

Privacy-aware Attribute-based Encryption with User Accountability

Jin Li¹, Kui Ren¹, Bo Zhu², Zhiguo Wan³

1. Illinois Institute of Technology, USA
2. Canada Concordia University, Canada
3. Tsinghua University, China

Outline

- **Background and Problem Description**
- **Our Construction**
- **Future work**

Outline

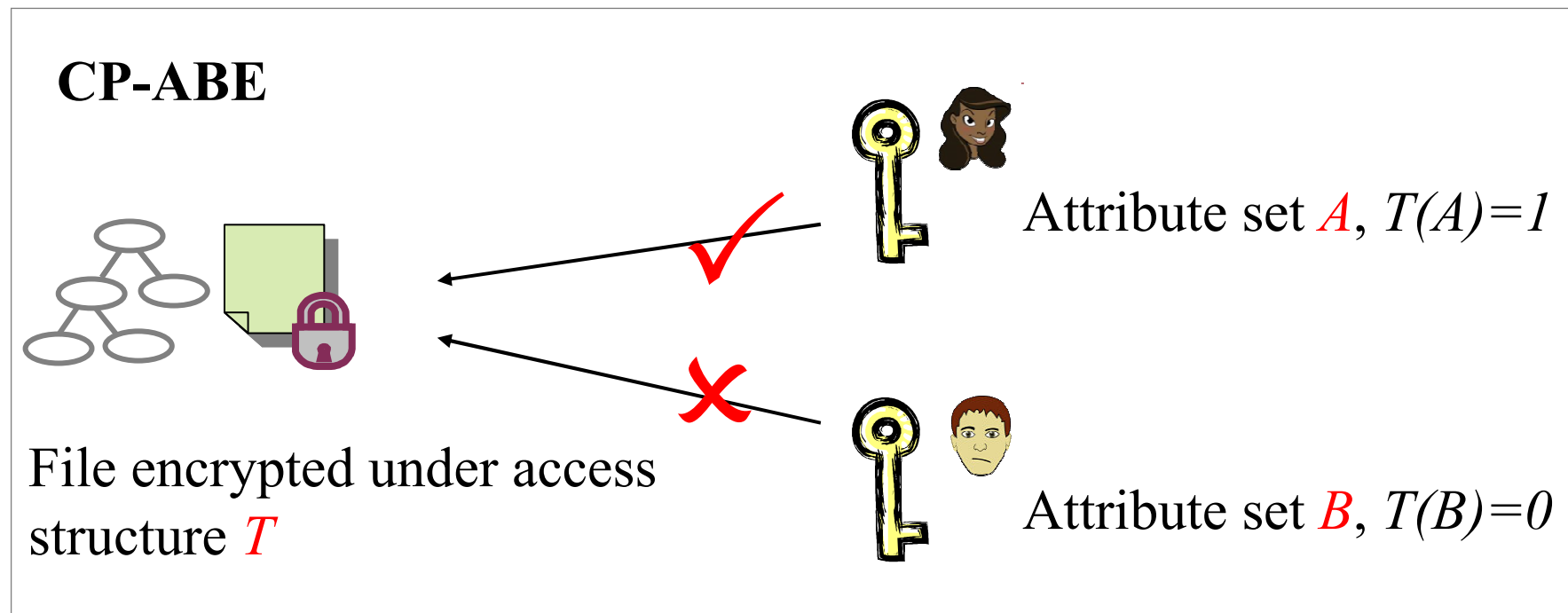
- **Background and Problem Description**
- Our Construction
- Future work

Attribute-Based Encryption

- ❖ A PKC proposed for fuzzy identity-based encryption
- ❖ Suitable for *one-to-many* encryption
- ❖ Key idea: public keys are user attributes
- ❖ Fine-grained access control

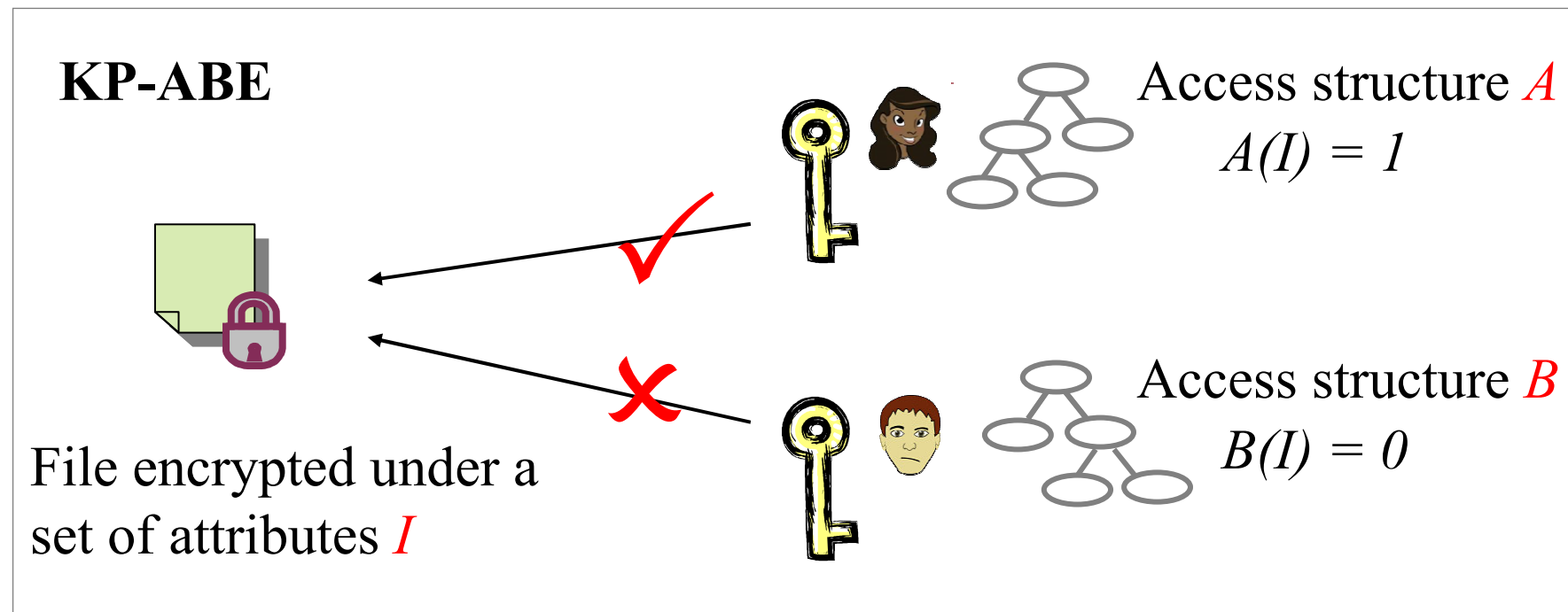
Attribute-Based Encryption

- ❖ Developed into two branches
 - Ciphertext Policy ABE (*CP-ABE*) and Key Policy ABE (*KP-ABE*)
 - Both are powerful tools for fine-grained access control



Attribute-Based Encryption

- ❖ Developed into two branches
 - Ciphertext Policy ABE (*CP-ABE*) and Key Policy ABE (*KP-ABE*)
 - Both are powerful tools for fine-grained access control



Privacy-aware ABE

- ❖ To protect the receivers' information, privacy-aware ABE is proposed:
 - ◆ Public keys (user attributes) are hidden in the ciphertext;
 - ◆ Users can only check whether their own keys are eligible to decrypt the ciphertext, without knowing other information.

Problem Description

- ❖ Illegal key sharing among users
 - How to prevent users from sharing their attribute private keys?
 - ◆ Some users may have common attributes.

Problem Description

❖ Our observation

- To detect illegal user, their identities IDs should be included in the private key of attribute list L.
- There is no user ID information in the ciphertext.

Problem Description

❖ Design Goals

- Construct a privacy-aware CP-ABE scheme with accountability, namely CP-A³BE.
- Achieve provable security.

❖ Challenges

- Existing technique such as traitor tracing in public key encryption can not be applied here directly.
- How to provide one-to-many encryption while supporting user accountability?

Outline

- Background and Problem Description
- **Our Construction**
- Future work

System Model

There are five algorithms in CP-A³BE, i.e.,

- 1) Setup:** Set up the system parameters;
- 2) KeyGen:** Generate an attribute private key on L to user with public key ID/pk ;
- 3) Enc:** Encrypt a message to users with certain access policy W ;
- 4) Dec:** Decrypt the ciphertext if the attributes in user secret key match the access policy in the ciphertext, i.e., $R(L,W)=1$;
- 5) Trace:** Given a pirate device, output identity associated with this attribute private key.

CP-A³BE Scheme

❖ Setup

- Public parameters as well as a master key for the attribute authority are chosen.

❖ KeyGen

- Assume that the attributes of user ID are $L=(L_1, L_2, \dots, L_k)$.
- The authority computes the attribute private key for $L\parallel ID$ with the technique of hierarchical identity-based encryption, where ID is viewed as another default attribute.

CP-A³BE Scheme

❖ Enc

- Assume that a message is encrypted with ciphertext-policy W .
- The sender computes a ciphertext with policy $w \parallel^*$, such that any user with attribute list $R(L,W)=1$ can decrypt, regardless of the identity ID.

CP-A³BE Scheme

❖ Dec

- Suppose that a message is encrypted with $W \parallel^*$.
- Assume the user's secret key is for $L \parallel ID$, where $R(L, W)=1$.
The user can only decrypt the ciphertext with attribute private key of L and the secret key of ID .

CP-A³BE Scheme

❖ Trace

- Suppose that a given pirate device can decrypt the ciphertext under ciphertext-policy W .
 1. The authority extracts part of the attribute list L out of W and determines the suspicious user set S from L .
 2. To pinpoint the exact identity from S : The authority just encrypts a message with respect to ciphertext-policy W and each ID in S until the identity is found.

Main Idea of the Construction

- In normal encryption algorithm, a message is encrypted under ciphertext-policy $W=W' \parallel *$ such that any user with $L \parallel ID$ satisfying $R(L \parallel ID, W)=1$ is able to decrypt.
- In tracing algorithm, a message is encrypted with $W' \parallel ID^*$ to test whether the identity in the pirate device is ID^* .
- Due to the anonymity of CP-A³BE, the ciphertext is indistinguishable between the normal encryption and tracing algorithms.

Security Results

The construction is based on an improved privacy-aware CP-ABE, with AND gate of access structure.

Theorem 1 The CP-A³BE construction is secure in sCP-IND-CPA model, under the DBDH and D-Linear assumptions.

Proof. The proof is given by applying a sequence of games, which is divided into two parts:

1. The indistinguishability of the encryption scheme;
2. The validity of the tracing algorithm, i.e., the user accountability.

Future Work

- Constructing CP-A³BE based on other privacy-aware CP-ABE;
- Constructing more fine-grained CP-A³BE;
- Designing constructions with provable security under standard assumptions;

Any question, please contact with Jin Li

jli25@iit.edu

Thank you!