Advanced Cryptographic Primitives:
Lecture 7

Scribe: François Pirot

M2IF
Applications of (H)IBE to chosen-ciphertext security

0.1.1 Definition

Definition (Rackoff-Simon, Crypto’91 [1]) A public-key encryption scheme is secure against adaptive chosen-ciphertext attacks (IND-CCA2) if no PPT adversary \( A \) has non-negligible advantage on the following game:

1. The challenger generates \((PK, SK) \leftarrow \text{Keygen}(\lambda)\) and gives \( PK \) to \( A \).
2. \( A \) invokes the decryption oracle a polynomial number of times: at each query, \( A \) chooses a ciphertext \( C \) and obtains \( M \leftarrow \text{Decrypt}(SK, C) \) (which may be the error symbol \( \bot \) if \( C \) is an invalid ciphertext).
3. \( A \) chooses two messages \((M_0, M_1)\) and obtains \( C^* \leftarrow \text{Encrypt}(PK, M_\gamma) \), where \( \gamma \leftarrow \mathcal{U}\{0, 1\} \).
4. \( A \) makes new decryption queries on arbitrary ciphertexts \( C \neq C^* \).
5. \( A \) outputs \( \gamma' \in \{0, 1\} \) and wins if \( \gamma' = \gamma \)

\[
\text{Adv}^\text{IND-CCA}_A(\lambda) := \left| \Pr[\gamma' = \gamma] - \frac{1}{2} \right|
\]

Remark

- In a non-adaptive chosen-ciphertext attack (CCA1), stage 4 is removed (Naor-Yung, STOC’90): no decryption query is allowed after the challenge phase.
- Elgamal is not IND-CCA2-secure: \( A \) is given the challenge ciphertext

\[
C^* = (g^\gamma, M_\gamma \cdot X^\gamma) = (C_1, C_2)
\]

and can compute \( C' = (C_1 \cdot g'^{r'}, C_2 \cdot X'^{r'}) = (g^{\gamma+r'}, M_\gamma \cdot X^{\gamma+r'}) \), for a randomly chosen \( r' \in_R \mathbb{Z}_p \), which may be submitted to the decryption oracle and reveals \( M_\gamma \) to \( A \).

0.2 Generic IND-CCA2 PKE from any IND-sID-CPA-secure IBE (Canetti-Halevi-Katz, Eurocrypt’04)

- \textbf{Keygen}(\lambda) : Generate \((MPK, MSK) \leftarrow \text{Setup}^\text{IBE}(\lambda)\).

Choose a one-time signature scheme \( \Sigma = (G, S, V) \). Define \( PK := (MPK, \Sigma), SK := MSK \).

- \textbf{Encrypt}(PK, M) :

1. Generate a key pair \((SVK, SSK) \leftarrow G(\lambda)\) for the one-time signature.
2. Compute \( C^\text{IBE} \leftarrow \text{Encrypt}^\text{IBE}(MPK, M, SVK) \), which is an encryption of \( M \) under the identity \( SVK \).
3. Compute \( \sigma \leftarrow S(SSK, C^\text{IBE}) \) and output \( C = (SVK, C^\text{IBE}, \sigma) \).

- \textbf{Decrypt}(SK, C) :

1. Return \( \bot \) if \( V(SVK, C^\text{IBE}, \sigma) = 0 \).
2. Compute \( d_{SVK} \leftarrow \text{Keygen}^\text{IBE}(MSK, SVK) \).
3. Output \( M \leftarrow \text{Decrypt}^\text{IBE}(MPK, d_{SVK}, C^\text{IBE}) \).
Definition: Strong Unforgeability  A one-time signature $\Sigma = (G, S, V)$ is strongly unforgeable under chosen-message attacks (SUF-CMA) if no PPT adversary $A$ has noticeable advantage one the following game:

1. The challenger generates $(SVK, SSK) \leftarrow G(\lambda)$ and gives $SVK$ to $A$.
2. $A$ chooses exactly one message $M$ and obtains $\sigma \leftarrow S(SSK, M)$.
3. $A$ outputs $(M^*, \sigma^*)$ and wins if
   
   (a) $V(SVK, M^*, \sigma^*) = 1$
   
   (b) $(M^*, \sigma^*) \neq (M, \sigma)$

In many signature schemes, signatures are not unique (i.e., a given message has many valid signatures). For such schemes, the above notion is strictly stronger than the usual notion of unforgeability, where condition (b) is replaced by $M \neq M^*$.

Theorem  The PKE scheme produced by the Canetti-Halevi-Katz transformation is IND-CCA2-secure assuming that

- $\Sigma$ is strongly unforgeable
- The IBE scheme is IND-sID-CPA-secure

Proof  Let $C^* = (SVK^*, C^{IBE^*}, \sigma^*)$ be the challenge ciphertext given to the adversary in the IND-CCA2 game. We consider two kinds of attacks:

- Type I attack: $A$ makes at least one valid decryption query $C = (SVK, C^{IBE}, \sigma)$ such that $SVK \neq SVK^*$ (by “valid decryption query”, we mean one where the one-time signature $\sigma$ correctly verifies w.r.t. $SVK$).

- Type II attack: All valid decryption queries $C_i = (SVK_i, C_{IBE_i}^{IBE}, \sigma_i)$ contain one-time verification keys $SVK_i$ such that $SVK_i \neq SVK^*$.

Type I attack contradicts the SUF-CMA-security of $\Sigma$. The proof is straightforward and omitted here.

Let $A$ be Type II adversary with noticeable advantage $\varepsilon$. Using $A$, we build an IND-sID-CPA adversary $B$ against the IBE scheme:

- $B$ generates a one-time signature key pair $(SVK^*, SSK^*) \leftarrow G(\lambda)$ and declares $SVK^*$ as its target identity $ID^* = SVK^*$ in the IND-sID-CPA security game.

- $B$ obtains $MPK^{IBE}$ from its own challenger and gives $PK = (MPK^{IBE}, \Sigma)$ to $A$ as a public key for the IND-CCA security game.

Queries: suppose that $A$ queries the decryption of a ciphertext $C = (SVK, C^{IBE}, \sigma)$. Since $A$ is a Type II attacker, we necessarily have $SVK \neq SVK^*$, so that $B$ can obtain an IBE private key $d_{SVK} \leftarrow Keygen(MSK^{IBE}, SVK)$ from its challenger, and compute $M \leftarrow Decrypt^{IBE}(MPK^{IBE}, d_{SVK}, C)$.

Challenge: $A$ chooses $(M_0, M_1)$ which $B$ sends to its own challenger. The latter returns a challenge ciphertext $C^{IBE^*} \leftarrow Encrypt^{IBE}(MPK^{IBE}, M_*, SVK^*)$ for the IND-sID-CPA game. Then, $B$ computes $C^* = (SVK^*, C^{IBE^*}, \sigma^*)$ where $\sigma^* \leftarrow S(SSK^*, C^{IBE^*})$ and gives it as a challenge to $A$.  

2
Output $A$ outputs $\gamma' \in \{0,1\}$ and $B$ outputs $\gamma'$.

Clearly, if $A$ is successful in the IND-CCA game, so is $B$ in the IND-sID-CPA game. □

**Remark** The CHK transform turns any 2-level HIBE with an IND-sID-CCA2-secure IBE scheme.

### 0.3 Attribute-based encryption and fuzzy IBE

#### 0.3.1 Definition

**Definition: Fuzzy IBE (Sahai-Waters, Eurocrypt’05 [3])**

- Decryption works when identities of ciphertext/key are close enough
- Identities are sets of descriptive attributes (“student”, “EU citizen”, “Driving license holder”, etc)
- If a ciphertext is encrypted for an attribute set $\omega'$ and private key corresponds to attribute set $\omega$, decryption works if $|\omega \cap \omega'| \geq d$ for some $d \in \mathbb{N}$.

**Motivation:**
- Use biometric identities (e.g., iris scan)
- Access control on encrypted data (e.g., at least 2 attributes among “research staff member”, “Patent engineer”, “CEO”)

**Selective security:** Let $d \in \text{poly}(\lambda)$ be the decryption threshold.

0. The adversary $A$ chooses a target attribute set $\omega^*$
1. The challenger generates $(\text{MPK}, \text{MSK}) \leftarrow \text{Setup}(\lambda, d)$ and gives $\text{MPK}$ to $A$
2. $A$ makes private key queries: $A$ chooses an arbitrary attribute set $\omega$ such that $|\omega \cap \omega'| < d$, and obtains $d_\omega \leftarrow \text{Keygen}(\text{MSK}, \omega)$.
3. $A$ chooses $(M_0, M_1)$ and obtains $C \leftarrow \text{Encrypt}(\text{MPK}, M_\gamma, \omega^*)$ with $\gamma \leftarrow \mathcal{U}(\{0,1\})$
4. $A$ makes more private key queries
5. $A$ outputs a bit $\gamma' \in \{0,1\}$ and wins if $\gamma = \gamma'$. Again, $A$ ’s advantage is defined to be

$$\text{Adv}_A^{\text{FIBE-CPA}}(\lambda) := \left| \Pr[\gamma' = \gamma] - \frac{1}{2} \right|$$

In the stronger notion of full (a.k.a. adaptive) security, the adversary chooses $\omega^*$ at step 3 at the same time as $M_0, M_1$. 

3
0.3.2 Construction for large attribute universes
(Sahai-Waters, Eurocrypt’05 [3])

- **Setup** $(\lambda, d)$:
  1. Choose cyclic groups $(G, G_T)$ of prime order $p > 2^\lambda$ with a bilinear map $e : G \times G \to G_T$ and generators $g, g_2 \in G$.
  2. Choose $y \leftarrow \mathbb{Z}_p$ and computes $g_1 := g^y$.
  3. Choose a function $T : \mathbb{Z}_p \to G$ (to be defined later)

Set $MPK := ((G, G_T), g, g_1 (= g^y), g_2, T)$ and $MSK := y \in \mathbb{Z}_p$.

- **Keygen** $(MSK, \omega)$:
  Choose a random polynomial $q(X) \in \mathbb{Z}_p[X]$ of degree $d - 1$ such that $q(0) = y$.

For each $i \in \omega$, choose $r_i \leftarrow \mathbb{Z}_p$ and compute $(D_i, d_i) = (g_2^{q(i)} \cdot T(i)^{r_i}, g^{r_i})$.

Return the private key $d_\omega := \{(D_i, d_i)\}_{i \in \omega}$.

Note that, for each $i \in \omega$, the pair $(D_i, d_i)$ satisfies the relation

$$e(D_i, g) = e(g, g_2)^{q(i)} \cdot e(T(i), d_i). \quad (1)$$

- **Encrypt** $(MPK, M, \omega')$:
  To encrypt $M \in G_T$ under the attribute set $\omega'$, choose $s \leftarrow \mathbb{Z}_p$ and compute

$$CT = (\omega', E' = M \cdot e(g_1, g_2)^s, E = g^s, \{E_i = T(i)^s\}_{i \in \omega'}).$$

- **Decrypt** $(MPK, d_\omega, CT)$:
  Given $d_\omega = \{(D_i, d_i)\}_{i \in \omega}$, find a set $S \subseteq \omega \cap \omega'$ such that $|S| = d$ (or return $\perp$ if none exists). For each $i \in S$, compute

$$\frac{e(D_i, E)}{e(E_i, d_i)} = e(g, g_2)^{q(i) \cdot s}. \quad (2)$$

Since $e(g, g_2)^{q(0) \cdot s} = e(g_1, g_2)^s$, if we define the function

$$\Delta_{i,S}(X) := \prod_{j \in S \atop j \neq i} \frac{X - j}{i - j},$$

the message $M$ can be obtained by performing a Lagrange interpolation in the exponent and computing

$$M = \prod_{i \in S} \left( \frac{E'}{e(D_i, E)} \right)^{\Delta_{i,S}(0)}.$$

The correctness of the scheme can be verified by observing that, if we raise both members of (1) to the power $s \in \mathbb{Z}_p$, we obtain (2).

**Theorem** The scheme provides selective security if the DBDH assumption holds.
Proof. Let $\mathcal{A}$ be selective adversary with advantage $\varepsilon$. We build a DBDH distinguisher $\mathcal{B}$ with advantage $\varepsilon$. Algorithm $\mathcal{B}$ takes as input $(g, g^a, g^b, g^c, Z)$ and uses $\mathcal{A}$ to decide if $Z = e(g, g)^{abc}$ or $Z \in_R G_T$.

The adversary $\mathcal{A}$ first chooses a target attribute set $\omega^*$. To generate $MPK$, $\mathcal{B}$ defines $g_1 = g^a, g_2 = g^b$ and chooses the function $T : Z_p \rightarrow G$ in such a way that $\forall x \in Z_p$, we can write

$$T(x) = g_2^{F(x)} \cdot g_1^J(x),$$

for certain functions $F, J : Z_p \rightarrow Z_p$ (which are kept internal to $\mathcal{B}$) chosen such that

$$F(x) = 0 \text{ if and only if } x \in \omega^*.$$ 

The adversary $\mathcal{A}$ is given $MPK := ((G, G_T), g, g_1(= g^a), g_2(= g^b), T)$, which implicitly defines $MSK := a$ (note that $MSK$ is not available to $\mathcal{B}$).

**Queries:** suppose that $\mathcal{A}$ queries a private key for $\omega$ such that $|\omega \cap \omega^*| < d$. Let $\Gamma = \omega \cap \omega^*$, and $\Gamma'$ be any set such that $\Gamma \subseteq \Gamma' \subseteq \omega$, and $|\Gamma'| = d - 1$.

- For each $i \in \Gamma' \subseteq \omega^*$, chooses $\lambda_i, r_i \in Z_p$, and sets $D_i := g_2^{\lambda_i} \cdot T(i)^{r_i} \quad d_i := g^{r_i}$.

- For each $i \in \omega \setminus \Gamma'$, we know that $i \notin \omega^*$ and we thus have $T(i) = g_2^{F(i)} \cdot g_1^{J(i)}$ with $F(i) \neq 0$. Hence, $\mathcal{B}$ can compute

$$D' = g_2^{g(i)} \cdot T(i)^{\tilde{r}} = T(i)^{\tilde{r}} \cdot (g^a)^{-\frac{J(i)}{F(i)}} \quad d' = g^\tilde{r} = g^r \cdot (g^a)^{-\frac{1}{F(i)}}$$

where $\tilde{r} = r - \frac{a}{F(i)}$ for a randomly chosen $r \in_R Z_p$. In turn, this allows $\mathcal{B}$ to compute

$$D_i = D_i^{\Delta_0,s(i)} \cdot \prod_{j \in S} g_2^{\lambda_j \Delta_j,s(i)} \quad d_i = d_i^{\Delta_0,s(i)}$$

where $S = \Gamma' \setminus \{0\}$. Then, $\mathcal{B}$ can return the complete private key $d_\omega = \{(D_i, d_i) = (g_2^{g(i)} \cdot T(i)^{r_i}, g^{r_i})\} = \omega$ to $\mathcal{A}$.

**Challenge:** $\mathcal{A}$ chooses two messages $M_0, M_1 \in G_T$. At this point, $\mathcal{B}$ picks $\gamma \leftarrow \{0, 1\}$ and computes

$$CT^* = (\omega^*, E^* = M_\gamma \cdot Z, E = g^c, \{E_i = (g^c)^{J(i)}\} = \omega^*).$$

If $Z = e(g, g)^{abc}$ then $CT^* = (\omega^*, E' = M_\gamma \cdot e(g_1, g_2)^c, E = g^c, \{E_i = T(i)^c\}) = \omega^*$, since $T(i) = g^{J(i)}$ for each $i \in \omega^*$. If $Z \in_R G_T$, we can write

$$CT^* = (\omega^*, E' = M_{\text{rand}} \cdot e(g_1, g_2)^c, E = g^c, \{E_i = T(i)^c\} = \omega^*),$$

for some uniformly random $M_{\text{rand}} \in_R G_T$.
\textbf{Output:} \( A \) outputs a bit \( \gamma' \in \{0,1\} \). Then, \( B \) outputs 1 (meaning that \( Z = e(g,g)^{abc} \)) if \( \gamma' = \gamma \). Otherwise, \( B \) outputs 0 (meaning that \( Z \in_R G_T \)). It should be clear that \( B \)'s advantage as a DBDH distinguisher is identical to \( A \)'s advantage \( \varepsilon \) as a selective adversary.

\[ \Box \]

In order to choose the function \( T : \mathbb{Z}_p \rightarrow G \), one possibility is to fix an upper bound \( n \) on the cardinality of any attribute set \( \omega \) in the scheme. The function \( T \) can be defined so as to implicitly compute a polynomial of degree \( n \) in the exponent. Namely, the master public key includes random group elements \( u_0, u_1, \ldots, u_n \in_R G \) and we define \( T(x) = \prod_{i=0}^{n} u_i^{(x^i)} \) for any \( x \in \mathbb{Z}_p \). In the security proof, the reduction \( B \) can choose \( F(x) \) as the polynomial \( F[X] = \prod_{i \in \omega^*}(X - i) = \sum_{i=0}^{n} f_i X^i \) and set \( u_i = g f_i^2 \cdot g t_i \), for each \( i \in \{0, \ldots, n\} \), using randomly chosen \( t_0, t_1, \ldots, t_n \in_R \mathbb{Z}_p \). This guarantees that \( \{u_i\}_{i=0}^{n} \) have a uniform distribution.

### 0.4 Extension: Key-Policy Attribute-based encryption (KP-ABE)

- Ciphertext is labeled with an attribute set \( \omega \).
- Private key corresponds to an access policy \( P \) and decryption works iff \( P(\omega) = 1 \).

\textbf{Motivation} Fine-grained access control using complex policies

Example of policy \( P \):

(“Research staff” OR “Patent engineer” OR “CEO”) AND (“Hired at least one year ago”)

FIBE is a particular case of KP-ABE: \( P \) consists of a single gate | \( \text{AND gate} \)
| \( \text{OR gate} \)
| \( \text{threshold gate} \)
Bibliography

Lecture Notes in Computer Science Volume 576, 1992, pp 433-444
Advances in Cryptology — CRYPTO ’91


Springer, Heidelberg (2005)