# Public-Key Revocation and Tracing Schemes with Subset Difference Methods Revisited

*ESORICS 2014*

*Kwangsu Lee, Woo Kwon Koo, Dong Hoon Lee, Jong Hwan Park*

*Korea University, Korea University, Korea University, Sangmyung University*

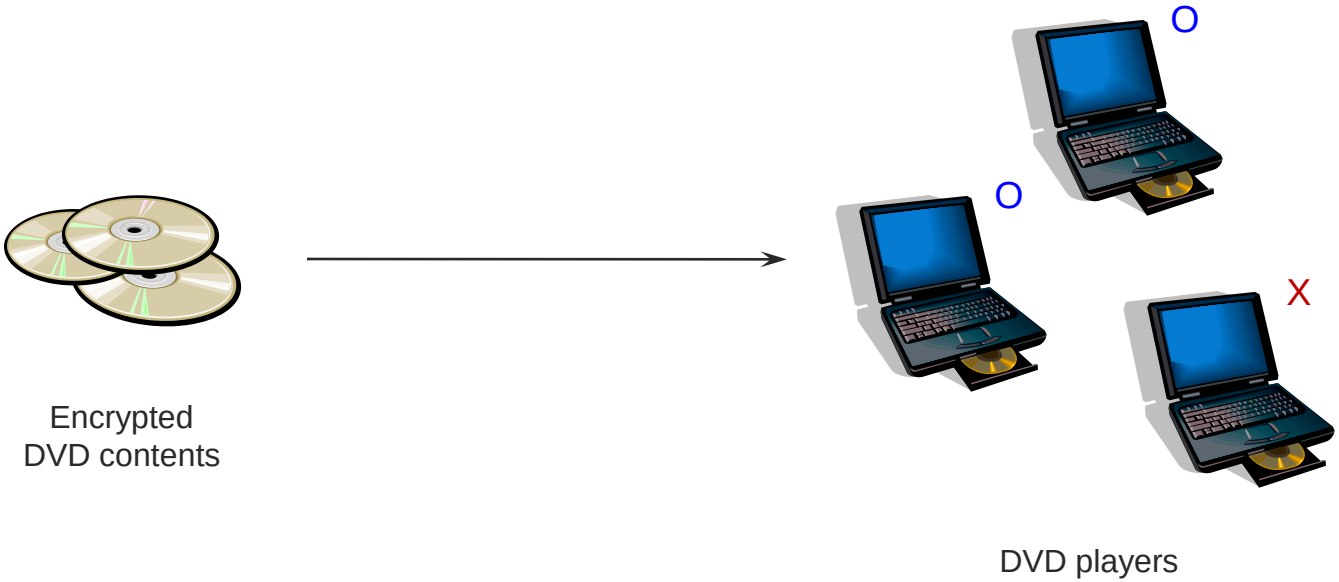
# Overview

- Motivation
  - Public-key revocation encryption (PKRE) is a powerful primitive since any user can send a ciphertext to a set of users excluding revoked users
  - We revisit the method of Dodis and Fazio that provides a PKRE scheme from subset difference (SD) methods to reduce the size of private keys and public keys

- Results
  - We introduce *single revocation encryption* (SRE) and construct an efficient SRE scheme
  - We present an *efficient PKRE scheme* with shorter private keys and public keys by combining the SD method and our SRE scheme
  - Our PKRE scheme provides the (weak) *tracing functionality* since it is derived from the SD method

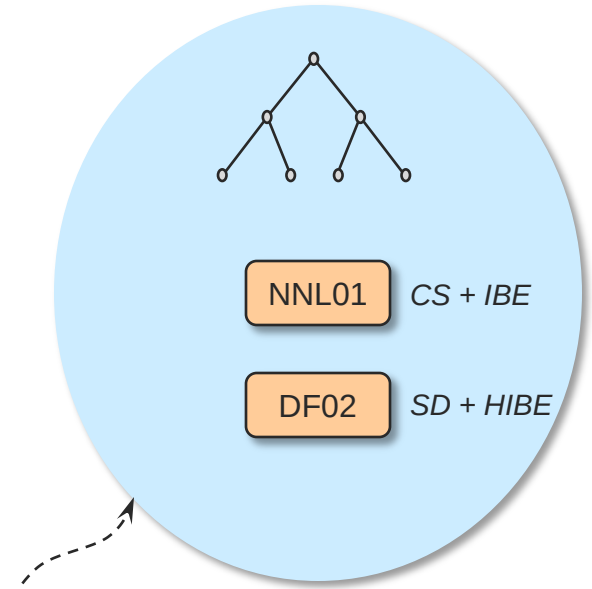
# Introduction

- Revocation Encryption
  - Revocation encryption is a mechanism to efficiently send an encrypted message to a set of receivers by excluding a set *R* of revoked users
  - The application includes pay-TV systems, DVD content distribution systems, and file systems

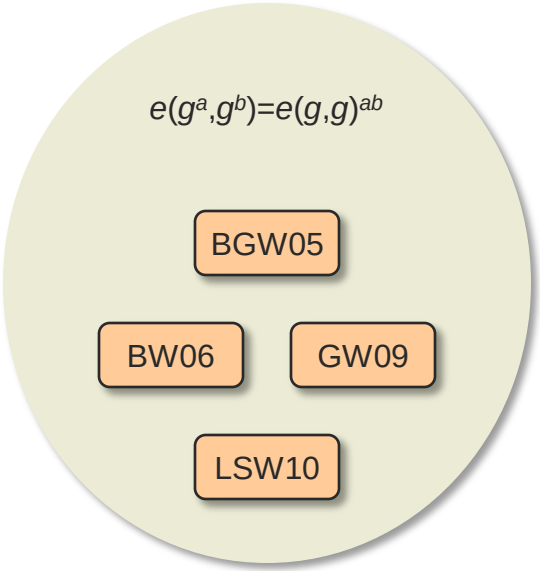


# Introduction

- A Classification of (Public-Key) Revocation Encryption
  - There are two general classes of PKRE schemes depending on their construction approaches
  - The first one is revocation schemes based on *binary trees* and the second one is revocation schemes based on *bilinear groups*



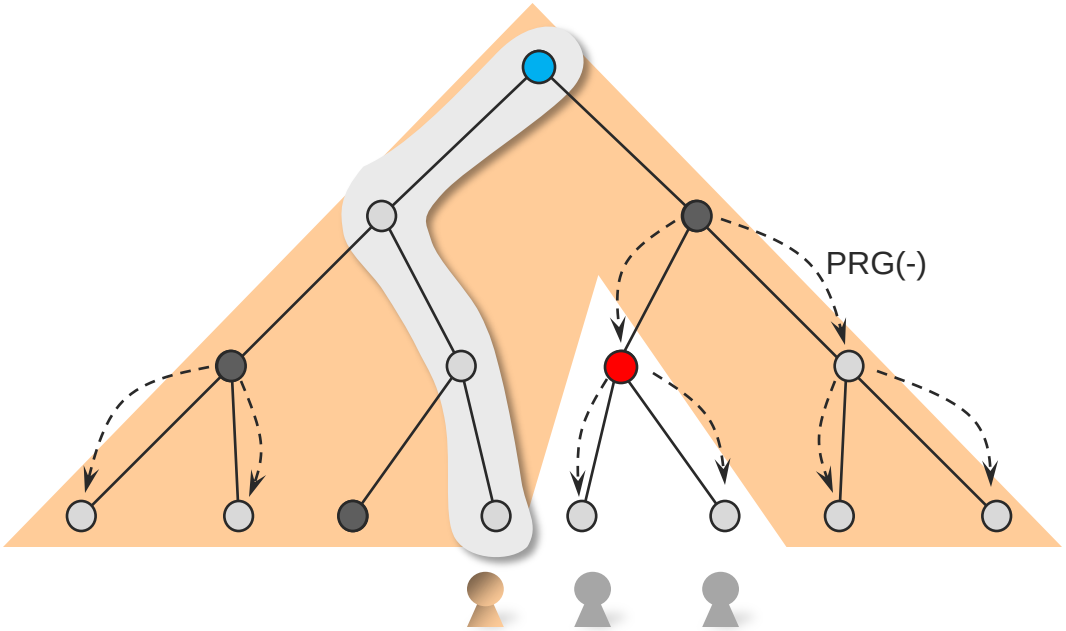

We focus on this approach !!




*CT = O($N^{1/2}$) or Decrypt = O(r)*

# Introduction

- The Subset Difference Method of Naor *et al.* [NNL01]
  - The subset difference (SD) method is a general methodology to construct efficient (symmetric-key) revocation encryption schemes
  - A user is assigned to a leaf in a tree and a ciphertext is associated with the minimum number of subsets that covers non-revoked users

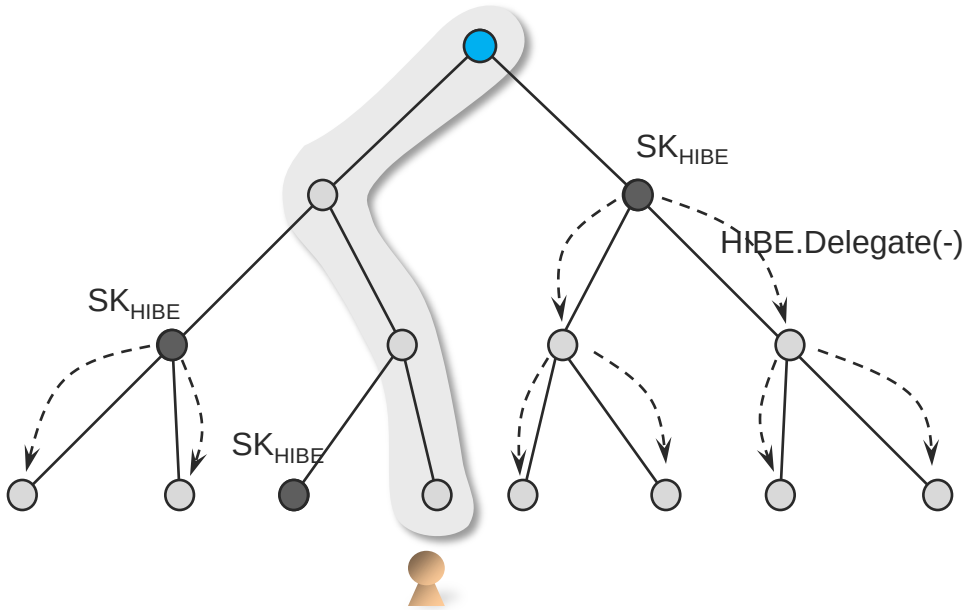



SD + PRG ⇒ SKRE
$SK = O(\log^2 N)$
$CT = O(r)$

$N$ = # of leaf nodes
$r$ = # of revoked nodes

# Introduction

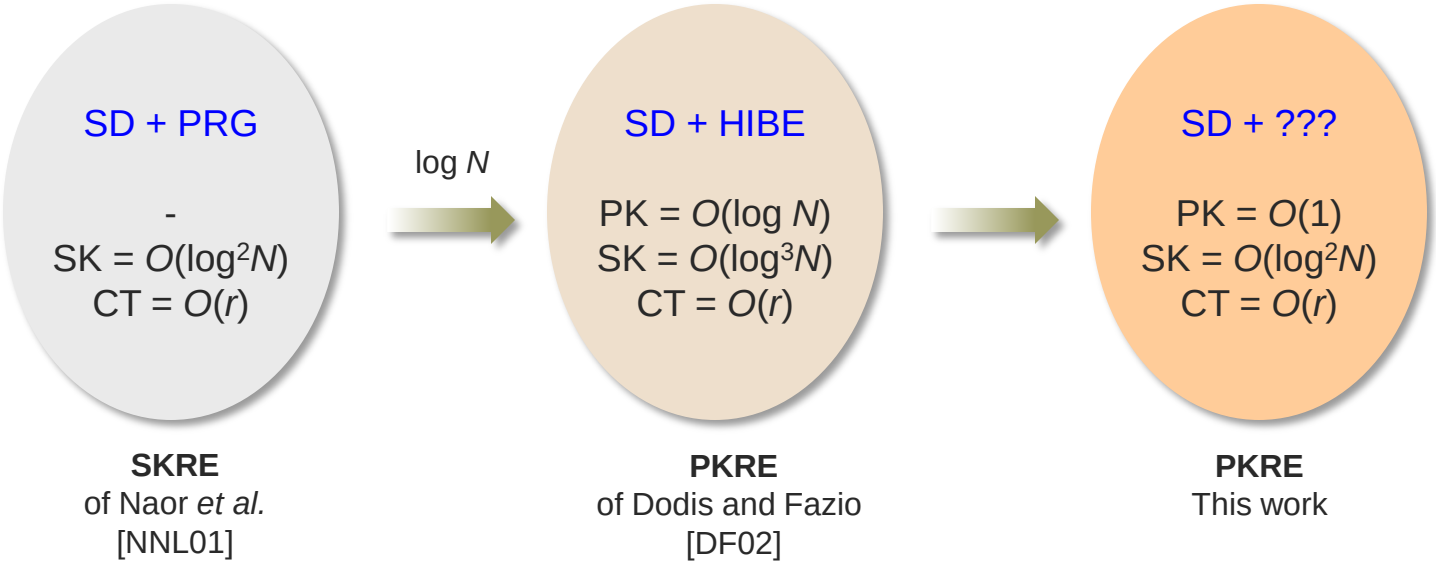
- Generic PKRE of Dodis and Fazio [DF02]
  - Dodis and Fazio showed that a PKRE scheme can be constructed by combining the SD scheme and any HIBE scheme
  - This method essentially uses *the key delegation property* of HIBE to decrypt a ciphertext




SD + HIBE ⇒ PKRE
but the overhead (log *N*)
of HIBE is added

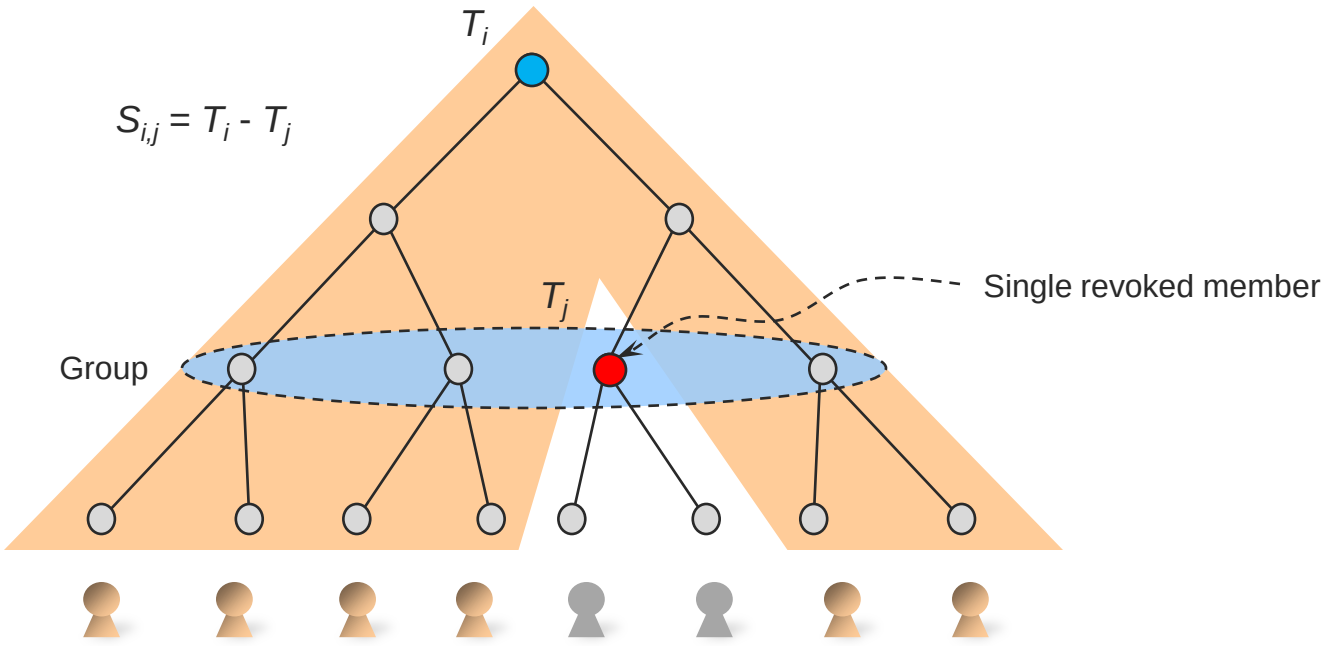
# Introduction

- Our Motivation
  - The generic PKRE scheme of Dodis and Fazio is not satisfactory since the size of private keys and public keys increases by log $N$ factor because of the overhead of an HIBE scheme
  - A new PKE scheme that can be tightly integrated with the SD scheme is required!!



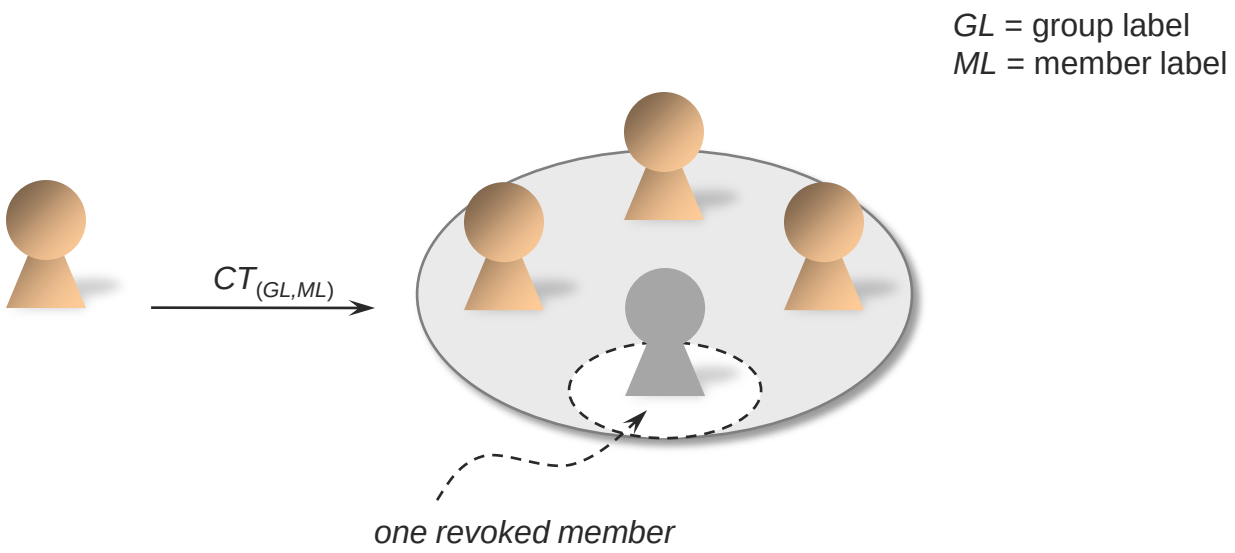
# Introduction

- Our Approach
  - A subset $S_{i,j}$ of the SD scheme is defined as the set of leaf nodes in $T_i$ - $T_j$ where $T_i$ and $T_j$ are two subtrees
  - We observe that a subset $S_{i,j}$ of the SD scheme can be reinterpreted as an encryption scheme with *single member revocation*



# Single Revocation Encryption

- Overview
  - Single revocation encryption (SRE) is a special type of public-key encryption such that a single user in a group can be revoked
  - A ciphertext is associated with a group label $GL$ and a (revoked) member label $ML$, and a user $u$ can decrypt it if ($u \in GL$) and ($u \neq ML$)



# Single Revocation Encryption

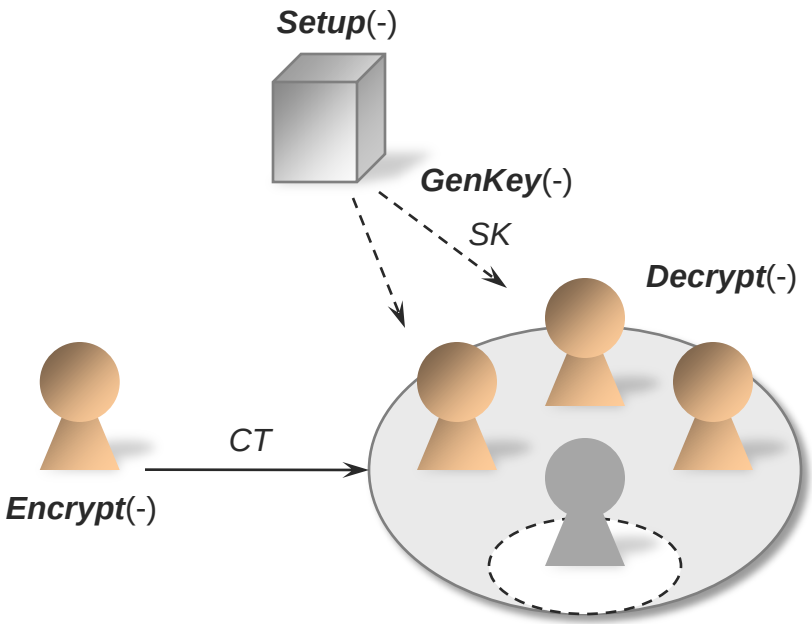
- Definition
  - SRE is a special type of broadcast encryption with the *single member revocation* property
  - An SRE scheme consists of algorithms: Setup, GenKey, Encrypt, and Decrypt

**Setup**$(1^{\lambda},U) \rightarrow MK,PK$

**GenKey**$((GL,ML),MK,PK) \rightarrow SK_{(GL,ML)}$

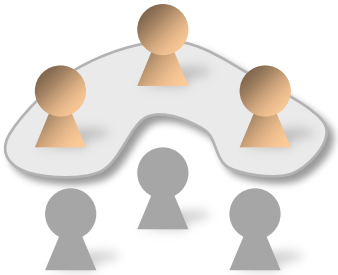
**Encrypt**$((GL,ML),M,PK) \rightarrow CT_{(GL,ML)}$

**Decrypt**$(CT_{(GL,ML)},SK_{(GL',ML')},PK) \rightarrow M$



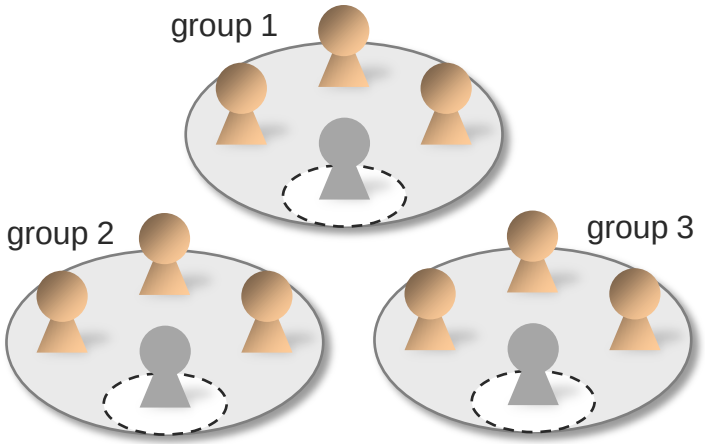
# Single Revocation Encryption

- Design Principle
  - Our SRE scheme is inspired by the IBRE scheme of Lewko, Sahai, and Waters that employs the two equation technique
  - To support groups, we modify a simple variation of the IBRE scheme by using two (random oracle) hash functions



$$SK = [g^{\alpha} w^{r}, (hw^{ID})^{r}, g^{-r}]$$

***IBRE***




$$SK = [g^{\alpha} H(GL)^{r}, (H(GL)H(GL)^{ML})^{r}, g^{-r}]$$

***SRE***

# Single Revocation Encryption

- Construction
  - Let $(p, G, G_T, e)$ be a bilinear group of prime order and $U = \{(GL_i, \{ML_j\})\}$ be the universe of groups and members

$$PK = [(p, G, G_T, e), g, H_1, H_2, \Omega = e(g,g)^{\alpha}]$$

$$SK_{(GL',ML')} = [K_0 = g^{\alpha} H_2(GL')^r, K_1 = (H_1(GL')H_2(GL')^{ML'})^r, K_2 = g^{-r}]$$

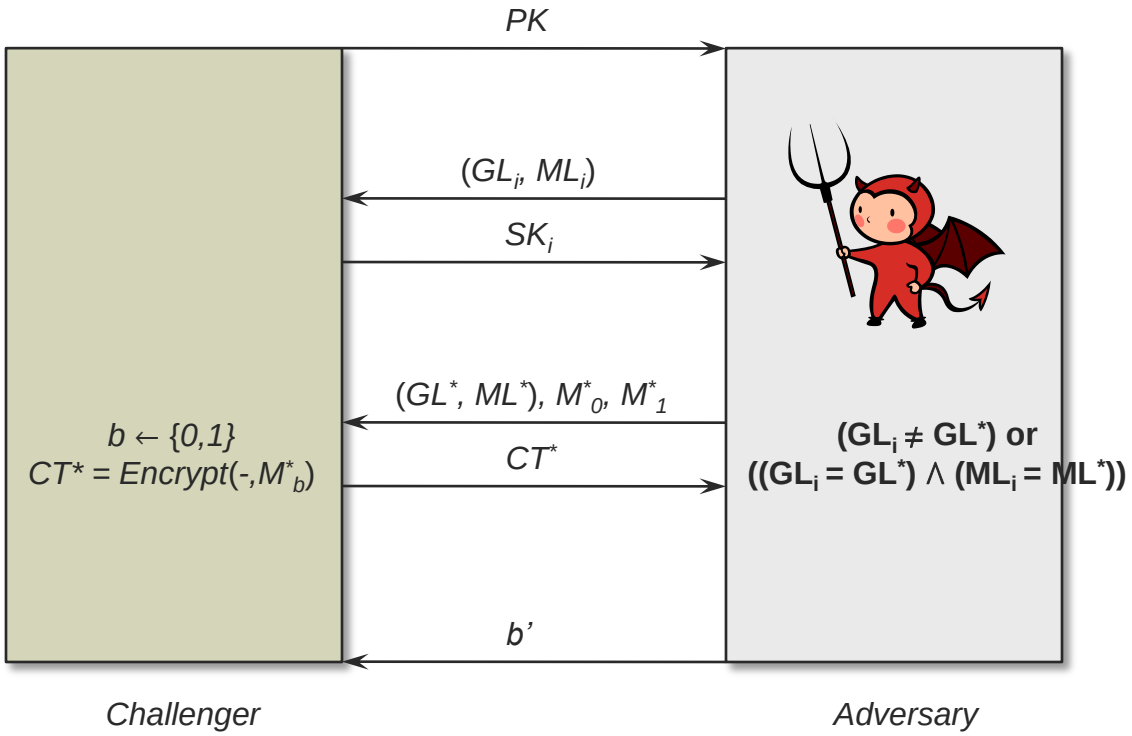
$$CT_{(GL,ML)} = [C_0 = \Omega^t M, C_1 = g^t, C_2 = (H_1(GL)H_2(GL)^{ML})^t]$$

$$if\ (GL = GL') \wedge (ML \neq ML'), then$$

$$M = C_0 \cdot \frac{(e(C_1, K_1) \cdot e(C_2, K_2))^{1/(ML'-ML)}}{e(C_1, K_0)}$$

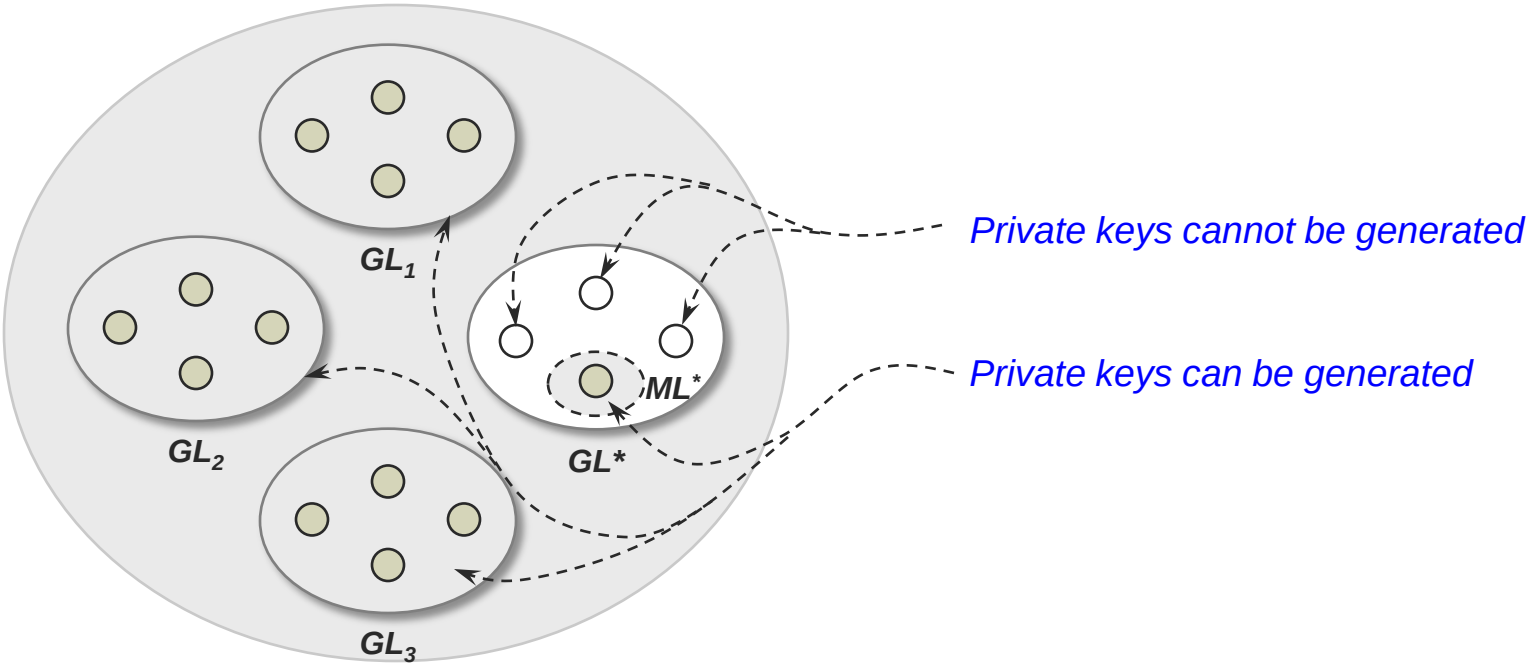
# Single Revocation Encryption

- Security Model
  - The security of SRE is defined as an indistinguishability game between a challenger *C* and an attacker *A*



# Single Revocation Encryption

- Security Analysis
  - The proof uses the *partitioning strategy* and the power of *q*-Type assumption to simulate the queries of private keys



# Revocation Encryption

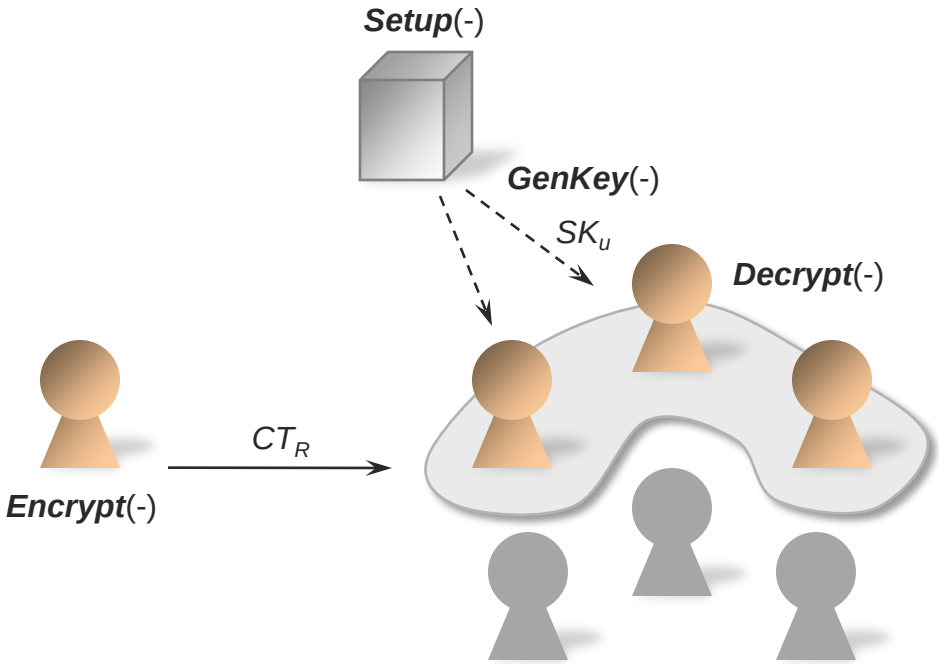
- Definition
  - PKRE is a slight variant of PKBE such that a ciphertext is specified by a revoke set $R$ instead of a receiver set $S$
  - A PKRE scheme for the set $N$ of users consists of algorithms: Setup, GenKey, Encrypt, and Decrypt

**Setup**$(1^{\lambda},N) \rightarrow MK,PK$

**GenKey**$(u,MK,PK) \rightarrow SK_u$

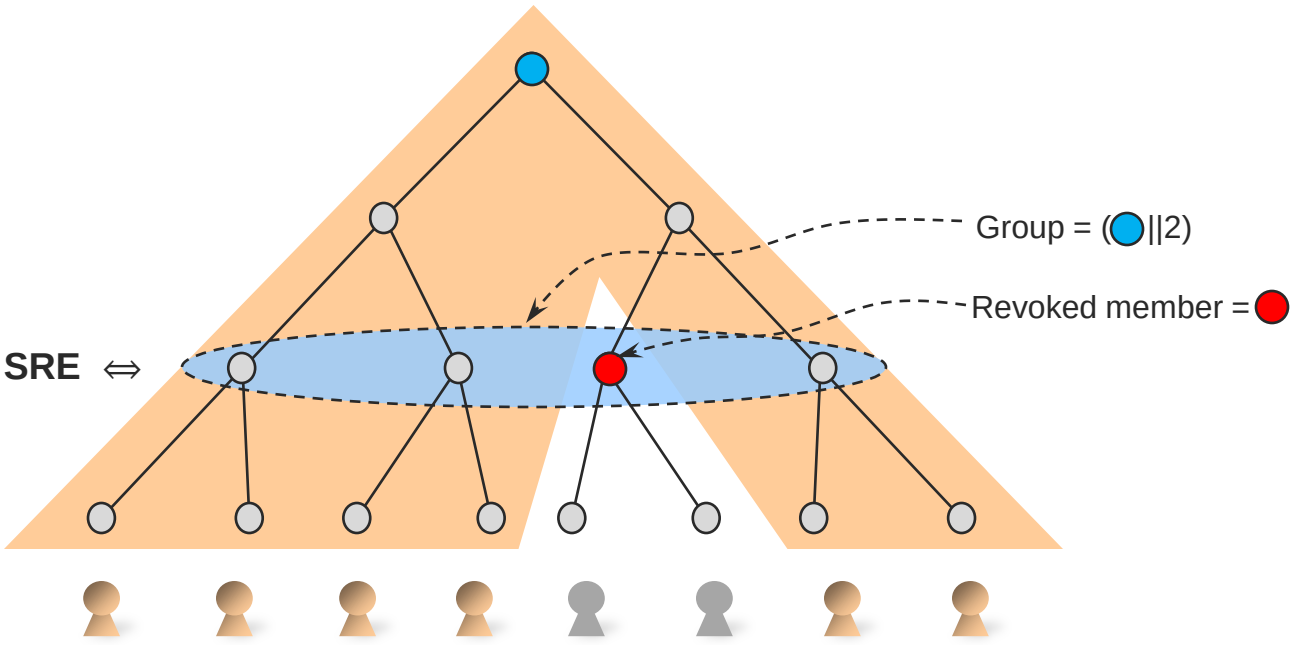
**Encrypt**$(R,M,PK) \rightarrow CT_R$

**Decrypt**$(CT_R,SK_u,PK) \rightarrow M$



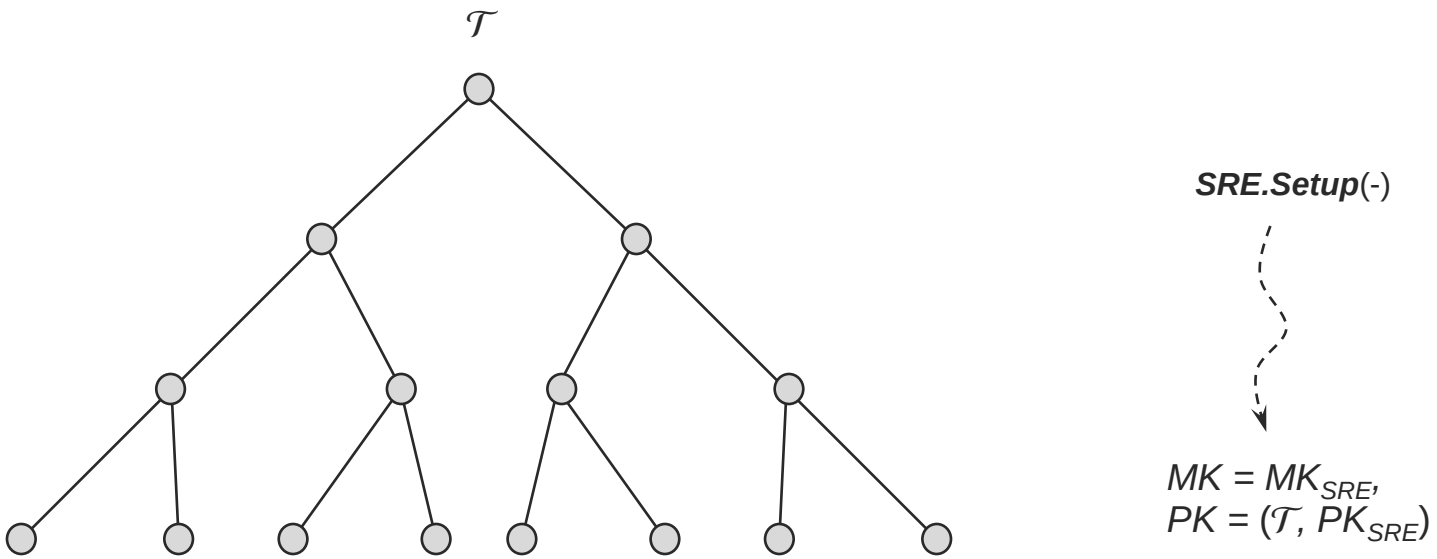
# Revocation Encryption

- Design Principle
  - The basic idea of our PKRE scheme is to combine the SD scheme and our SRE scheme
  - We observe that a subset $S_{i,j}$ in the SD scheme can be easily mapped to the group and member labels ($GL$, $ML$) of the SRE scheme



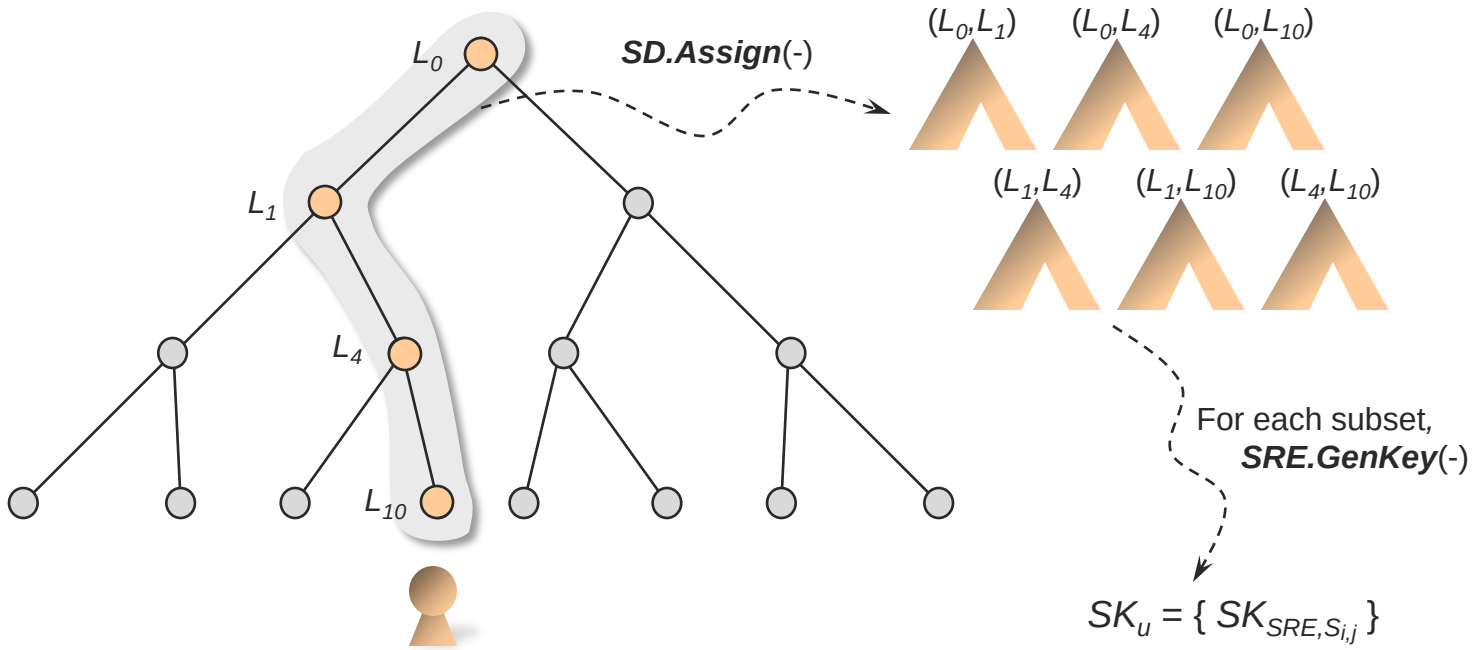
# Revocation Encryption

- Construction
  - $MK, PK \leftarrow \text{Setup}(1^{\lambda}, N)$: It implicitly sets a full binary tree $\mathcal{T}$ and obtains $MK_{SRE}, PK_{SRE}$ of the SRE scheme



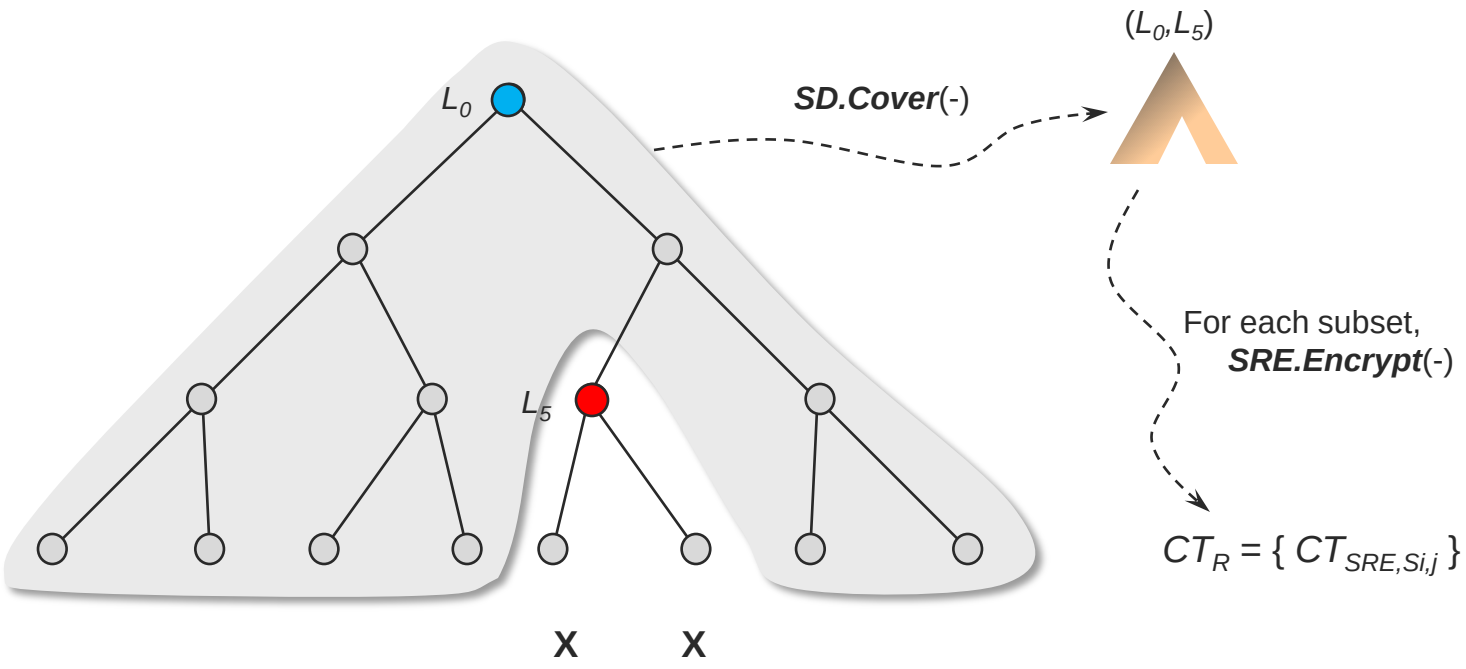
# Revocation Encryption

- Construction
  - $SK_u \leftarrow \text{GenKey}(u, MK, PK)$: The private key consists of SRE private keys that are associated with subsets $\{S_{i,j}\}$ obtained from path nodes of a user



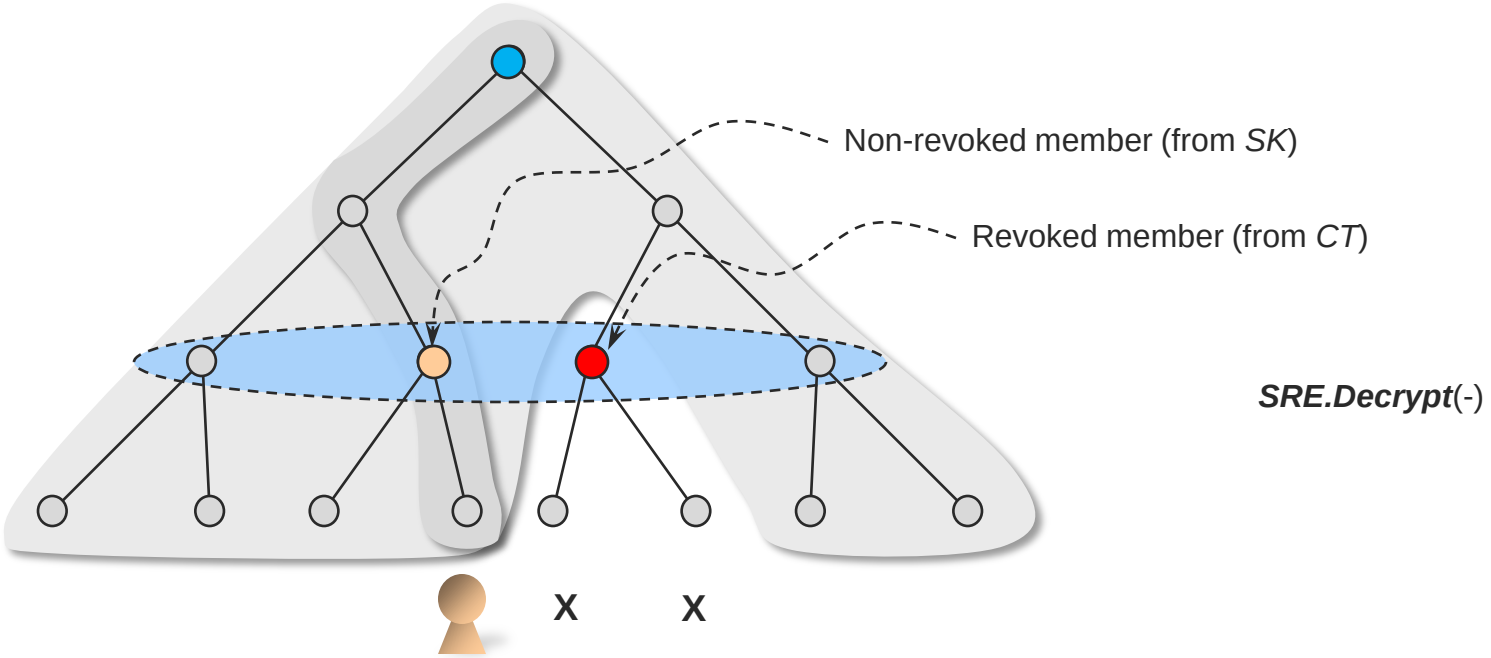
# Revocation Encryption

- Construction
  - $CT_R \leftarrow \text{Encrypt}(R, M, PK)$: The ciphertext consists of SRE ciphertexts associated with minimal covering subsets



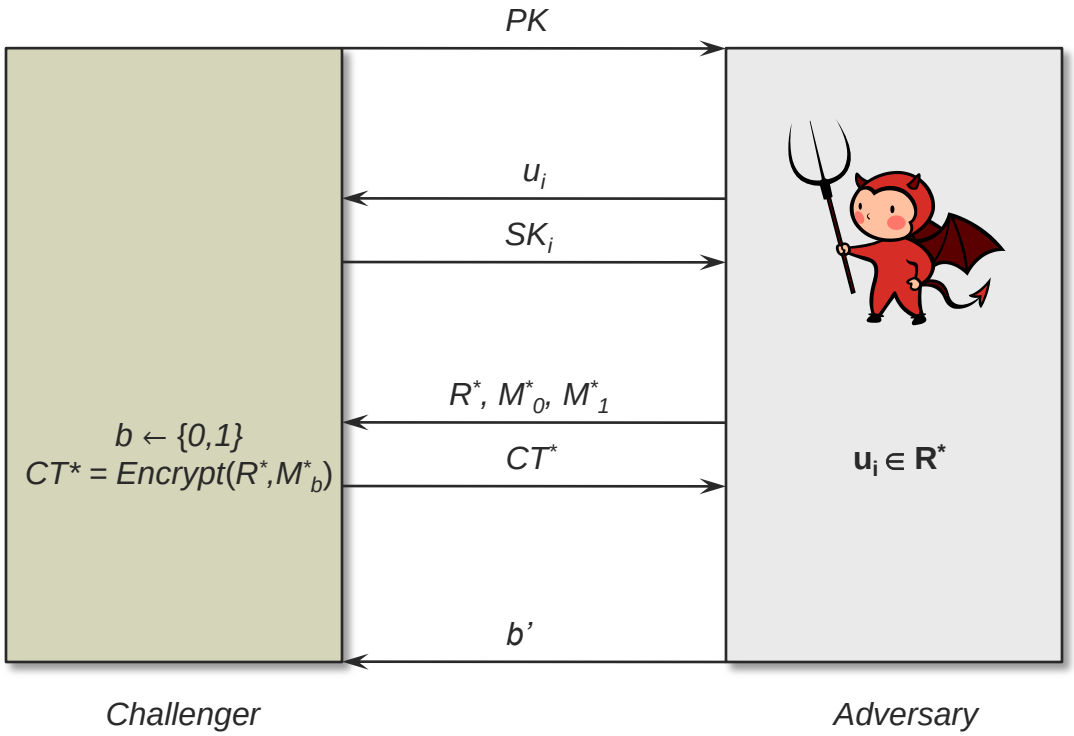
# Revocation Encryption

- Construction
  - $M \leftarrow \text{Decrypt}(CT_R, SK_u, PK)$: If $u \notin R$, the decryption algorithm of SRE can be used since there exist two subsets $S_{i,j}$ and $S'_{i',j'}$ such that $i=i'$ and $j \neq j'$



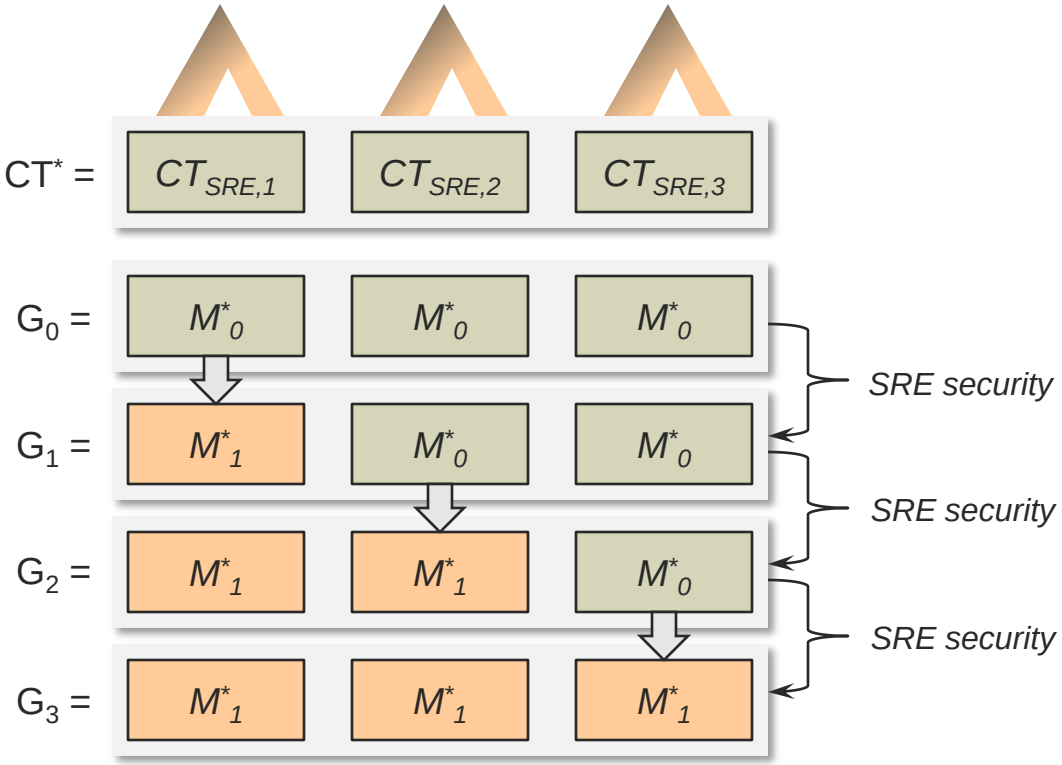
# Revocation Encryption

- Security Model
  - The security of PKRE is defined as an indistinguishability game between a challenger *C* and an attacker *A*



# Revocation Encryption

- Security Analysis
  - The proof uses *hybrid games* that convert the challenge ciphertext from an encryption of $M^*_0$ to an encryption of $M^*_1$
  - Let the size of covering subsets of the challenge revoked set $R^*$ is $w$



# Revocation Encryption

- Discussions
  - **Efficiency**: In our PKRE scheme, a public key, a private key, and a ciphertext consists of $O(1)$, $O(\log^2 N)$, $O(r)$ group elements, respectively
  - **Layered Subset Difference**: If the LSD scheme is used, then the group elements of a private key can be reduced from $O(\log^2 N)$ to $O(\log^{1.5} N)$
  - **Chosen-Ciphertext Security**: A CCA-secure PKRE scheme can be constructed by combining a CCA-secure SRE scheme with an one-time signature (OTS) scheme
  - **Trace and Revoke**: Our PKRE scheme provides the tracing property since it is derived from the subset cover framework of Naor *et al.*, but it can only trace to a subset pattern in some colluding scenarios

# Thank You