9th Annual National Cyber Summit

University of Pittsburgh
School of Information Sciences

Insider Threat Mitigation in Attribute based Encryption

National Cyber Summit, June 8, 2017

Runhua Xu, James Joshi, Prashant Krishnamurthy, David Tipper

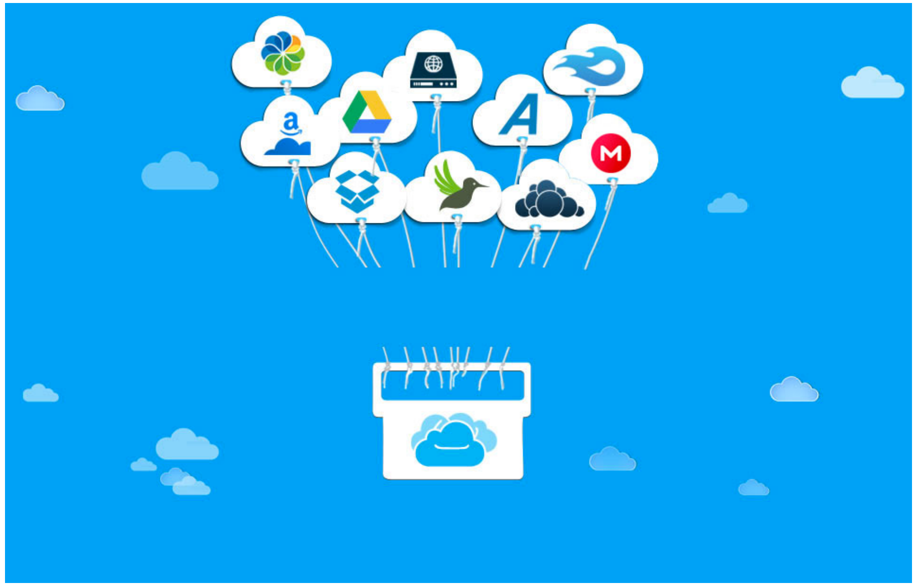
University of Pittsburgh

(jjoshi@pitt.edu)

The **L**aboratory for **E**ducation and **R**esearch on **S**ecurity **A**ssured **I**nformation **S**ystems (**LERSAIS**)

Cloud Computing/Storage Service

❖It has been gaining significant success
- *potential "infinite" storage size*
- *convenience of synchronization*
- *ease of access (at anytime, from anywhere)*



❖Users/Organizations
- *increasingly utilize/rely on the cloud storage services*

Security & Privacy Concerns

Cloud Storage Providers

Honest-but-Curious

-- run the programs and algorithms correctly,

-- but gather information related to the stored data.

A Solution

- *Confidentiality for data*
- *Fine-grained access control for data*

Initial Requirement

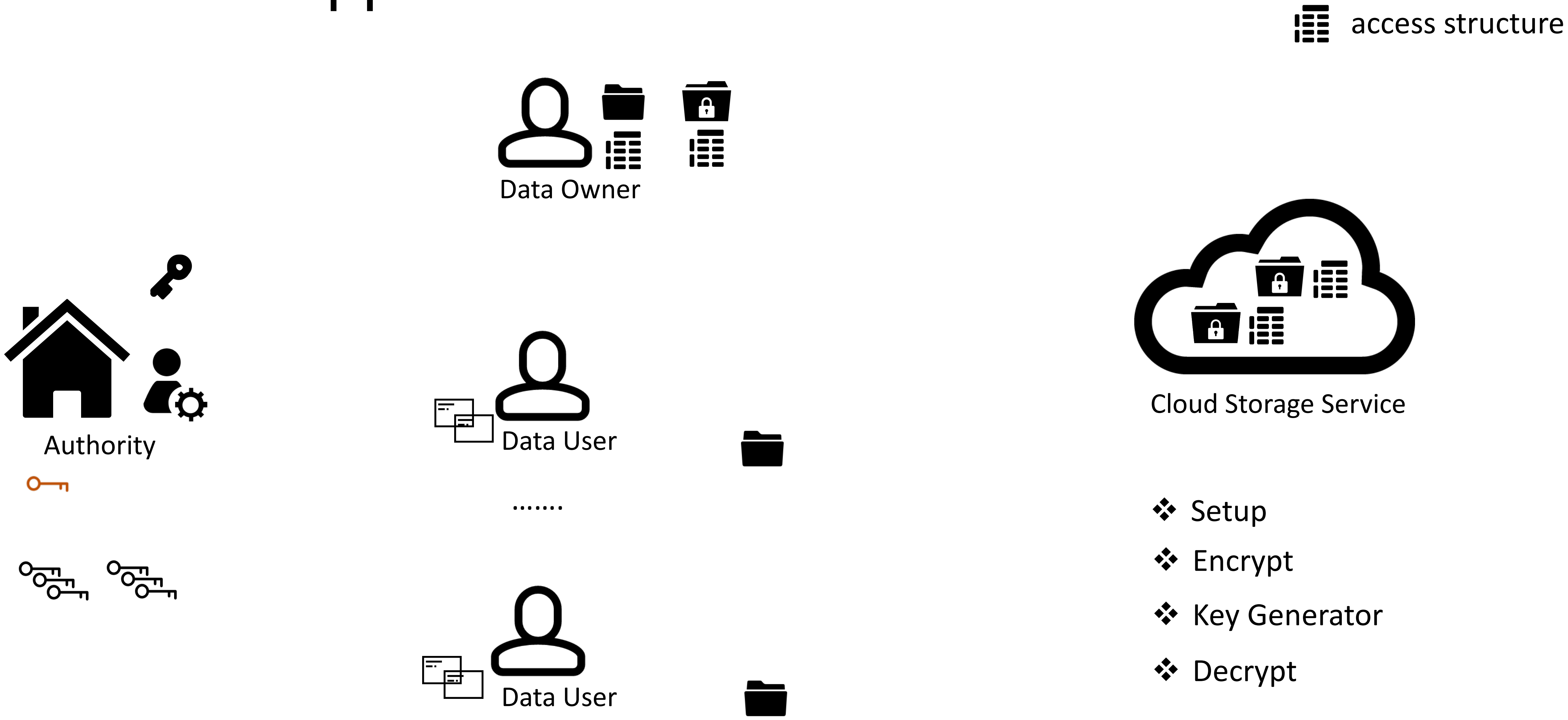
Ciphertext Policy Attribute Based Encryption

- *Combination of encryption and access control*
- *Useful for access scenario in cloud storage*

Data → self-protection feature / abilitity

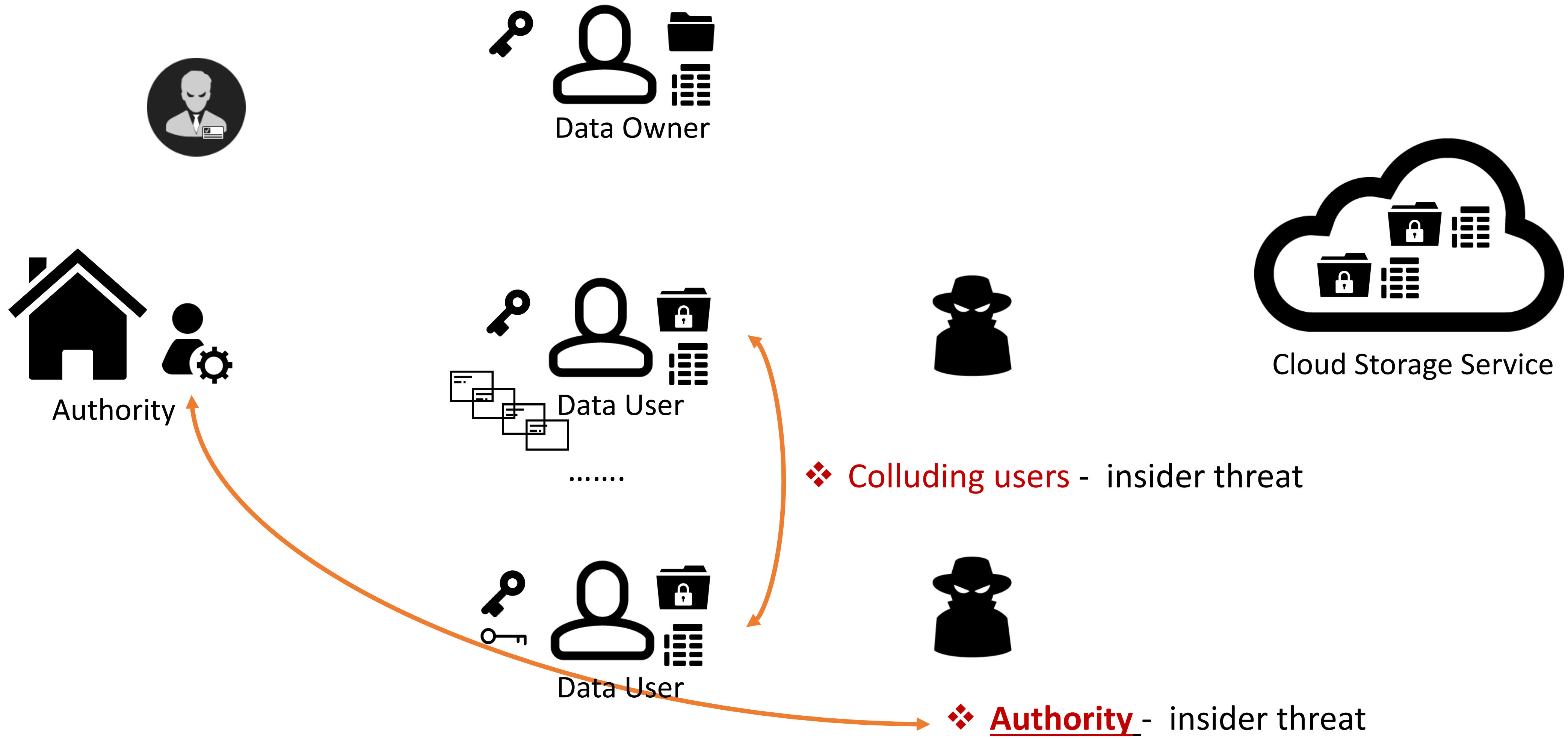
*Bethencourt John, Amit Sahai, and Brent Waters. "Ciphertext-policy attribute-based encryption." *2007 IEEE symposium on security and privacy (S&P'07)*. IEEE, 2007.

Overview of application



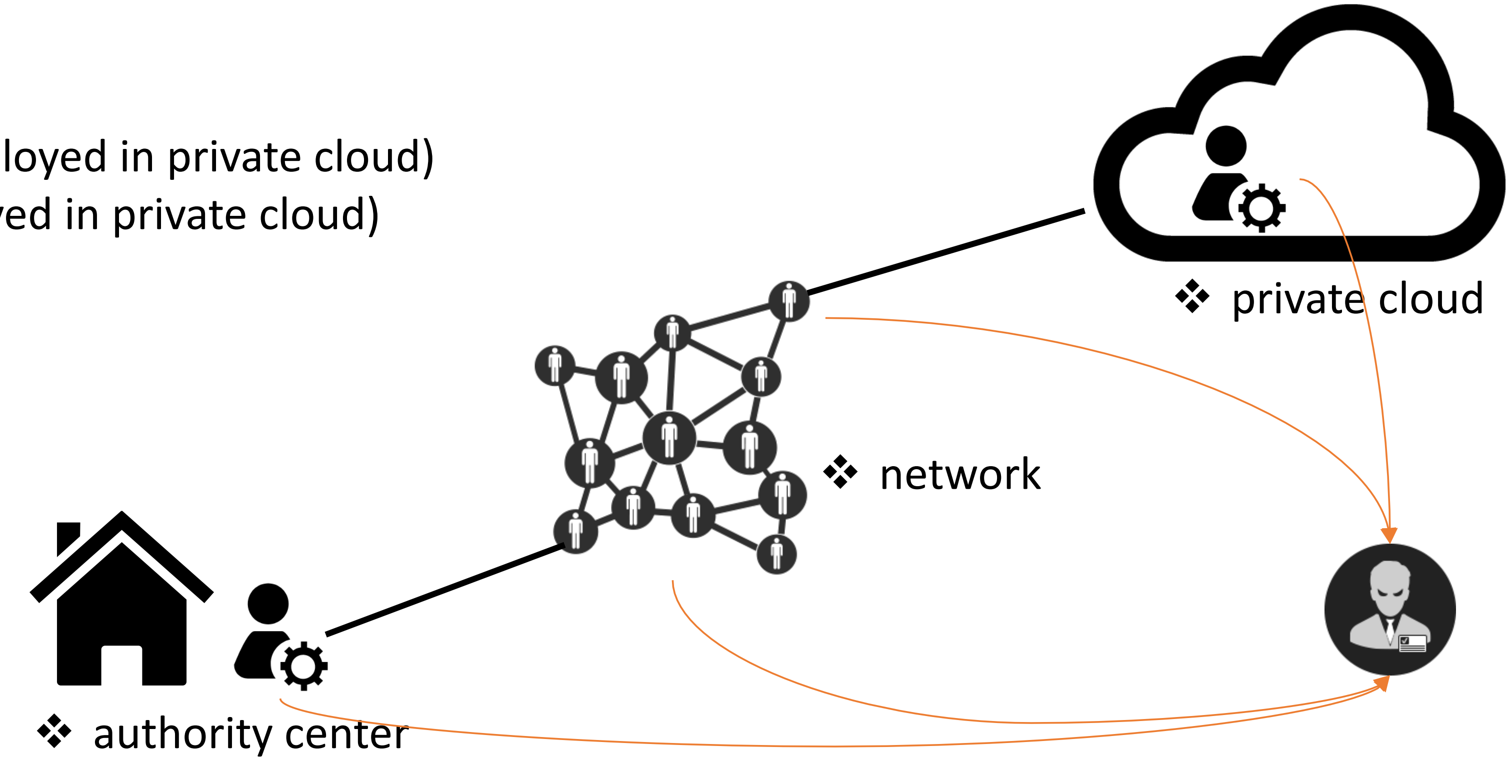
- Setup
- Encrypt
- Key Generator
- Decrypt

Two Types of Insider in ABE

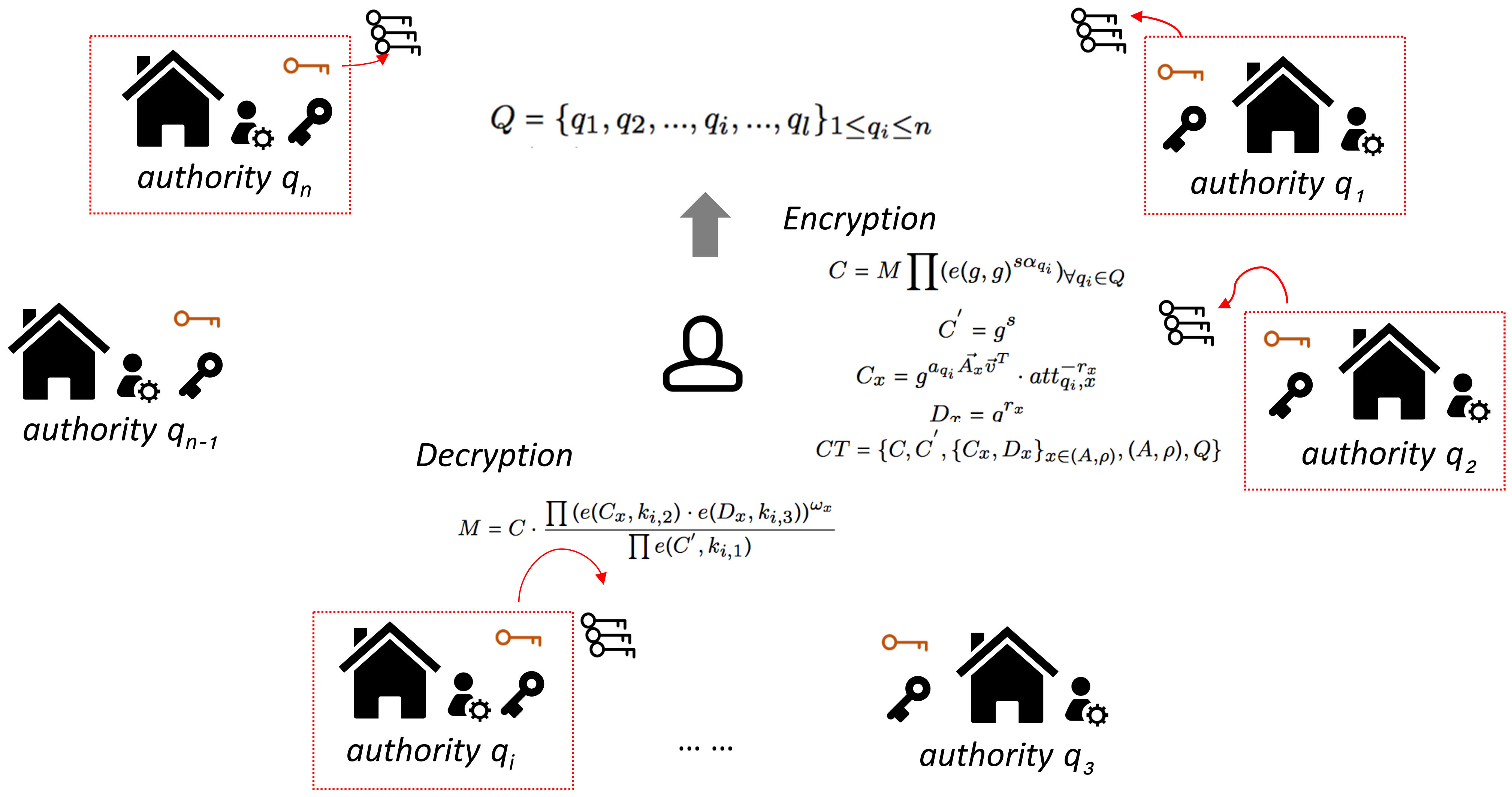


Authority as Insider threat

- Potential Insiders
  - system administrator
  - attribute authenticator
  - other employees
  - network administrator (if deployed in private cloud)
  - cloud administrator (if deployed in private cloud)



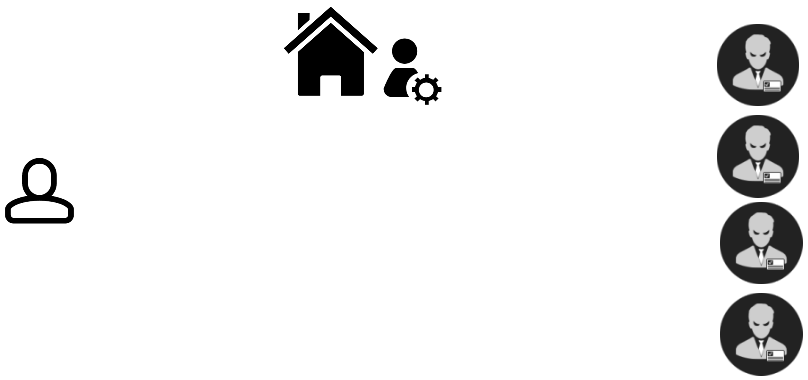
Multi-Authority CP-ABE



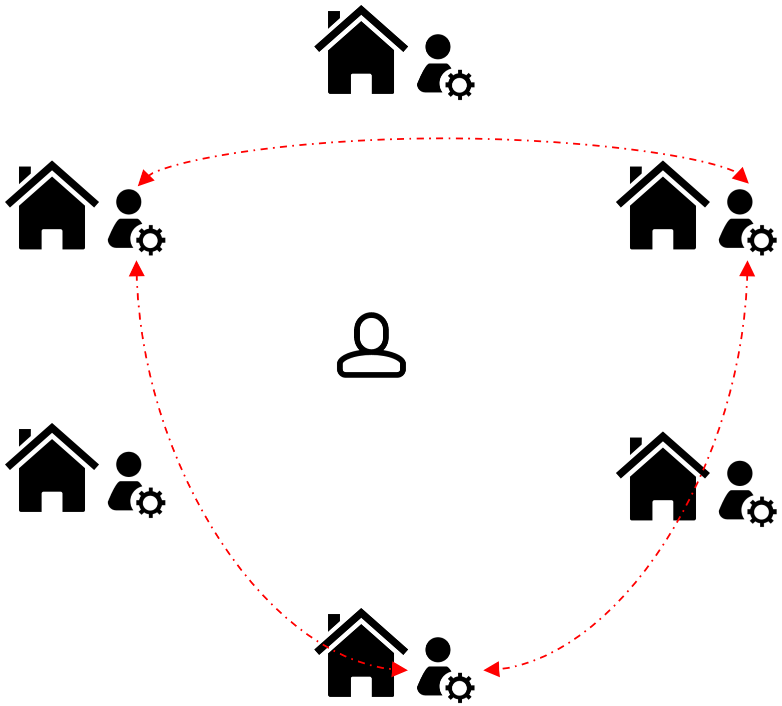
Insider Threat Mitigation Solutions

Two specific insider threat issues in Authority

- ❖ single authority as a threat
  - ❖ MA-CP-ABE removes that



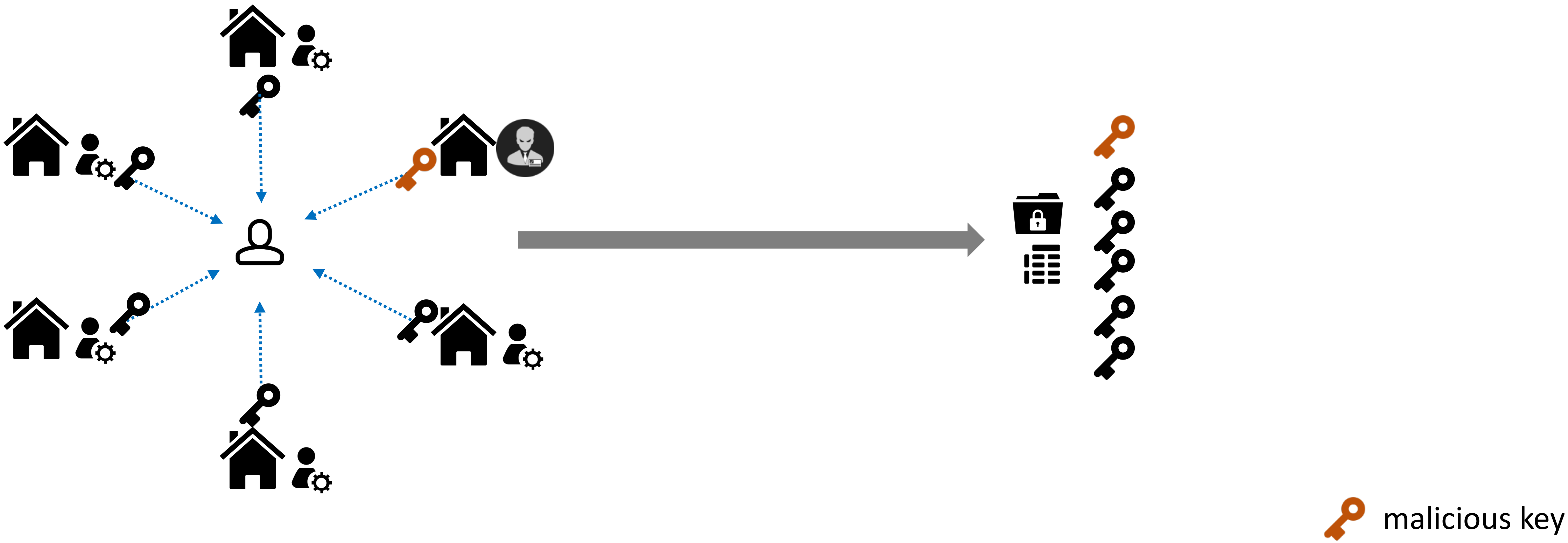
- ❖ with insiders' collusion: different authorities



Insider Threat Mitigation Solutions

single authority as insider

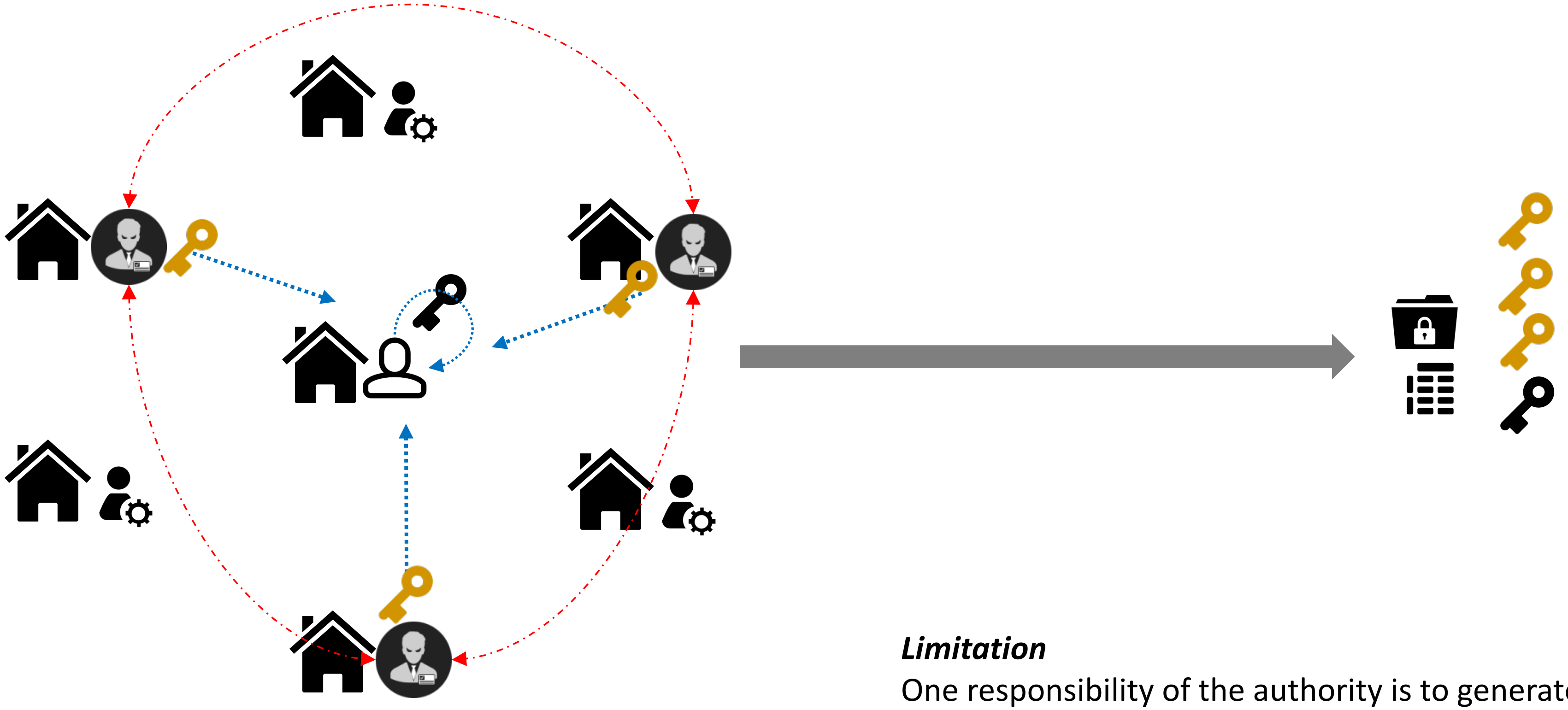
❖ multi-authority scheme can directly prevent the insider's attack from a single authority.



Insider Threat Mitigation Solutions

Collusion among different authorities

***I_N tolerance**: self-authority, the data owner can play as an ABE authority itself*



Limitation

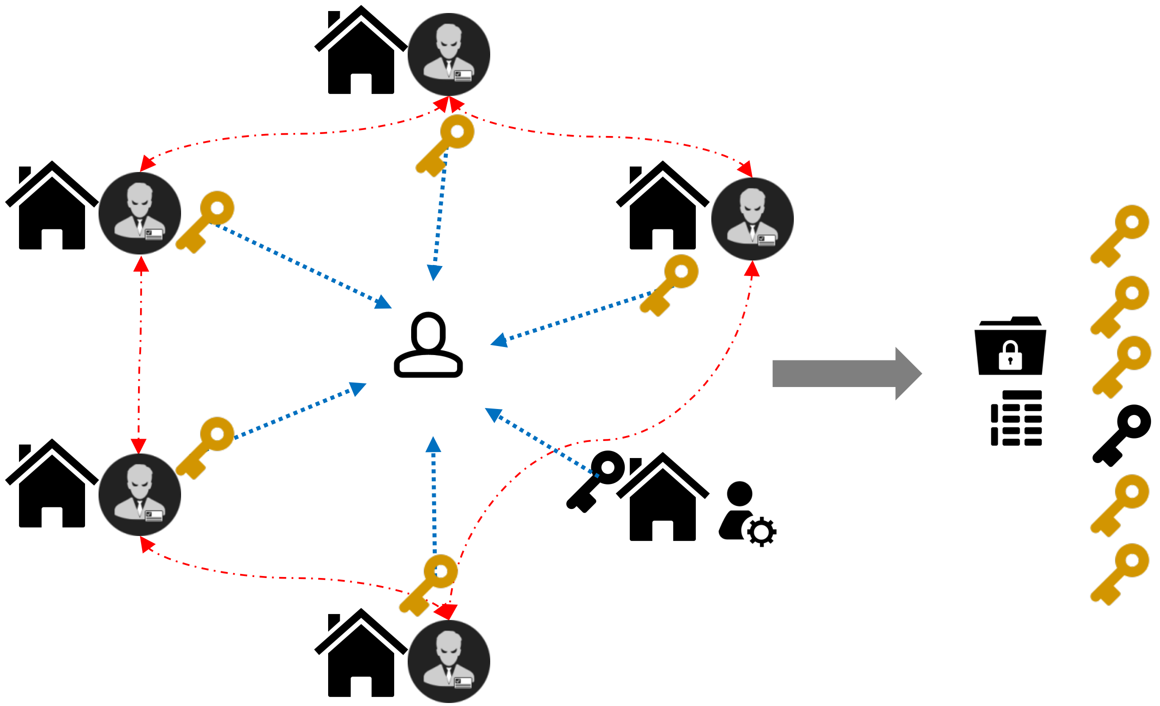
One responsibility of the authority is to generate the users' private keys

→the self-authority should be available when the data user needs the key services.

Insider Threat Mitigation Solutions

ollusion among different authorities posing insider threat

I_{N-1}* tolerance: resist at most N – 1 insiders among the N authorities*



$$Q = \{q_1, q_2, \ldots, q_i, \ldots, q_l\}_{1 \le q_i \le n}$$

Algorithm 1 The sequence Q generating algorithm.

Input: the number of attributes in the access structure l; the number of authorities N; the identity set of authorities $S_{\mathcal{A}}$.

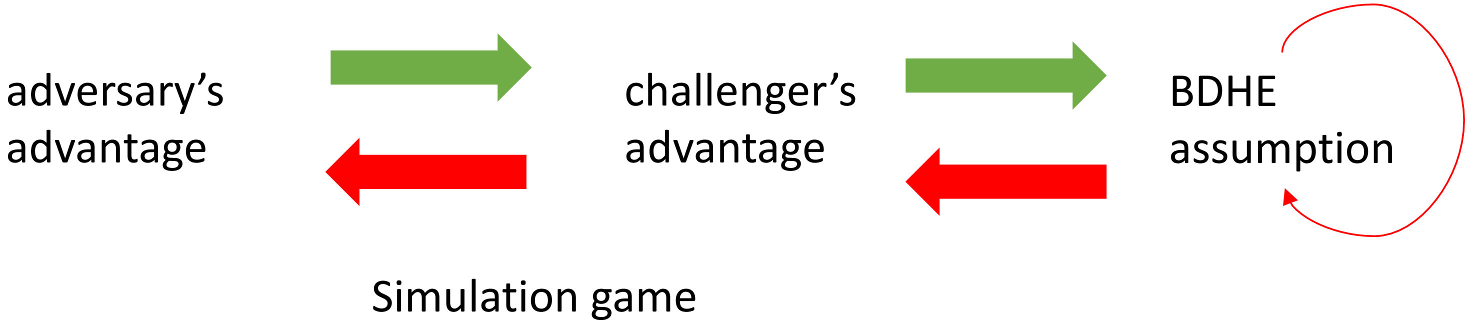
Output: the generated sequence Q.

```
if l ≥ N then
    Q_A ← select all identities from S_A.
    Q_rest ← randomly select l − N identities from S_A.
    Q ← Q_A ∪ Q_rest
    Shuffle the Q.
else
    Q ← randomly select l identities from S_A.
    Shuffle the Q
end if
return Q
```

Security Analysis

Security of MA-CP-ABE

- Simulation game [4,12]
  - Setup
  - Secret Key Queries
  - Challenge
  - More Secret Key Queries
  - Guess



- The adversary tries to break the scheme

- Insider Tolerance Analysis

- Complexity Analysis

Table 1: Comparison of efficiency

schemes	Our scheme	[8]
Encryption	$(4l+1)\mathcal{C}_{exp}$	$(4\|i\|+1)\mathcal{C}_{exp} + \|l\|\mathcal{C}_{map}$
Decryption	$3\|S\|\mathcal{C}_{map} + \|S\|\mathcal{C}_{exp}$	$3\|S\|\mathcal{C}_{map} + 3\|S\|\mathcal{C}_{exp}$

[1] Let $|\mathcal{C}_{exp}|$, $|\mathcal{C}_{map}$ be the calculation of exponent and bilinear map over $\mathcal{G}$, respectively.
[2] l is the attribute number in the access structure, and $|S|$ is the minimum set of users' attributes.

[8] Allison Lewko and Brent Waters. 2011. Decentralizing attribute-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 568–588.

Conclusion

- Cloud computing/storage services are increasingly used
- Data confidentiality and Access control are among primary issues
- CP-ABE is useful in addressing both Data confidentiality and access control issues
- Authority needs to be trusted – hence can pose as insider threat
- MA-CP-ABE scheme proposed addresses the Authority as insider threat agent
    - Two schemes
    - Complexity of the scheme is better than that of another existing scheme

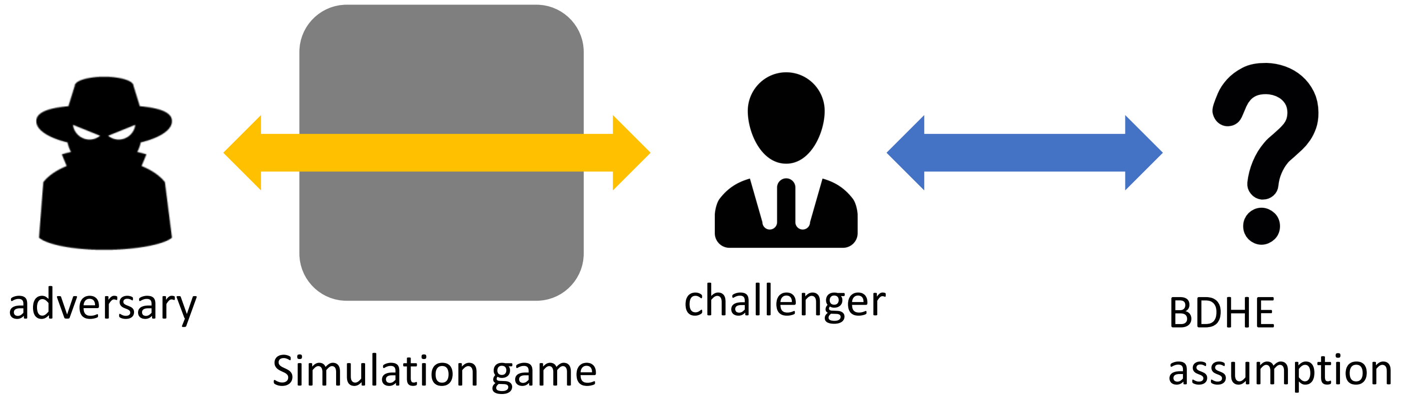
Acknowledgement:
This work was supported by NSA cybersecurity grant

Thanks!
Questions?

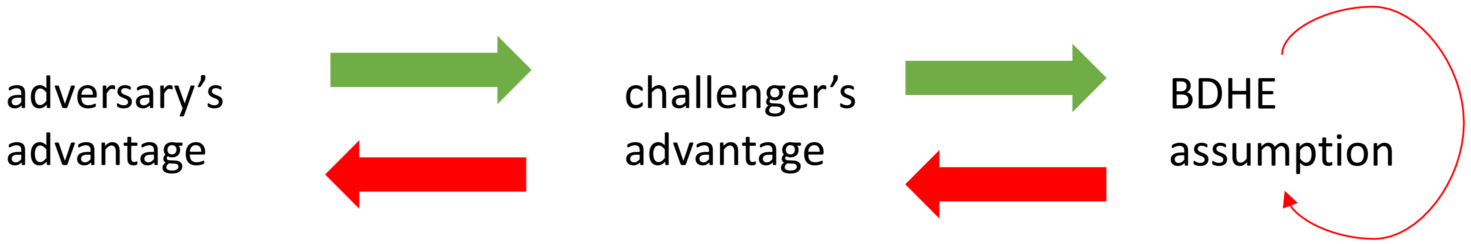
Security Analysis

Security of MA-CP-ABE

❖ Simulation game [4,12]
  - ❖ Setup
  - ❖ Secret Key Queries
  - ❖ Challenge
  - ❖ More Secret Key Queries
  - ❖ Guess



- The adversary tries to break the scheme
- The challenger tries to solve the mathematical hard problem by taking the advantage of the adversary



Complexity Analysis and Correctness

The complexity of our proposed MA-CP-ABE scheme

Table 1: Comparison of efficiency

schemes	Our scheme	[8]
Encryption	$(4l+1)\mathcal{C}_{exp}$	$(4\lvert i\rvert+1)\mathcal{C}_{exp}+\lvert l\rvert\mathcal{C}_{map}$
Decryption	$3\lvert S\rvert\mathcal{C}_{map}+\lvert S\rvert\mathcal{C}_{exp}$	$3\lvert S\rvert\mathcal{C}_{map}+3\lvert S\rvert\mathcal{C}_{exp}$

[1] Let $|\mathcal{C}_{exp}|$, $|\mathcal{C}_{map}$ be the calculation of exponent and bilinear map over $\mathcal{G}$, respectively.

[2] l is the attribute number in the access structure, and $|S|$ is the minimum set of users' attributes.

[8] Allison Lewko and Brent Waters. 2011. Decentralizing attribute-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 568–588.

Correctness inference

$$T = \frac{\prod_{i\in Q} e(C', k_{i,1})}{\prod_{i\in Q, x\in I}(e(C_x,k_{i,2})e(D_x,k_{i,3}))^{\omega_x}}$$

$$= \frac{\prod_{i\in Q} e(g^s, g^{\alpha_i}\cdot g^{a_i t_i})}{\prod_{i\in Q,x\in I}(e(g^{a_i \vec{A}_x \vec{v}^T}\cdot att_{i,x}^{-r_x}, g^{t_i})e(g^{r_x}, att_{i,j}^{t_i})))^{\omega_x}}$$

$$= \frac{e(g,g)^{\sum_{i\in Q} s(\alpha_i+a_i t_i)}}{e(g,g)^{\sum_{i\in Q}(a_i t_i \sum_{x\in I}\vec{A}_x\vec{v}^T\omega_x)}}$$

$$= \frac{e(g,g)^{\sum_{i\in Q} s(\alpha_i+a_i t_i)}}{e(g,g)^{\sum_{i\in Q} a_i t_i s}}$$

$$= e(g,g)^{\sum_{i\in Q} s\alpha_i}$$

Then the message M could be recovered as follows:

$$\frac{C}{T} = \frac{M\prod(e(g,g)^{s\alpha_{q_i}})_{q_i\in Q}}{e(g,g)^{\sum_{i\in Q} s\alpha_i}} = \frac{Me(g,g)^{\sum_{q_i\in Q} s\alpha_i}}{e(g,g)^{\sum_{i\in Q} s\alpha_i}} = M$$