# Large Universe Ciphertext-Policy Attribute-Based Encryption with White-Box Traceability

**Jianting Ning**

Shanghai Jiao Tong University, Shanghai, China

**Joint work with Zhenfu Cao, Xiaolei Dong, Lifei Wei, and Xiaodong Lin**

Accepted by the 19th European Symposium on Research in Computer Security (ESORICS) 2014

# Outline

- ❑ Introduction
- ❑ Related Work
- ❑ Motivation
- ❑ Our Results
- ❑ Our construction
- ❑ Extensions
- ❑ Future Work

# Introduction: What is CP-ABE?

- CP-ABE is a tool for implementing fine-grained access control over encrypted data, and is conceptually closer to traditional access control methods such as Role-Based Access Control.
- A user is described by a set of descriptive attributes, and a corresponding private key is issued by an authority according to the attributes the user possess.
- During encryption, an encryptor associates an access policy over attributes with the ciphertext.
- A user will only be able to decrypt a ciphertext if that user's attributes pass through the ciphertext's access structure.

# Introduction: What is CP-ABE?

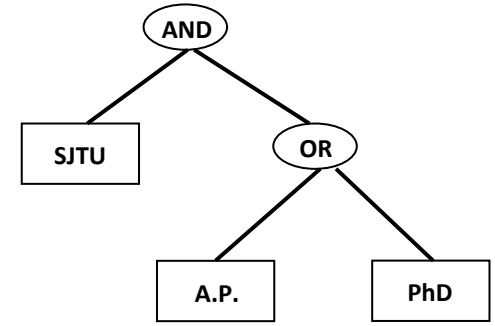
$PK$

$PK{\downarrow}SJTU$, $PK{\downarrow}THU$, …
$PK{\downarrow}CS$, $PK{\downarrow}EE$, …
$PK{\downarrow}A.P.$, $PK{\downarrow}PhD$, …
$PK{\downarrow}M$, $PK{\downarrow}F$, …
……
…..

$MSK$

Univ.: SJTU, THU, …
Dept.: CS, EE, …
Type: Assi. Prof., PhD Stud., …
Gender: Male, Female
……
……

$C=Enc(PK,\mathcal{P},M)$




$\mathcal{P}=SJTU\ AND\ (A.P.\ OR\ PhD)$

Storage Server
(Untrusted)

$SK{\downarrow}S{\downarrow}A$

$S{\downarrow}A$ satisfies $\mathcal{P}$

$S{\downarrow}A=\{SJTU, PhD\}$

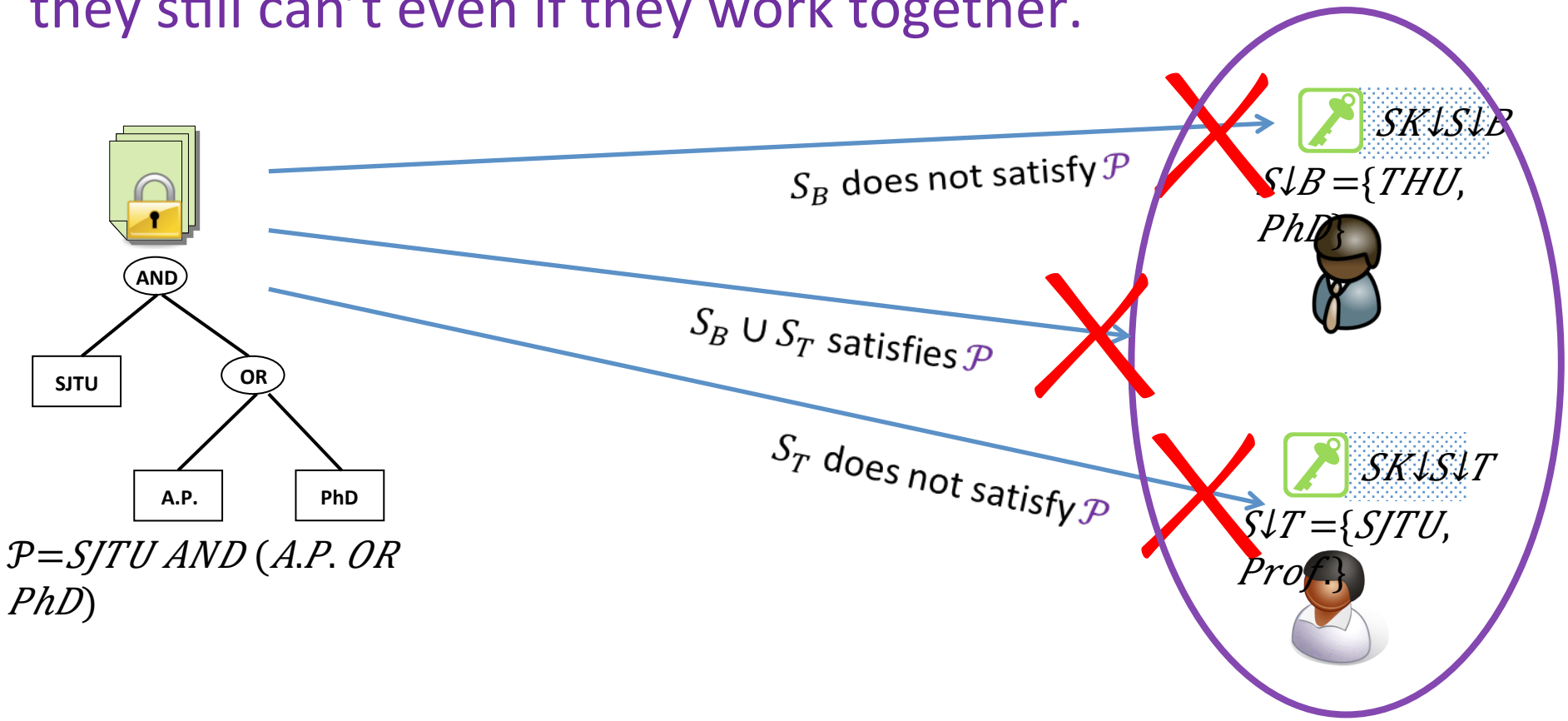
$S{\downarrow}B$ does not satisfy $\mathcal{P}$

$S{\downarrow}B=\{THU, PhD\}$

$SK{\downarrow}S{\downarrow}B$

# Introduction: What is CP-ABE?
# -- Collusion-resistant

If none of the users can decrypt a ciphertext individually, they still can't even if they work together.



# Introduction: What is CP-ABE? -- Definition

- $Setup(1\lambda, U) \longrightarrow pp, msk.$
- $Encrypt(1\lambda, pp, \mathcal{P}, m) \longrightarrow ct.$ $\mathcal{P}$ is implicitly included in $ct.$
- $KeyGen(1\lambda, pp, msk, S) \longrightarrow SK{\downarrow}S$ .
- $Decrypt(1\lambda, pp, SK{\downarrow}S, ct) \longrightarrow m$ $or \perp$. If and only if $S$ satisfies $\mathcal{P}$, $m$ can be recovered.

# Introduction: Why needs T-LU-CP-ABE? -- A Motivating Story

- ✓ Consider a commercial application such as a pay-TV system with huge number of users
  - ❖ Each user is labeled lots of related attributes (which are defined as the TV channels that the user have ordered).
  - ❖ Those who have paid for the TV channels could satisfy the access policy to decrypt the ciphertext and enjoy the ordered TV channels.

- ✓ There appears two problems as following
  - ❖ If someone buys the decryption key from the Internet at a lower cost, she/he could get access to the TV channels. Then who is selling the decryption key?
  - ❖ As the TV channels expand, an increasing number of new attributes need to be added. If the number of the attributes exceeds the bound set during the initial deployment of the pay-TV system, then the entire system has to be re-deployed and possibly all its data have to be re-encrypted.

# Introduction: Why needs T-LU-CP-ABE? -- Analysis

- ✓ Due to the nature of CP-ABE, it is difficult to find out the original key owner from an exposed key since the decryption key is shared by multiple users who have the same attributes
  - ❖ It is necessary f… e malicious users who intentionally le… tion keys.

traceability is required !

- ✓ In previous CP-ABE constructions, the attributes are fixed at system setup and the number of the attributes are bounded
  - ❖ If the bound is not specified large enough, the attributes may exhaust.
  - ❖ If the bound is … e the storage and communicatio… e to the corresponding increase of the …
  - ❖ Thus, it is necessary for the pay-TV system to support flexible number of attributes.

large universe is required !

# Related Work: Existing ABE Schemes

- ✓ Sahai et al. [SW05]: introduce ABE, but only for "threshold policies".
- ✓ Goyal et al. [GPSW06]: the CP-ABE notion.
- ✓ Bethencourt et al. [BSW07] : The first CP-ABE scheme.
- ✓ … …
- ✓ Many advances have been made for ABE as the following directions:
  - ❖ New proof techniques to obtain fully secure [LW10,OT10,LOSTW10,LW12];
  - ❖ Decentralizing trust by setting multiple authorities [Chase07, CC09, LW11];
  - ❖ Outsourcing computation [PRV12, GHW11];
  - ❖ … …

# Related Work: Existing LU-CP-ABE and T-CP-ABE

- ✓ Existing LU-CP-ABE directions:
  - ❖ Lewko and Waters [LW10a]: the first large universe KP-ABE construction built on composite order groups
  - ❖ Lewko [Lewko12] : the first large universe KP-ABE construction built on prime order groups
  - ❖ Rouselakis and Waters [RW13]: the first large universe CP-ABE construction built on prime order groups

- ✓ Existing T-CP-ABE directions:
  - ❖ Li et al. [LRK09]: the first notion of accountable CP-ABE to prevent illegal key sharing among colluding users
  - ❖ Li et al. [LHCCX11]: multi-authority ciphertext-policy (AND gates with wildcard) ABE scheme with accountability
  - ❖ Liu et al. [LCW13a]: white-box traceability CP-ABE
  - ❖ Liu et al. [LCW13b]: black-box traceability CP-ABE

# Motivation

To solve the obstacles of CP-ABE implementation in the commercial applications such as pay-TV systems and social networks:

- To trace the malicious users who intentionally leak their decryption keys, to prevent ( such as the pay-TV company) suffering from severe financial loss
- To realize large universe construction, i.e., to support flexible number of attributes (for such as the pay-TV company)
- To achieve the storage for traceability being at a constant level in the ideal case

# Our Results

We constructed a large universe CP-ABE system which is white-box traceable on prime order bilinear groups .

- We
- W
- W
- Th

The first practical CP-ABE system that supports :

white-box traceability

large universe

constant storage for tracing

# Our Results

| | LRK09 | LHCCX11 | LCW13 | RW13 | Ours |
|---|---|---|---|---|---|
| Large Universe | ✗ | ✗ | ✗ | ✓ | ✓ |
| Traceability | ✓ | ✓ | ✓ | ✗ | ✓ |
| Constant Storage for Tracing | ✓ | ✗ | ✗ | ⊘ | ✓ |
| Supporting Any Monotone Access Structures | ✗ | ✗ | ✓ | ✓ | ✓ |
| Constructed on Prime Order Groups | ✓ | ✗ | ✗ | ✓ | ✓ |
| Standard Model | ✗ | ✓ | ✓ | ✓ | ✓ |

The rest of this presentation…

1. Our construction
2. Extensions
3. Future Work

# Our T-LU-CP-ABE System : Abstract

- $Setup(1\lambda)\rightarrow pp,msk.$

  $pp$:$GD,g,u,h,w,v,\ g\uparrow\alpha\ ,e(g,g)\uparrow\alpha\ ;\ msk$:$\alpha,a,k\downarrow 1\ \ ,k\downarrow 2$

  - $k\downarrow 1\ \ ,k\downarrow 2$ are keys for probabilistic encryption scheme ($Enc,Dec$). Also, initializes an instance of Shamir's threshold scheme.

- $KeyGen(1\lambda,pp,msk,id,S=(A\downarrow 1\ ,A\downarrow 2\ ,\ldots,A\downarrow k\ ))\rightarrow sk\downarrow id,S=(K,K\uparrow'\ ,L,\ L\uparrow'\ ,\{K\downarrow\tau,1\ ,$ $K\downarrow\tau,2\ \}\downarrow\tau\in[k]\ )$.

  $K=g\uparrow\alpha/(a+c)\ w\uparrow r\ ,\ K\uparrow'=c\{K\downarrow\tau,2$ $(a$

  - $x=Enc\downarrow k\downarrow 1\ \ (id),\ y=f(x),c=Enc\downarrow k\downarrow 2\ \ (x||y)$.

- $Encrypt(1\lambda,pp,\ m,(M,\rho))\rightarrow ct=((M,\rho),C,C\downarrow 0\ ,C\downarrow$

  $C=m\cdot(e(g,g)\uparrow\alpha\ )\uparrow s\ ,\{C\downarrow i,1=(w\uparrow\lambda\downarrow i\ \ v)\uparrow t\downarrow i\ ,C$ $3=$ $g\uparrow t\downarrow i\ \}\downarrow i\in[l]\ .$

  - Exponents $t\downarrow 1\ ,\ t\downarrow 2\ ,\ldots,t\downarrow l\in Z\downarrow p$ are chosen randomly.

**no attributes are fixed !**

**“secret sharing” layer**

**“attribute” layer Boneh-Boyen-style hash function**

**“bind” two layers**

# Our T-LU-CP-ABE System : Abstract

- $Decrypt(1\lambda, pp, sk\downarrow id, S, ct) \rightarrow m$.

  $C / e(K, C\downarrow 0 \uparrow K\uparrow\prime \ C\downarrow 0 \uparrow\prime) / \prod i \in I \uparrow \blacksquare (e(L \uparrow K\uparrow\prime \ L\uparrow\prime, C\downarrow i, 1) \ e(K\downarrow \tau, 1, C\downarrow i, 2) e(K\downarrow \tau, 2, C\downarrow i, 3)) \uparrow w\downarrow i = m$.

  - Constants $\{w\downarrow i\}$ satisfy $\sum i \in I \uparrow \blacksquare w\downarrow i \ M\downarrow i = (1, 0, \ldots, 0)$ .

- $Trace(pp, INS\downarrow(t, n), msk, sk) \rightarrow id \ or \ \perp$.

  - Test whether $sk$ is well-formed.
  - (1) extracts $(x\uparrow *, y\uparrow *)$ from $x||y = Dec\downarrow k\downarrow 2 \ (K\uparrow\prime)$ .

    (2) if $(x\uparrow *, y\uparrow *) \in \{(x\downarrow 1, y\downarrow 1), \ldots, (x\downarrow t-1, y\downarrow t-1)\}$ , compute $Dec\downarrow k\downarrow 1 \ (x\uparrow *)$ to get $id$.

    Otherwise, go to (3).

    (3) recover the secret $a\downarrow 0 \uparrow *$ of $INS\downarrow(t, n)$ by interpolating with $\{(x\downarrow 1, y\downarrow 1), \ldots, (x\downarrow t-1, y\downarrow t-1)\}$

    and $(x\uparrow * = x, y\uparrow * = y)$. If $a\downarrow 0 \uparrow * = f(0)$, compute $Dec\downarrow k\downarrow 1 \ (x\uparrow *)$ to get $id$.

    Otherwise, the algorithm outputs

**fully white-box traceability !**

# Conclusion

We constructed a **T-LU-CP-ABE** system, where

- Could trace the malicious users leaking the partial or modified decryption keys to others for profits.
- The attributes' size is unbounded and the public parameters' size does not grow linearly with the number of attributes.
- Optimize the system in tracing the malicious users to cut down the storage cost for traceability and to make the system efficient in the user revocation.

# Extensions

- Transform from One-Use T-LU-CP-ABE to Multi-Use T-LU-CP-ABE:
  - ✓ Extend our new T-LU-CP-ABE system to a multi-use system using the encoding technique in [LOSTW10].

- Revocable T-LU-CP-ABE :
  - ✓ Extend our new T-LU-CP-ABE system to a revocable system using ciphertext delegation and piecewise key generation introduced in [SSW12].

# Future Work

- To obtain a large universe CP-ABE system which supporting black-box traceability:
  - the malicious users leak their decryption devices instead of decryption keys.
  - the malicious users could hide the decryption algorithm by tweaking it, as well as the decryption keys.

- T-LU-CP-ABE System with public auditors:
  - to judge whether a user is in fact innocent or not.
  - the suspected user does not trust the system and the system needs to provide some evidence persuasive enough to prove that the suspected user is guilty.

# References


- [SW05] Sahai, A., Waters, B.: Fuzzy identity-based encryption. EUROCRYPT 2005.
- [GPSW06] Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for finegrained access control of encrypted data. ACM CCS 2006.
- [BSW07] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. IEEE Symposium on Security and Privacy, 2007
- [LW10]: Allison Lewko and Brent Waters. New techniques for dual system encryption and fully secure hibe with short ciphertexts. In Theory of Cryptography, pages 455-479. Springer, 2010.
- [OT10]: Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In Advances in Cryptology-CRYPTO 2010, pages 191-208. Springer, 2010.
- [LOSTW10]: Allison Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Advances in Cryptology-EUROCRYPT 2010, pages 62-91. Springer, 2010.

# Reference


- [LW12]: Allison Lewko and Brent Waters. New proof methods for attribute-based encryption: Achieving full security through selective techniques. In Advances in Cryptology-CRYPTO 2012, pages 180-198. Springer, 2012.
- [Chase07] Melissa Chase. Multi-authority attribute based encryption. In Theory of Cryptography, pages 515-534. Springer, 2007.
- [CC09]: Melissa Chase and Sherman SM Chow. Improving privacy and security in multi-authority attribute-based encryption. In Proceedings of the 16th ACM conference on Computer and communications security, pages 121-130. ACM, 2009.
- [LW11]: Allison Lewko and Brent Waters. Decentralizing attribute-based encryption. In Advances in Cryptology-EUROCRYPT 2011, pages 568-588. Springer, 2011.
- [PRV12]: Bryan Parno, Mariana Raykova, and Vinod Vaikuntanathan. How to delegate and verify in public: Verifiable computation from attribute-based encryption. In Theory of Cryptography, pages 422-439. Springer, 2012.

# Reference


- [GHW11]: Matthew Green, Susan Hohenberger, and Brent Waters. Outsourcing the decryption of abe ciphertexts. In USENIX Security Symposium, page 3, 2011.
- [LW10a]: Allison Lewko and Brent Waters. Unbounded hibe and attribute-based encryption. In Advances in Cryptology-EUROCRYPT 2011, pages 547-567. Springer, 2011.
- [Lewko12]: Allison Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In Advances in Cryptology{EUROCRYPT 2012, pages 318-335. Springer, 2012.
- [RW13]: Yannis Rouselakis and Brent Waters. Practical constructions and new proof methods for large universe attribute-based encryption. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, pages 463-474. ACM, 2013.
- [LRK09]: Jin Li, Kui Ren, and Kwangjo Kim. A2be: Accountable attribute-based encryption for abuse free access control. IACR Cryptology ePrint Archive, 2009:118, 2009.

# Reference


- [LHCCX11]: Jin Li, Qiong Huang, Xiaofeng Chen, Sherman SM Chow, Duncan S Wong, and Dongqing Xie. Multi-authority ciphertext-policy attribute-based encryption with accountability. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pages 386-390. ACM, 2011.
- [LCW13a]: Zhen Liu, Zhenfu Cao, and Duncan S. Wong. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures. IEEE Transactions on Information Forensics and Security, 8(1):76-88, 2013.
- [LCW13b]: Zhen Liu, Zhenfu Cao, and Duncan S Wong. Blackbox traceable cp-abe: how to catch people leaking their keys by selling decryption devices on ebay. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, pages 475-486. ACM, 2013.
- [SSW12]: Amit Sahai, Hakan Seyalioglu, and Brent Waters. Dynamic credentials and ciphertext delegation for attribute-based encryption. In Advances in Cryptology-CRYPTO 2012, pages 199-217. Springer, 2012.

# Thanks.

## Q&A