Attribute-Based Encryption

Presenter: 張耀文、陳居廷、朱劭璿
Advisor: Professor Fan

In this presentation

- What to expect
  - Understand what is Attribute-Based Encryption
  - Understand why ABE is needed
  - Understand the difference between key-policy and ciphertext-policy ABE
  - Understand how to use a C++ library, OpenABE, to add ABE to your project
- What to NOT expect
  - The comparison between different schemes of ABE in detail
  - Understand how to transform attributes into math problems
  - Understand what security assumptions are used in ABE

Outline

- Limitations on the Asymmetric Encryption
- Identity-Based Encryption
- Attribute-Based Encryption
  - Key-Policy Attribute-Based Encryption
  - Ciphertext-Policy Attribute-Based Encryption
- Implementation Details
- Demo
  - KP-ABE & CP-ABE Examples
  - Secure Chatting Service

Limitations on the Asymmetric Encryption

- Asymmetric Encryption
  - The sender uses the receiver’s public key to encrypt the messages
  - The receiver uses its own private key to decrypt the messages
- Limitations
  - Relying on PKI, which requires huge overhead on certification management and verification
  - What if you want to send the same message to a group of people
  - Many keys!

Identity-Based Encryption

- Proposed by Adi Shamir in 1984
- The sender uses the receiver’s identity as a public key
  - E.g., email address
- The receiver creates a private key based on his identity
  - All he needs is to prove its identity, for example, a username-password combo
- A central system, Private Key Generator (PKG), is required
  - Authenticate the receiver’s identity and generate the private key
  - Publish the master public key
    - To let anyone compute a public key corresponding to the identity by combining the master public key with the identity value

Identity-Based Encryption

- Pros:
  - No prior public-private-key-pair distribution
  - You only need to known other's identity!
  - The PKG can evaluate the identifier and decline the extraction if the expiration date has passed.
- Cons:
  - Still need to send multiple versions of an encrypted message to many people
  - PKG must be highly trusted
    - If a PKG is compromised, all messages protected over the entire lifetime of the public-private key pair used by that server are also compromised.
  - A secure channel between a user and the PKG is required.

Attribute-Based Encryption

- Proposed by Amit Sahai and Brenet Waters in 2004
  - Fuzzy Identity-Based Encryption
    - Fuzzy → multiple private keys to be used with a single public key
- Public keys are constructed from a list of attributes instead of an identity
- Decide who get the permission by a policy

Attribute-Based Encryption

- Example
  - Define the policy as
    - ((user=Chu and location=TW) or (user=David and location=US))
  - Chu from TW and David from US would have permission to the message
  - Chu from US and David from TW would not
  - Of course, other people also cannot decrpyt the messasge

Attribute-Based Encryption

- Key-Policy Attribute-Based Encryption
  - The PKG generates the private key based on a policy (logical operation between attributes) from receiver.
  - The sender's attributes need to match the receiver's policy
- Ciphertext-Policy Attribute-Based Encryption
  - The PKG generates the private key based on a given set of attributes from receiver.
  - The receiver's attributes need to match the sender's policy

Key-Policy Attribute-Based Encryption

- Example
  - Define the data1 attribute encrypted as {2021, CSE, prof.}
  - Define the data2 attribute encrypted as {2021, BST, prof.}
  - User1 policy: (2021 and CSE)
  - User2 policy: (2021 prof.)
  - User1 can decrypt data1 and user2 can decrypt both data.

Key-Policy Attribute-Based Encryption

- The sender encrypts the message with a set attributes
- The sender's attributes must match the receiver's policy in order to use the corresponding key to decrypt
- The sender do not know what is the policy
- The sender cannot comfirm who get to decrypt the message
- Typically used in the paid serverice (e.g. Netflix)
  - A Netflix video's attribute: {paid}
  - A paid client's policy: (free or paid)
  - A free client's policy: (free)

Ciphertext-Policy Attribute-Based Encryption

- Example
  - Define the data encrypted policy as (NSYSU and (CSE or BST))
  - User1 is CSE from NSYSU.
  - User2 is BST from NSYSU.
  - User1 and user2 can decrypt the data.
  - NCKU, NTU can’t access.

Ciphertext-Policy Attribute-Based Encryption

- The sender define the policy
- The receiver's attributes must match the sender's policy in order to use the corresponding key to decrypt
- The sender knows who get to decrypt the message
- Typically used in file sharing

P: PKG
S: Sender
R: Receiver

Implementation Details

Key-policy ABE

P
- Setup()
  - Generate master public & private keys.

S
- Encrypt()
  - Encrypt with a set of attributes.

P
- KeyGen()
  - Generate a private key based on a policy. And distribute to the receiver based on the given access structure.

R
- Decrypt()
  - Decrypt the ciphertext w/ private key.
  - The sender's attributes must match the receiver's policy (i.e., the key).

Cyphertext-policy ABE

- Setup()
  - Generate master public & private key.
- Encypt()
  - Encrypt with a policy (logical operation between attributes).
- KeyGen()
  - Generate a private key based on receiver's attributes
- Decrypt()
  - Decrypt the ciphertext w/ private key.
  - The receiver's attributes (i.e., the key) must match the sender's policy.

Demo

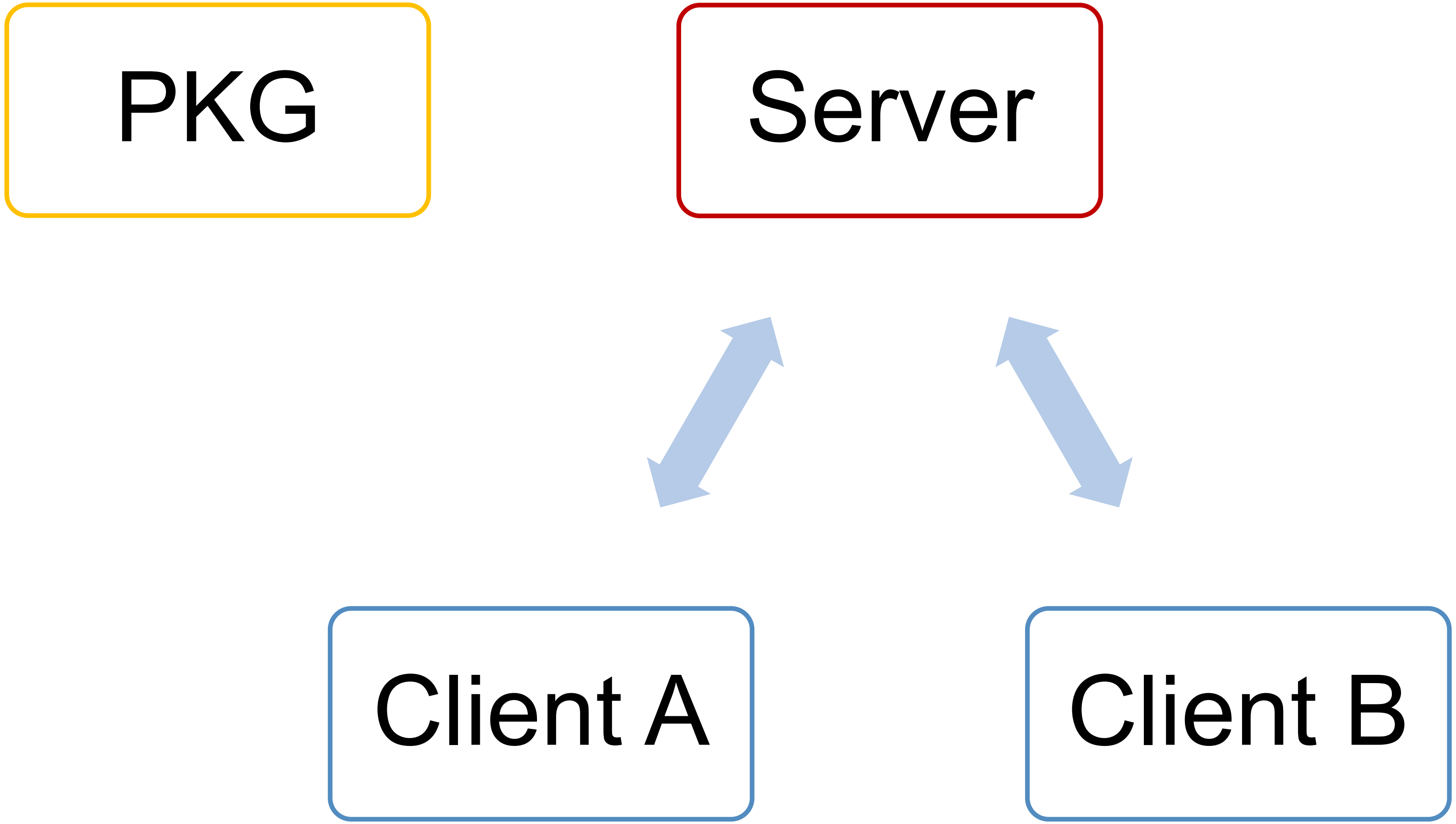
KP-ABE & CP-ABE Examples

- https://github.com/ernestchu/abe-examples

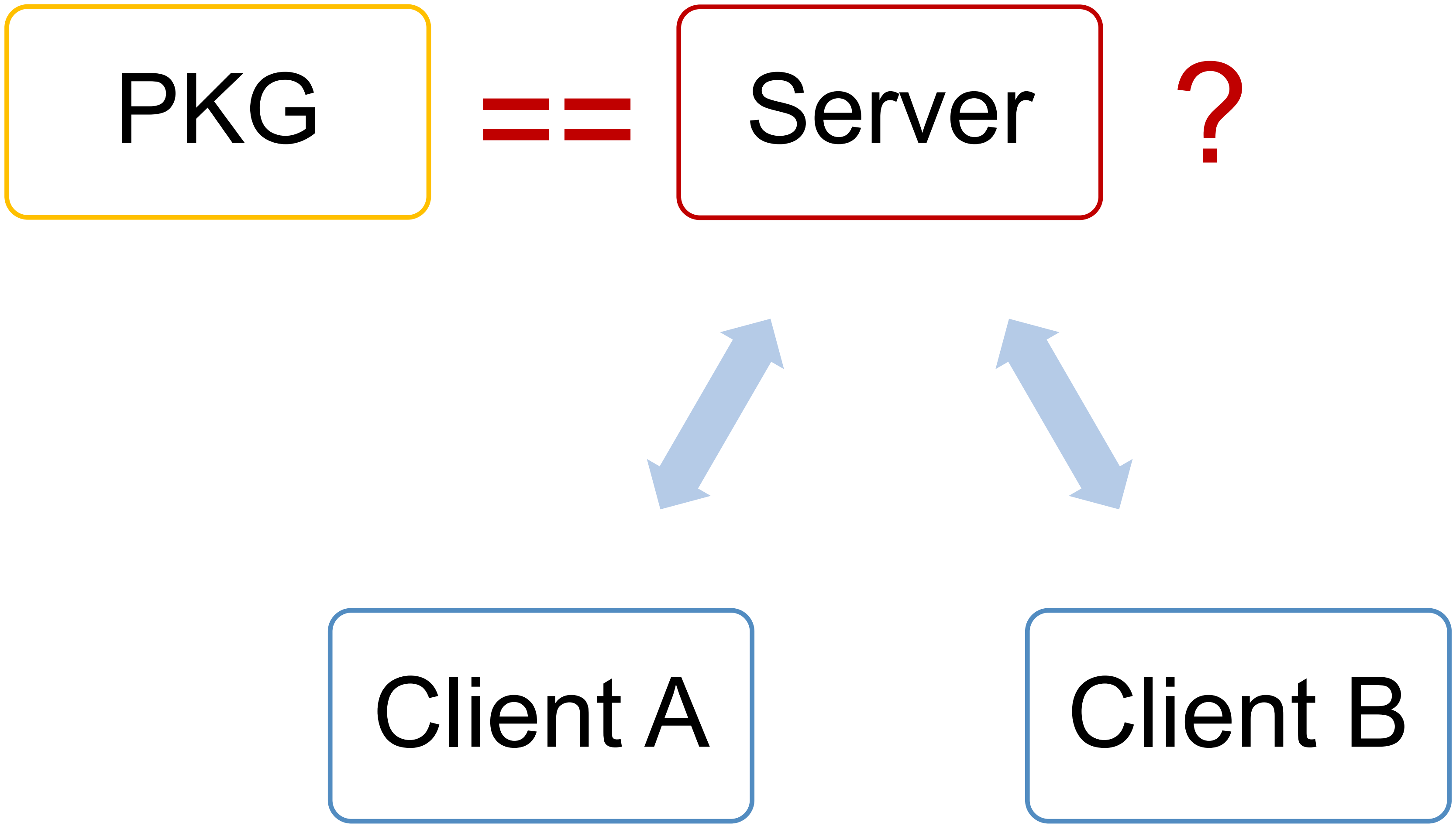
Secure Chatting Service

- https://github.com/ernestchu/on-line-chatting-service/tree/abe

Secure Chatting Service

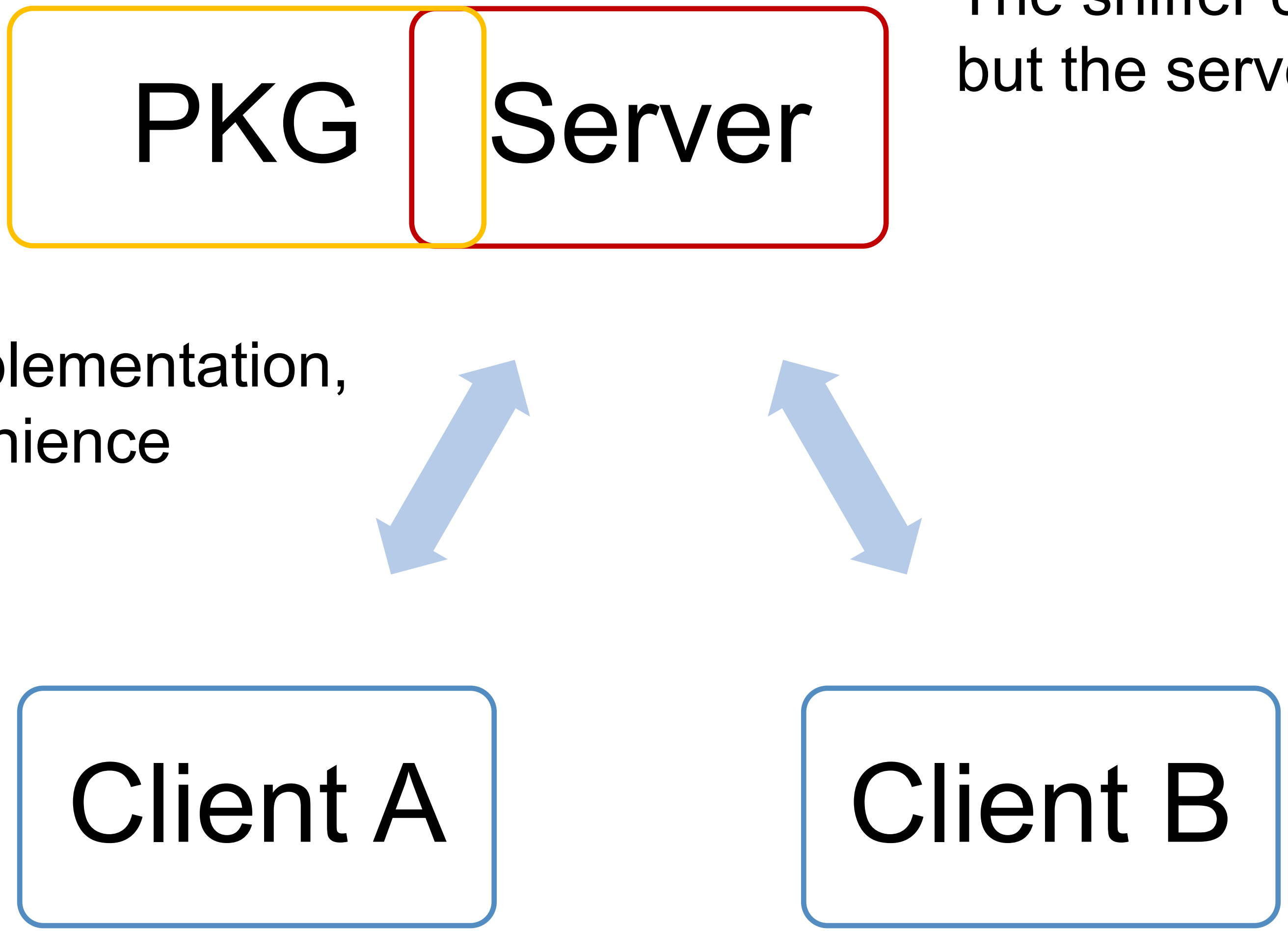


Secure Chatting Service



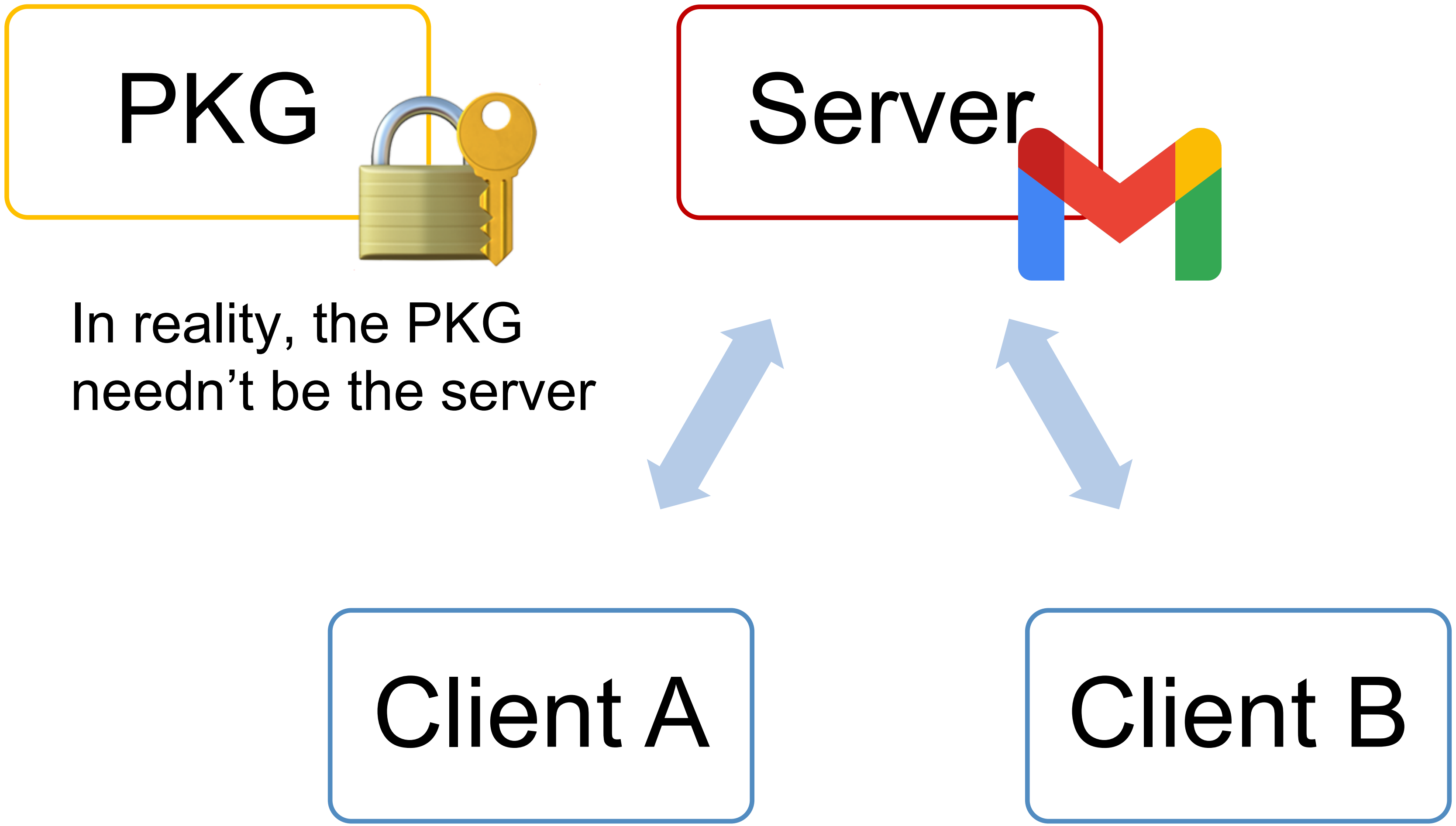
Secure Chatting Service

The sniffer cannot decrypt,
but the server can!



In our implementation,
for convenience

Secure Chatting Service



References

- Wikipedia
- https://medium.com/@dbkats/a-gentle-introduction-to-attribute-based-encryption-edca31744ac6
- https://asecuritysite.com/encryption/abe
- https://ir.nctu.edu.tw/bitstream/11536/71651/1/601601.pdf
- https://www.ijcsmc.com/docs/papers/May2017/V6I5201741.pdf
- https://cat.chriz.hk/2019/11/kp-abe-vs-cp-abe.html
- https://github.com/zeutro/openabe