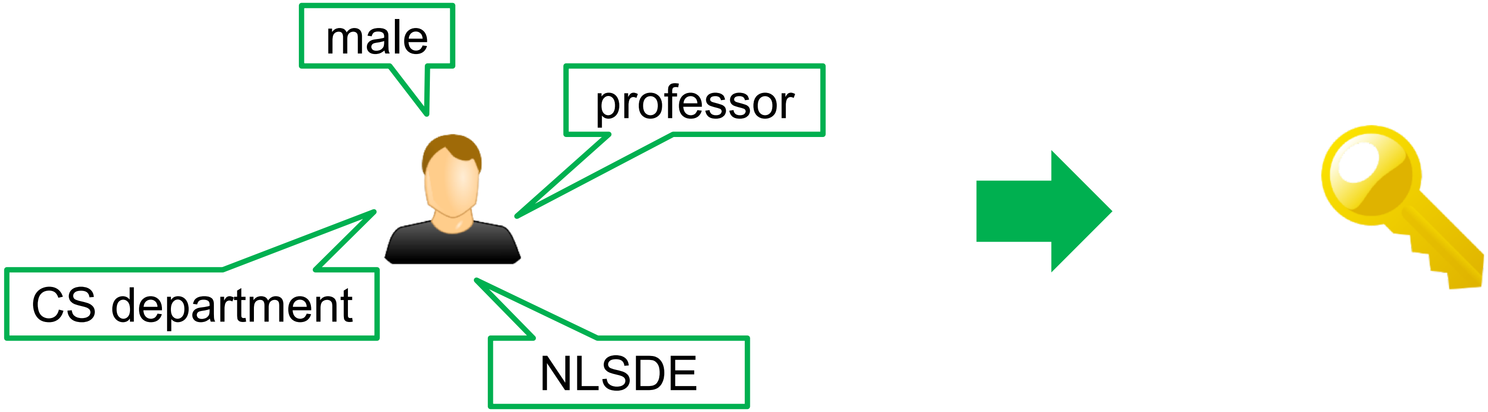
Background

➢ Identity Based Encryption

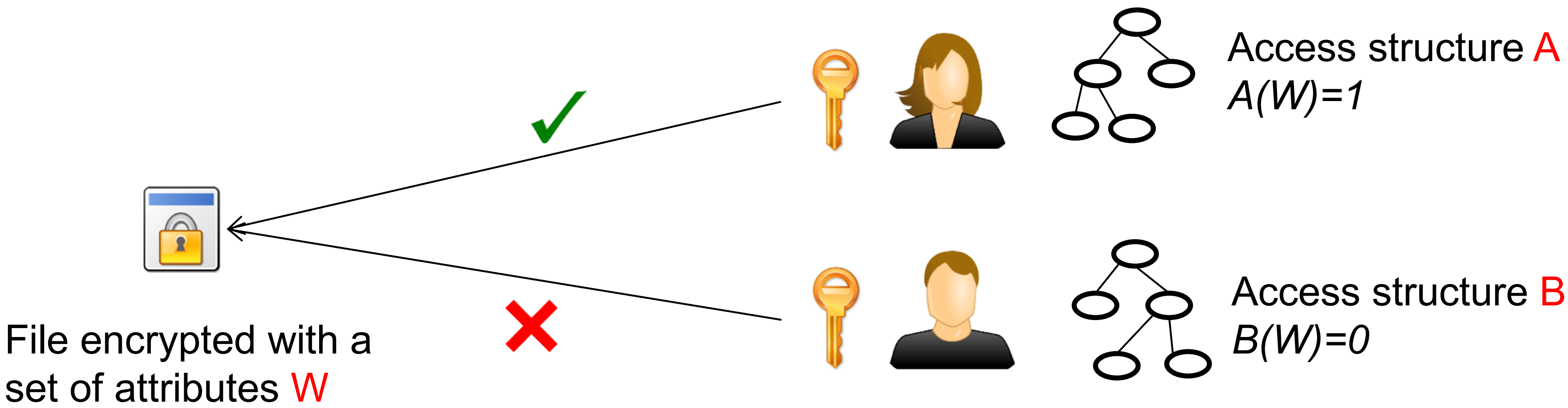


Background

- Attribute Based Encryption
  - ✓ An extend scheme of Identity based Encryption
  - ✓ Utilization of attribute information for Encryption/Decryption
  - ✓ Dynamically control the user group of the encrypted data

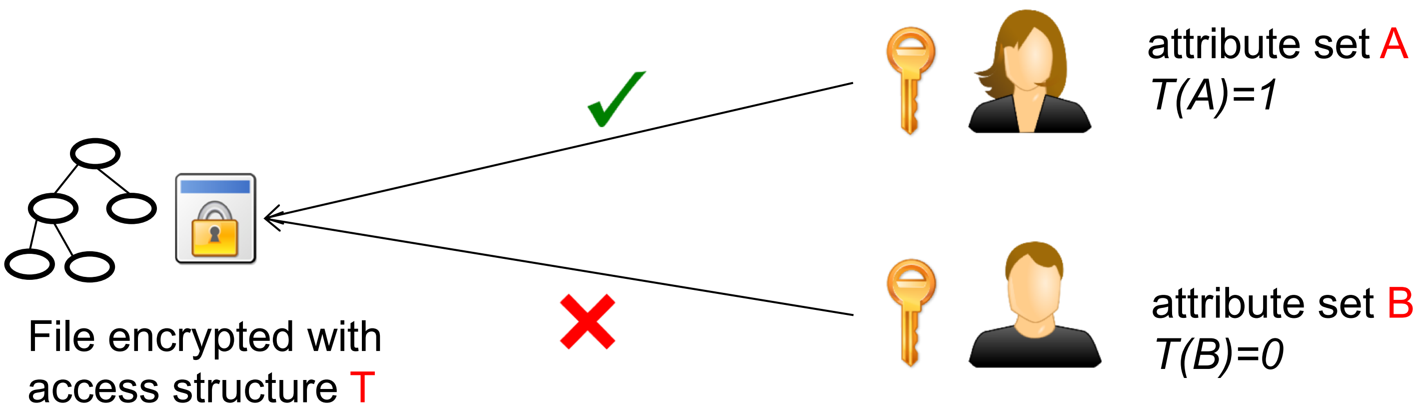


- Key Policy Attribute based Encryption (Goyal et al., 2006)



Background

- Ciphertext Policy Attribute based Encryption (Bethencourt et al., 2007)



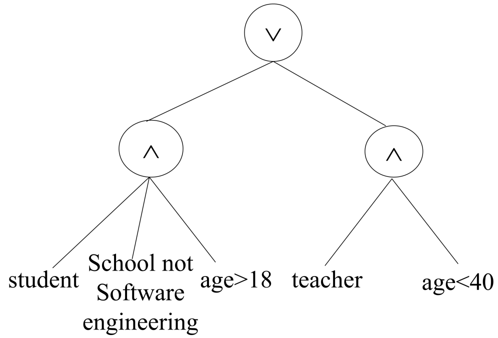
Background

CP-ABE
Access Structure

AND-gate

$$A_1 = (1 \wedge 2 \wedge 3 \wedge 4)$$

Tree



$$A_2 = (student \wedge school\ not\ SE \wedge age > 18) \vee (\text{teacher} \wedge \text{age} < 40)$$

LSSS matrix

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & -1 \\ 1 & 1 & 0 \end{pmatrix}$$

$$A_3 = (1 \wedge 2 \wedge 3) \vee (1 \wedge 4)$$

State Key Laboratory of Software Development Environment
xurunhua@nlsde.buaa.edu.cn

Background

- Original CP-ABE scheme
  - ✓ the access structure is embedded in the ciphertext
  - ✓ someone obtains the ciphertext can see the content of the access structure
- Privacy disclose
  - ✓ Full exposure of data’ s access policy will disclose sensitive information of the decryption or encryption party.

File encrypted with access structure T

Related Work

- CP-ABE Schemes
  - BSW07
    - The initial structure of CP-ABE
    - Security:
      - General group model rather than the standard numerical theoretical assumptions
    - Expressive ability : Tree Structure
      - AND, OR and threshold operations
      - “bag of bits” for express policies containing <, ≤, >, ≥
  - CN07
    - Security
      - CPA security under DBDH assumption
    - Expressive ability : AND-gate Structure
      - AND, NOT opeartions
  - Waters08
    - Expressive ability : LSSS matrix
    - Improvement of Lewko et al
      - supported any monotone access formula

Related Work

- CP-ABE Schemes
  - ✓ BCP-ABE
    - Security
      - CPA security under DBDH assumption
    - Expressive ability : Tree Structure
      - AND, OR and threshold operations
    - Improvement of Liang et al
      - Shorten the system's public key
      - Shorten the user's private key
      - Shorten the length of the ciphertext
  - ✓ ITHJ09
    - Security
      - CPA security under DBDH assumption
    - Expressive ability : Tree Structure
      - AND, OR and threshold operations
    - the costs of key generation, encryption and decryption are lower than BSW07

xurunhua@nlsde.buaa.edu.cn

Related Work

- CP-ABE Schemes with Hidden Policy
  - ✓ NYO08(Nishide et al, 2008)
    - Security
      - CPA security under DBDH assumption and D-Linear assumption
    - Access Structure:
      - Only support And-gate structure
  - ✓ LDL12(Lai et al, 2012)
    - Security
      - Fully secure in the standard model using the dual system encryption methodology .
    - Access Structure
      - LSSS Matrix structure
    - Partial hidden policy
  - ✓ XGRDY12(Xiaohui et al, 2012)
    - Security
      - CPA security under DBDH assumption in the standard model.
    - Access Structure
      - And-gate access structure

Related Work

- Conclusion
  - ✓ CP-ABE scheme with flexible policy expression ability will have broad application prospects.
  - ✓ XGRDY12 and LDL12 support the access structure hidden
    - And-gate access structure:
      - the expressive ability of policy is limited.
    - LSSS matrix structure:
      - It’s hard to construct the LSSS matrix
      - No normal method of construction.
  - ✓ The research of tree-based access structure CP-ABE scheme with hidden policy.

Our Contribution

Theorem:
Element's orthogonal property in subgroup of composite order bilinear groups

CP-ABE

Introduces some random elements into the policy key component.

ITHJ09 Scheme

CP-ABE-HP

State Key Laboratory of Software Development Environment
xurunhua@nlsde.buaa.edu.cn

CP-ABE-HP specific scheme

- **Initialize**
  - ✓ Generate public parameter *pk* and master key *mk*
    - Generate the bilinear groups G and a bilinear map $e: G \times G \rightarrow G_T$
      - G and G_T are the cyclic groups of order $N=pr$ (p and r are distinct primes)
      - G_p and G_r be the subgroup of the G with order p and r respectively.
      - Also g_p and g_r are the generator of G_p and G_r respectively.
    - Generate the attribute set U={$a_1, a_2, \ldots, a_n$}, and random elements $\alpha, t_1, t_2, \ldots, t_n \in Z_p^*$ and $R_0, R_1, R_2, \ldots, R_n \in G_r$
    - Compute the pk elements
      $$x = g_p \cdot R_0, y = e(g_p, g_p)^{\alpha}, T_j = g_p^{t_j} \cdot R_j (1 \le j \le n)$$
    - The public key is $pk = (e, x, y, T_j (1 \le j \le n))$, and the master key is $mk = (\alpha, t_j (1 \le j \le n))$.
  - ✓ Give *pk* to the encryption party.

CP-ABE-HP specific scheme

- **Encryption**
  - ✓ Select a random element $s \in Z_p^*$ and compute
    $$c_0 = x^s \cdot R_0', c_1 = m \cdot y^s = m \cdot e(g_p, g_p)^{\alpha s}$$
  - ✓ Set the value of the root node of τ to be s
  - ✓ Mark all child nodes as un-assigned, and mark the root node assigned
  - ✓ Recursively, for each un-assigned non-leaf node, do the following:
    - If its child nodes are un-assigned, the secret s is divided using (t,n)-Shamir secret sharing technique. The relation of n and t is:
      - if the symbol is of then $1 < t < n$;
      - if the symbol is AND, then $t = n$;
      - if the symbol is OR, then $t = 1$.
    - To each child node a share secret $s_i = f(i)$ is assigned , $f(x) = \sum_{j=0}^{t-1} b_j x^j$
    - Mark this node assigned.
  - ✓ For each leaf attribute
    $$\forall a_{j,i} \in \tau, c_{j,i} = T_j^{s_i} \cdot R_j'$$
  - ✓ Return the ciphertext: $c_\tau = (c_0, c_1, \forall a_{j,i} \in \tau : [i, c_{j,i}])$.

CP-ABE-HP specific scheme

Secret key generation

- Verify the basic attribute
- Generate the secret key sk_{w*} corresponds to w^*
  - Select a random value $r \in Z_p^*$, $d_0 = g^{\alpha - r}$.
  - For each attribute a_j in w, compute $d_j = g^{rt_j^{-1}}$
- Send key back to the user

Decryption

- For every attribute element $a_j \in w'$, computing:

$$m = \frac{c_1}{e(c_0, d_0) \cdot \prod_{a_j \in w'} e(c_{j,i}, d_j)^{l_i(0)}}$$

- $l_i(0)$ is a Lagrange coefficient.

xurunhua@nlsde.buaa.edu.cn

CP-ABE-HP specific scheme

- **Correctness Proof:**

$$m' = \frac{c_1}{e(c_0, d_0) \cdot \prod_{a_j \in w} e(c_{j,i}, d_j)^{l_i(0)}}$$

$$= \frac{m \cdot e(g_p, g_p)^{\alpha s}}{e(g_p^s, g_p^{\alpha - r}) \cdot e(R_0^s \cdot R_0^{'}, g_p^{\alpha - r})} \cdot \frac{1}{\prod_{a_j \in w} (e(g_p^{t_j s_i}, g_p^{r t_j^{-1}})^{l_i(0)} \cdot e(R_j^{s_i} \cdot R_j^{'}, g_p^{r t_j^{-1}})^{l_i(0)})}$$

$$= \frac{m \cdot e(g_p, g_p)^{\alpha s}}{e(g_p^s, g_p^{\alpha - r}) \cdot e(g_p, g_p)^{\sum r s_i l_i(0)}}$$

$$= \frac{m \cdot e(g_p, g_p)^{\alpha s}}{e(g_p^s, g_p^{\alpha - r}) \cdot e(g_p, g_p)^{rs}}$$

$$= m$$

CP-ABE-HP Performance analysis

Table Comparison of our scheme with other schemes in computing cost

Scheme	Access Structure	Hidden Policy	Encrypt	Decrypt
CN07	And-gate	N	$(n+1)G+2G_t$	$(n+1)C_e+(n+1)G_t$
Emura09	And-gate	N	$(n+1)G+2G_t$	$2C_e+2G_t$
Xiao12	And-gate	Y	$(n+3)G+2G_t$	$2C_e+2G_t$
BSW07	Tree	N	$(2\|A_c\|+1)G+2G_t$	$2\|A_u\|C_e+(2\|S\|+2)G_t$
ITHJ09	Tree	N	$(\|A_c\|+1)G+2G_t$	$(\|w\|+1)C_e+(\|w\|+1)G_t$
CP-ABE-HP	Tree	Y	$2(\|A_c\|+1)G+2G_t$	$(\|w\|+1)C_e+(\|w\|+1)G_t$

CP-ABE-HP Security Model

- IND-sAtt-CPA game
  - ✓ Init Phase.
    - The adversary chooses a challenge access tree τ^* and gives it to the challenger.
  - ✓ Setup Phase.
    - The challenger runs Setup algorithm to generate (*PK*, *MK*) and gives the public key *PK* to adversary *A*.
  - ✓ Phase 1.
    - Adversary *A* makes a secret key request to the key generation oracle for any attribute sets. The challenger runs Key-Generation (*MK*, *S*) algorithm to generate a private key.
  - ✓ Challenge Phase.
    - Adversary *A* sends to the challenger two equal length messages m_0, m_1. The challenger picks a random bit $b \in \{0, 1\}$ and returns c_b = Encrypt (m_b, τ^*, *PK*).
  - ✓ Phase 2.
    - Adversary *A* can continue querying key generation oracle with the same restriction as in Phase 1.
  - ✓ Guess Phase.
    - Adversary *A* outputs a guess $b' \in \{0, 1\}$.

CP-ABE-HP Security Proof

- DBDH assumption
  - ✓ No probabilistic polynomial-time algorithm β can distinguish the tuple $(g, g^a, g^b, g^c, e(g, g)^{abc})$ from the tuple $(g, g^a, g^b, g^c, e(g, g)^z)$ with more than a negligible advantage.
- Methodology
  - ✓ Suppose that the IND-sAtt-CPA game can be won by an adversary A with a non-negligible advantage ε.
  - ✓ From the attack ability of adversary A, we will build a simulator β, which has the ability to solve the DBDH assumption problem with advantage $\varepsilon/2$.
  - ✓ According to the DBDH assumption: there are no effective polynomial algorithms which can solve the DBDH assumption problem with non-negligible advantage.
  - ✓ The adversary also cannot win the IND-sAtt-CPA game with the above advantage ε.
- Conclusion:
  - ✓ the adversary having no advantage to break through CP-ABE-HP system

CP-ABE-HP Security Proof

- Proof
  - Init Phase.
    - The adversary chooses a challenge access τ^* and sends it to the challenger.
  - Setup Phase.
    - The challenger selects a random element $x' \in Z_p$ and sets α = $ab + x'$, then calculates pk:

$$x = g_p \cdot R_0$$

$$y = e(g_p, g_p)^{\alpha} = e(g_p, g_p)^{ab} e(g_p, g_p)^{x'}$$

$$\forall a_j \in U : T_j = \begin{cases} g_p^{b/t_j} \cdot R_j, a_j \notin \tau^* \\ g_p^{t_j} \cdot R_j, a_j \in \tau^* \end{cases}, (1 \le j \le n)$$

  - Phase 1
    - The adversary sends a user private key query request to the challenger by the following attributes set:

$$w_j = \{a_j \mid a_j \in \Omega\}, (a_j \notin \tau^*)$$

    - For each query request of the adversary, the challenger selects random element $r' \in_R Z_p$ and sets $r = ab + br'$ and calculates private key:

$$d_0 = g_p^{\alpha-(ab+r'b)} = g_p^{x'-r'b} = g_p^{x'}(g_p^{b})^{-r'} \qquad d_j = g_p^{rt_j/b} = (g_p^{a})^{t_j} g_p^{r't_j}, (a_j \notin \tau^*)$$

State Key Laboratory of Software Development Environment
xurunhua@nlsde.buaa.edu.cn

CP-ABE-HP Security Proof

- Proof
  - Challenge Phase.
    - The adversary submits two plaintext messages m_0, m_1 to the challenger.
    - The challenger selects a random plaintext message m_b from the two messages, where b$\in_R${0,1}. Encrypt the message as follows:

$$c_0 = g_p^c \cdot R_0^c \cdot R_0^{'}$$

$$c_1 = m_b e(g_p, g_p)^{abc} e(g_p^c, g_p^{x'})$$

    - Use the Shamir Secret Sharing scheme over the access tree.
  - Phase 2.
    - The adversary continues to send the secret key requests to the challenger with the same restriction as in Phase 1.
  - Guess Phase.
    - The adversary outputs a guess $b' \in \{0, 1\}$.
    - If $b' = b$, the challenger can guess that $u = 0$, $Z_u = e(g_p, g_p)^{abc}$.

$$\Pr[b' = b \mid Z_u = e(g_p, g_p)^{abc}] = 1/2 + \varepsilon$$

    - Otherwise, the challenger guesses that $u = 0$, $Z_u = e(g_p, g_p)^{\theta}$.

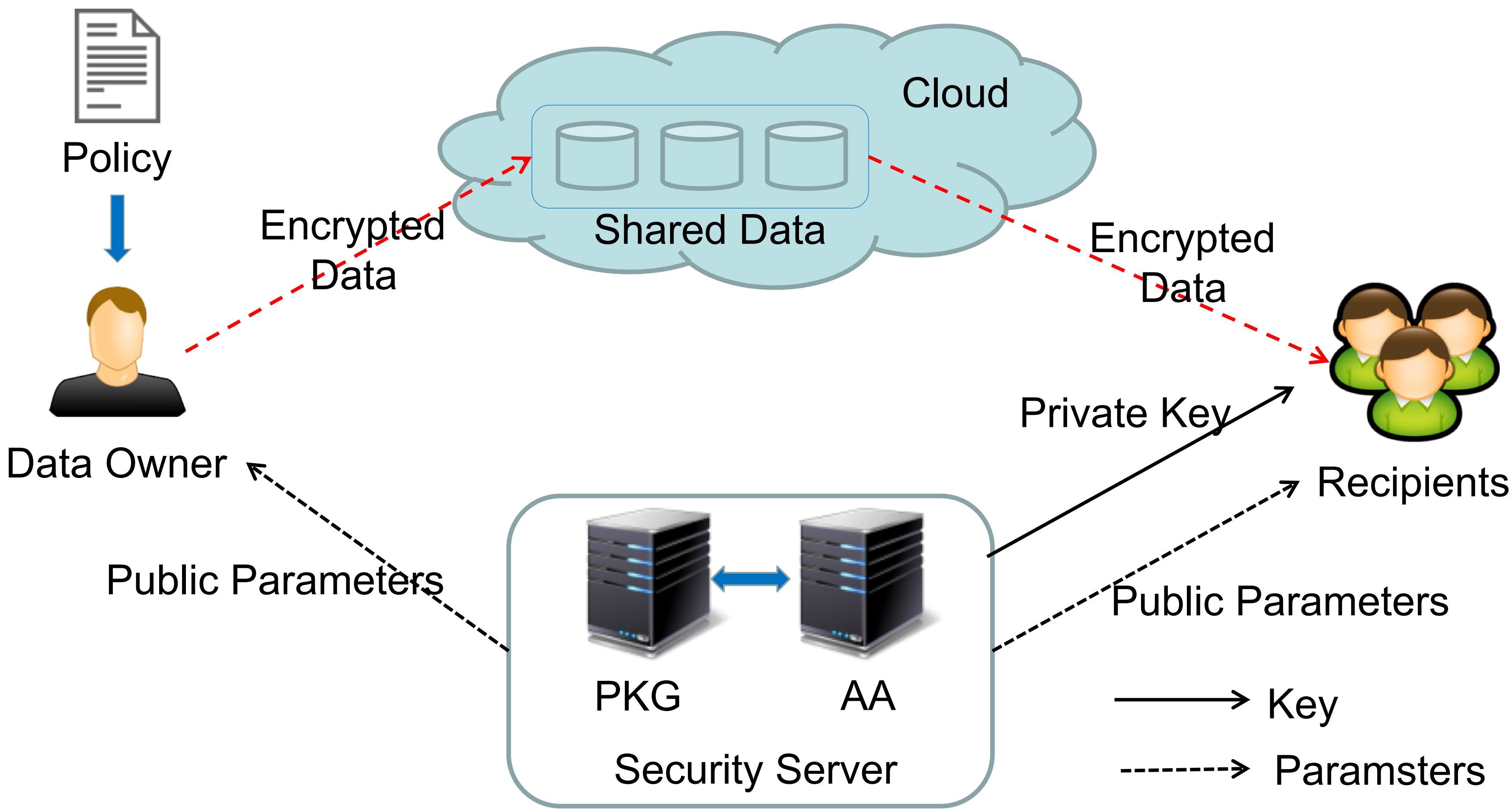
$$\Pr[b' \neq b \mid Z_u = e(g_p, g_p)^{\theta}] = 1/2$$

$$\frac{1}{2}\Pr[u' = u \mid u = 0] + \frac{1}{2}\Pr[u' = u \mid u = 1] - \frac{1}{2} = \frac{\varepsilon}{2}$$

State Key Laboratory of Software Development Environment
xurunhua@nlsde.buaa.edu.cn

An implementation framework

The implementation framework of CP-ABE-HP scheme for outsourced data sharing



State Key Laboratory of Software Development Environment
xurunhua@nlsde.buaa.edu.cn

Conclusion

- Propose an CP-ABE-HP scheme
  - Introduces the tree-based CP-ABE scheme with hidden policy
    - Keep the security and efficiency properties of the CP-ABE scheme
    - Preserve the privacy in the access policy
- Future work
  - Implement an efficient CP-ABE-HP mechanism
  - Apply it to some specific cloud storage environments

xurunhua@nlsde.buaa.edu.cn

北京航空航天大學
Beihang University

Thank you!
Q & A

xurunhua@nlsde.buaa.edu.cn