

Identity and Attribute-Based Encryption: Part 2

Benoît Libert

UCL Crypto Group, Belgium

`benoit.libert@uclouvain.be`

September 28th 2010

Overview

- Overview of HIBE schemes before 2009
- The Dual System paradigm
 - General principle
 - Waters' fully secure (H)IBE under simple assumptions
 - The Lewko-Waters HIBE
 - Extensions
- Other applications
 - Fully secure identity-based broadcast encryption
 - Revocation schemes with short ciphertexts.

1 Review of Hierarchical IBE schemes

- Several HIBE appeared in the last decade:
 - Partial collusion-resistance (Horwitz-Lynn, Eurocrypt'02)
 - Using random oracles (Gentry-Silverberg, Asiacrypt'02)
 - Selective-security (Boneh-Boyen, Eurocrypt'04) and adaptive security with few levels (Waters, Eurocrypt'05)
 - With short ciphertexts (Boneh-Boyen-Goh, Eurocrypt'05)
 - With anonymous ciphertexts (Boyen-Waters, Crypto'06)
- ...but all of them are only selectively secure or suffer from an exponential security degradation in the number of levels
 \Rightarrow they only support a (small) constant number of levels.

Before 2009, all HIBE schemes were based on the *partitioning* paradigm:

- The identity space is *divided* into two subspaces
 - a. Identities for which the reduction can compute private keys
 - b. Identities that can be used to build a “challenge ciphertext” by embedding a problem instance in it.
- The reduction generates parameters hoping that
 1. Identities queried for key generation will fall into class a.
 2. The “challenge identity” will fall into category b.
- Typically, condition 2 is only satisfied with probability $\delta = O(1/\text{poly}(\lambda)) < 1$ *at each level* of the hierarchy.

 \Rightarrow Security degradation becomes δ^L for L levels.

- Before 2009, all HIBE schemes were based on *partitioning* ...
- ... except Gentry's IBE (Eurocrypt'06)
 - Security proof features a tight reduction.
 - But the scheme does not scale into a multi-level HIBE.
 - Security relies on a non-standard “ q -type” assumption:
Given $(g, g^\alpha, \dots, g^{(\alpha^q)}, h, h^{(\alpha^{q+2})})$, $T = e(g, h)^{(\alpha^{q+1})}$ is indistinguishable from random.
- In 2009, Gentry and Halevi (TCC'09) presented a HIBE with a meaningful reduction for polynomially-many levels.
 - Similarities with Gentry's IBE and departs from the partitioning approach.
 - Security relies on a strong q -type assumption.

- Waters (Crypto'09) introduced *dual system* encryption.
 - Yields HIBE schemes with full security for a polynomial number of levels
 - Simpler constructions and security under simple assumptions:

Decision Bilinear Diffie-Hellman (DBDH) problem:

Given $(g, g^a, g^b, g^c, T) \in \mathbb{G}^4 \times \mathbb{G}_T$, decide if $T = e(g, g)^{abc}$.

Decision Linear (DLIN) problem: Given

$(g, g^a, g^b, g^{ac}, g^{bd}, \eta) \in \mathbb{G}^6$, decide if $\eta = g^{c+d}$.

- Later on, Lewko and Waters (TCC'10) refined the approach:
 - Even simpler constructions (conceptually close to selectively-secure schemes like Boneh-Boyen).
 - Gives fully secure HIBE with constant-size ciphertexts
 - ... under simple assumptions in groups of *composite* order.

2 The Dual System Paradigm

- Uses a sequence of games where
 - Game_{real} proceeds like the real attack.
 - Game_{final} leaves no advantage to the adversary.
- Intermediate games $\text{Game}_1, \dots, \text{Game}_q$ are organized such that
 - Adversary's view is modified step by step.
 - Under some decisional assumption, Game_i is indistinguishable from Game_{i-1} for $1 \leq i \leq q$.
- From Game_q , proving the security is much easier (transition based on indistinguishability between Game_q and Game_{final}).

The dual encryption paradigm:

At each step of the proof,

- Ciphertexts and private keys can be either
 - Normal (as in the real scheme).
 - Semi-functional: have a slightly modified (but typically indistinguishable) distribution w.r.t. the real scheme.
- Semi-functional ciphertexts always decrypt under normal keys.
- Semi-functional keys can always decrypt normal ciphertexts.
- ...but attempts to decrypt semi-functional ciphertexts using a semi-functional key fail.

The dual encryption paradigm:

Interaction between the two types of ciphertext/keys for the *same* identity upon decryption:

Private keys	Normal	Semi-functional
Ciphertexts		
Normal	Succeeds	Succeeds
Semi-functional	Succeeds	Fails

Figure 1: Results of decryption attempts

General principle:

- Game_{real} : is like the real attack game.
- Game_0 : challenge ciphertext is made *semi-functional*.
- Game_i ($1 \leq i \leq q$):
 - Challenge ciphertext remains semi-functional.
 - Private key queries:
 - For $1 \leq j \leq i$, private keys SK_{ID_j} are semi-functional.
 - For $i + 1 \leq j \leq q$, private keys SK_{ID_j} are normal.
- In Game_q , challenge ciphertext and all private keys are semi-functional.
- Transition between Game_q and Game_{final} is easy.

General principle: a subtlety.

- In Game_{*i*} ($1 \leq i \leq q$):
 - Challenge ciphertext C^* is semi-functional.
 - Private keys $SK_{ID_1}, \dots, SK_{ID_i}$ are semi-functional.
 - Private keys $SK_{ID_{i+1}}, \dots, SK_{ID_q}$ are normal.
- Challenger is able to compute private keys for *all* identities.
- Game_{*i*} only differs from Game_{*i-1*} in the shape of the i^{th} key.
 \Rightarrow How can Game_{*i*} be indistinguishable from Game_{*i-1*} while the challenger can attempt to decrypt C^* by itself?
- To resolve this
 - Ciphertext and keys contain tags tag_c and tag_k such that decryption works when $tag_c \neq tag_k$.
 - In Game_{*i-1*}/Game_{*i*}, challenger can *only* generate a private key such that $tag_k = tag_c$, where tag_c is the tag in C^* .

Fully secure (H)IBE: strategy of the proof:

- Game_{real} : real attack game
- Game_0 : ciphertext C^* becomes *semi-functional*. Under the DLIN assumption, adversary's behavior is about the same.
- $\text{Game}_{i-1}/\text{Game}_i$ ($1 \leq i \leq q$): challenge C^* is semi-functional.
 - For $1 \leq j < i$, private keys SK_{ID_j} are semi-functional.
 - For $i + 1 \leq j \leq q$, private keys SK_{ID_j} are normal.
 - Answer to the i^{th} query contains a DLIN instance $(g, g^a, g^b, g^{ac}, g^{bd}, \eta \stackrel{?}{=} g^{c+d})$.
- In Game_q , ciphertext C^* and keys are all semi-functional.
- $\text{Game}_q/\text{Game}_{final}$: challenge C^* contains a DBDH instance $(g, g^a, g^b, g^c, \eta \stackrel{?}{=} e(g, g)^{abc})$

Fully Secure HIBE: (Waters, Crypto'09)

- Gives a fully secure HIBE with polynomially-many levels based on DLIN and DBDH.
- Ciphertexts have linear length in the depth of the hierarchy
- Uses tags in ciphertexts and keys (decryption works when tags are different).
- Due to the use of tags, the same technique does not apply to get short ciphertexts (cf. Boneh-Boyen-Goh, Eurocrypt'05).
- How can one get $O(1)$ -size ciphertexts?

Fully Secure HIBE with Short Ciphertexts: use of composite order groups (Lewko-Waters, TCC'10).

- Does not use tags.
⇒ Ciphertext compression is possible.
- Uses bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ whose order is a product $N = p_1 p_2 p_3$ of three primes and assumptions related to the hardness of factoring the group order.

N.B. for each $i \neq j \in \{1, 2, 3\}$ and all $g_i \in \mathbb{G}_{p_i}, g_j \in \mathbb{G}_{p_j},$

$$e(g_i, g_j) = 1_{\mathbb{G}_T}.$$

Ex.: $e(g_{p_1}, g_{p_2}) = e(g_N^{x p_2 p_3}, g_N^{y p_1 p_3}) = e(g_N, g_N)^{x y p_1 p_2 p_3^2} = 1_{\mathbb{G}_T}$

- Also uses semi-functional ciphertext and private keys in the security proof.

Fully Secure HIBE with Short Ciphertexts:

Uses bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of order $N = p_1 p_2 p_3$ and assumes the intractability of the following problems.

1. Let $g \xleftarrow{R} \mathbb{G}_{p_1}, X_3 \xleftarrow{R} \mathbb{G}_{p_3}$. Given $(g, X_3) \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_3}$ and $T \in \mathbb{G}$, decide if $T \in \mathbb{G}_{p_1 p_2}$ or $T \in \mathbb{G}_{p_1}$.
2. Let $g, X_1 \xleftarrow{R} \mathbb{G}_{p_1}, X_2, Y_2 \xleftarrow{R} \mathbb{G}_{p_2}, Y_3, Z_3 \xleftarrow{R} \mathbb{G}_{p_3}$. Given elements

$$(g, Z_3, X_1 X_2, Y_2 Y_3)$$

and $T \in \mathbb{G}$, decide if $T \in_R \mathbb{G}_{p_1 p_2 p_3}$ or $T \in_R \mathbb{G}_{p_1 p_3}$.

3. Let $g \xleftarrow{R} \mathbb{G}_{p_1}, X_2, Y_2, Z_2 \xleftarrow{R} \mathbb{G}_{p_2}, X_3 \xleftarrow{R} \mathbb{G}_{p_3}$ and $\alpha, s \xleftarrow{R} \mathbb{Z}_N$. Given elements

$$(g, Z_2, X_3, g^\alpha X_2, g^s Y_2)$$

and $T \in \mathbb{G}_T$, decide if $T = e(g, g)^{\alpha s}$ or $T \in_R \mathbb{G}_T$.

Application to the Boneh-Boyen IBE:

- **Setup:** chooses groups $(\mathbb{G}, \mathbb{G}_T)$ of order $N = p_1 p_2 p_3$, $g, u, v \xleftarrow{R} \mathbb{G}_{p_1}$, $X_3 \xleftarrow{R} \mathbb{G}_{p_3}$, $\alpha \xleftarrow{R} \mathbb{Z}_N$ and sets

$$MPK = (g, u, v, e(g, g)^\alpha, X_3).$$

The master key is $MSK = g^\alpha$.

- **Extract:** picks $r \xleftarrow{R} \mathbb{Z}_N$, $R_3, R'_3 \xleftarrow{R} \mathbb{G}_{p_3}$ and computes

$$SK_{ID} = (D_1, D_2) = (g^\alpha \cdot (u^{ID} \cdot v)^r \cdot R_3, g^r \cdot R'_3).$$

- **Encrypt:** picks $s \xleftarrow{R} \mathbb{Z}_N$ and computes

$$(C_0, C_1, C_2) = (M \cdot e(g, g)^{\alpha \cdot s}, g^s, (u^{ID} \cdot v)^s).$$

- **Decrypt:** computes

$$e(g, g)^{\alpha \cdot s} = \frac{e(C_1, D_1)}{e(C_2, D_2)}.$$

Strategy of the proof: use two types of ciphertext/keys

- Ciphertexts can be either **Normal** or **Semi-functional**:

$$C_0 = M \cdot e(g, g)^{\alpha s}, \quad C_1 = g^s \cdot \mathbf{g}_2^{\mathbf{x}}, \quad C_2 = (u^{\text{ID}} \cdot v)^s \cdot \mathbf{g}_2^{\mathbf{x} \cdot \mathbf{z}_c}$$

- Private keys can be either **Normal** or **Semi-functional**:

$$D_1 = g^\alpha \cdot (u^{\text{ID}} \cdot v)^r \cdot \mathbf{g}_2^{\mathbf{y} \cdot \mathbf{z}_k} \cdot R_3, \quad D_2 = g^r \cdot \mathbf{g}_2^{\mathbf{y}} \cdot R'_3.$$

- If ciphertexts/keys are both semi-functional, decryption gives

$$\frac{e(C_1, D_1)}{e(C_2, D_2)} = e(g, g)^{\alpha \cdot s} \cdot \mathbf{e}(\mathbf{g}_2, \mathbf{g}_2)^{\mathbf{x}(\mathbf{z}_k - \mathbf{z}_c)},$$

which is correct when $z_k = z_c$ (*nominally* semi-functional key).

Strategy of the proof: gradually move to a game where all keys and the challenge ciphertext are semi-functional.

- Game_{real} : real attack game
- Game_0 : ciphertext C^* becomes *semi-functional*. Adversary does not see the difference under some appropriate assumption.
- $\text{Game}_{i-1}/\text{Game}_i$ ($1 \leq i \leq q$): challenge C^* is semi-functional.
 - For $1 \leq j < i$, private keys SK_{ID_j} are semi-functional.
 - For $i + 1 \leq j \leq q$, private keys SK_{ID_j} are normal.
 - Answer to the i^{th} query contains a problem instance.
- In Game_q , ciphertext C^* and keys are all semi-functional.
- $\text{Game}_q/\text{Game}_{final}$: challenge C^* contains an instance of another decisional problem.

Sketch of the proof: transition $\text{Game}_{real}/\text{Game}_0$.

- Challenge ciphertext is made semi-functional:

$$C_0 = M_d \cdot e(g, g)^{\alpha \cdot s}, \quad C_1 = g^s \cdot \mathbf{g}_2^{\mathbf{x}}, \quad C_2 = (u^{\text{ID}} \cdot v)^s \cdot \mathbf{g}_2^{\mathbf{x} \cdot \mathbf{z}_c}$$

- Relies on **Assumption 1**: given $(g, X_3) \in \mathbb{G}_{p_1} \times \mathbb{G}_{p_3}$, it is hard to distinguish $T \in_R \mathbb{G}_{p_1 p_2}$ from $T \in_R \mathbb{G}_{p_1}$.

The reduction:

- Takes as input (g, X_3, T) and prepares public parameters $MPK = (g, u = g^a, v = g^b, e(g, g)^\alpha, X_3)$ with $a, b, \alpha \xleftarrow{R} \mathbb{Z}_N$.
- Can answer all private key queries using $MSK = g^\alpha$
- The challenge ciphertext

$$C_0 = M_d \cdot e(T, g)^\alpha, \quad C_1 = T, \quad C_2 = T^{a \cdot \text{ID}^* + b},$$

is semi-functional with $z_c = a \cdot \text{ID}^* + b \pmod{p_2}$ if $T \in_R \mathbb{G}_{p_1 p_2}$.

Sketch of the proof: transition $\text{Game}_i/\text{Game}_{i+1}$.

- The $(i + 1)^{\text{th}}$ private key becomes semi-functional:

$$D_1 = g^\alpha \cdot (u^{\text{ID}} \cdot v)^r \cdot \mathbf{g}_2^{\mathbf{xz}_k} \cdot R_3, \quad D_2 = g^r \cdot \mathbf{g}_2^{\mathbf{x}} \cdot R'_3$$

- Relies on **Assumption 2**: given (g, X_3, X_1X_2, Y_2Y_3) , it is hard to distinguish $T \in_R \mathbb{G}_{p_1p_2p_3}$ from $T \in_R \mathbb{G}_{p_1p_3}$.

The reduction:

- Takes as input (g, X_3, X_1X_2, Y_2Y_3) and prepares $MPK = (g, u = g^a, v = g^b, e(g, g)^\alpha, X_3)$ with $a, b, \alpha \xleftarrow{R} \mathbb{Z}_N$.
- Challenge ciphertext is semi-functional

$$C_0 = M_d \cdot e(X_1X_2, g)^\alpha, \quad C_1 = X_1X_2, \quad C_2 = (X_1X_2)^{a \cdot \text{ID}^* + b},$$

with $s = \log_g(X_1)$, $z_c = a \cdot \text{ID}^* + b \pmod{p_2}$.

- Sets the $(i + 1)^{\text{th}}$ key as $(D_1, D_2) = (g^\alpha \cdot T^{a \cdot \text{ID} + b}, T)$, which is semi-functional with $z_k = a \cdot \text{ID} + b \pmod{p_2}$ if $T \in \mathbb{G}_{p_1p_2p_3}$.

Sketch of the proof: transition $\text{Game}_q/\text{Game}_{final}$.

- Ciphertext and all keys are now semi-functional.
- Relies on **Assumption 3**: given $(g, Z_2, Z_3, g^\alpha X_2, g^s Y_2)$, it is hard to distinguish $\eta = e(g, g)^{\alpha \cdot s}$ from $\eta \in_R \mathbb{G}_T$.

The reduction:

- Takes as input $(g, Z_2, Z_3, g^\alpha X_2, g^s Y_2)$ and prepares

$$MPK = (g, u = g^a, v = g^b, e(g, g)^\alpha = e(g^\alpha X_2, g), Z_3)$$

with $a, b \xleftarrow{R} \mathbb{Z}_N$.

- Generate semi-functional keys using $g^\alpha X_2$.
- The challenge ciphertext

$$C_0 = M_d \cdot \eta, \quad C_1 = g^s Y_2, \quad C_2 = (g^s Y_2)^{a \cdot \text{ID}^* + b},$$

which perfectly hides M_d if $\eta \in_R \mathbb{G}$.

Extension: tweaks the Boneh-Boyen-Goh HIBE to get full security under the same assumptions.

- **Setup**(L): chooses groups $(\mathbb{G}, \mathbb{G}_T)$ of order $N = p_1 p_2 p_3$, $g \xleftarrow{R} \mathbb{G}_{p_1}$, $h_0, h_1, \dots, h_L \xleftarrow{R} \mathbb{G}_{p_1}$, $X_3 \xleftarrow{R} \mathbb{G}_{p_3}$, $\alpha \xleftarrow{R} \mathbb{Z}_N$ and sets

$$MPK = (g, \{h_i\}_{i=0}^L, e(g, g)^\alpha, X_3).$$

The master key is $MSK = g^\alpha$.

- **Extract**($MSK, (ID_1, \dots, ID_\ell)$): picks $r \xleftarrow{R} \mathbb{Z}_N$, $R_3, R'_3 \xleftarrow{R} \mathbb{G}_{p_3}$, $R_{3,\ell+1}, \dots, R_{3,L} \xleftarrow{R} \mathbb{G}_{p_3}$ and computes

$$SK = \left(\underbrace{g^\alpha \cdot (h_0 \cdot h_1^{ID_1} \cdots h_\ell^{ID_\ell})^r \cdot R_3, g^r \cdot R'_3}_{\text{Decryption component}}, \underbrace{h_{\ell+1}^r \cdot R_{3,\ell+1}, \dots, h_L^r \cdot R_{3,L}}_{\text{Delegation component}} \right).$$

- **Encrypt**($MPK, (ID_1, \dots, ID_\ell)$): picks $s \xleftarrow{R} \mathbb{Z}_N$ and computes

$$(C_0, C_1, C_2) = (M \cdot e(g, g)^{\alpha \cdot s}, g^s, (h_0 \cdot h_1^{ID_1} \cdots h_\ell^{ID_\ell})^s).$$

Other extensions: attribute-based and predicate encryption

- Fully secure key-policy and ciphertext-policy attribute-based encryption:
 - In composite order groups for monotonic access structures (Lewko-Okamoto-Sahai-Takashima-Waters, Eurocrypt'10)
 - In prime order groups for non-monotonic access structures (Okamoto-Takashima, Crypto'10).
- Fully secure attribute-hiding predicate encryption (Lewko-Okamoto-Sahai-Takashima-Waters, Eurocrypt'10)
 - In prime order groups under q -type assumptions (Lewko-Okamoto-Sahai-Takashima-Waters, Eurocrypt'10)
 - In prime order groups using simple assumptions (Okamoto-Takashima, Crypto'10)

3 Applications to Identity-Based Broadcast Encryption and Revocation

Identity-Based Broadcast Encryption (IBBE): allows encrypting to several receivers using their identities.

- With selective security and constant-size ciphertexts
 - Quadratic-size private keys (Abdalla-Kiltz-Neven, ESORICS'07), linear-size private keys (Boneh-Hamburg, Asiacrypt'08), short private keys under a strong assumption (Delerablée, Asiacrypt'07).
- With adaptive security
 - Short ciphertexts in the random oracle model or sublinear-size ciphertexts (Gentry-Waters, Eurocrypt'09)

Applications to Identity-Based Broadcast Encryption:

- Dual encryption systems give fully secure IBBE with $O(1)$ -size ciphertexts (Attrapadung-Libert, PKC'10):
 - Simple constructions in groups of composite order:
Fully secure tweaks of Boneh-Hamburg (linear-size private keys), generalizes into *spatial encryption*.
 - Constructions based on DLIN and DBDH assumptions in prime order groups: first IBBE scheme based on *simple* assumptions with short ciphertexts.
- (Identity-based) revocation: anyone holding a private key for an identity *outside* the list attached to the ciphertext can decrypt
 - Short ciphertexts with non-adaptive security
 - Tradeoff schemes generalizing Lewko-Sahai-Waters (Security & Privacy 2010).

Fully Secure IBBE with short ciphertexts: [AL'10]

- Simple realization in composite order groups (special case of spatial encryption)
- More efficient variants in prime order groups using tags.
- Uses inner products (like Katz-Sahai-Waters, Eurocrypt'08, but without anonymity):
 - Ciphertext and keys corresponds to attribute vectors $\vec{X} = (x_1, \dots, x_n)$ and $\vec{Y} = (y_1, \dots, y_n)$.
 - Decryption works when $\vec{X} \cdot \vec{Y} = 0$.
- Gives IBBE by defining $P[Z] = \prod_{ID_j \in S} (Z - ID_j)$ where $S = \{ID_1, \dots, ID_s\}$ is the receiver set.
 - $\vec{X} = (x_1, \dots, x_n)$ contains the coefficients of $P[Z]$.
 - The private key SK_{ID} defines $\vec{Y} = (y_1, \dots, y_n)$ where $y_i = ID^{i-1}$ for $i = 1$ to n .

Fully Secure IBBE with short ciphertexts: [AL'10]

- **Setup**(n): chooses groups $(\mathbb{G}, \mathbb{G}_T)$ of order $N = p_1 p_2 p_3$, $g \xleftarrow{R} \mathbb{G}_{p_1}$, $h_0, h_1, \dots, h_n \xleftarrow{R} \mathbb{G}_{p_1}$, $X_3 \xleftarrow{R} \mathbb{G}_{p_3}$, $\alpha \xleftarrow{R} \mathbb{Z}_N$ and sets

$$MPK = (g, \{h_i\}_{i=0}^n, e(g, g)^\alpha, X_3).$$

The master key is $MSK = g^\alpha$.

- **Encrypt**($MPK, \vec{X} = (x_1, \dots, x_n)$): picks $s \xleftarrow{R} \mathbb{Z}_N$ and sets

$$(C_0, C_1, C_2) = (M \cdot e(g, g)^{\alpha \cdot s}, g^s, (h_0 \cdot h_1^{x_1} \cdots h_n^{x_n})^s).$$

- **Extract**($MSK, \vec{Y} = (y_1, \dots, y_n)$): picks $r \xleftarrow{R} \mathbb{Z}_N$, $R_3, R'_3 \xleftarrow{R} \mathbb{G}_{p_3}$, $R_{3,1}, \dots, R_{3,n} \xleftarrow{R} \mathbb{G}_{p_3}$ and computes

$$SK_{\vec{Y}} = (g^\alpha \cdot h_0^r \cdot R_3, g^r \cdot R'_3, (h_0^{y_1} \cdot h_1)^r \cdot R_{3,1}, \dots, (h_0^{y_n} \cdot h_n)^r \cdot R_{3,n}).$$

Fully Secure IBBE with short ciphertexts: [AL'10]

- Private keys have the form

$$\begin{aligned} SK_{\vec{Y}} &= (D_1, D_2, K_1, \dots, K_n) \\ &= \left(g^\alpha \cdot h_0^r \cdot R_3, g^r \cdot R'_3, (h_0^{y_1} \cdot h_1)^r \cdot R_{3,1}, \dots, (h_0^{y_n} \cdot h_n)^r \cdot R_{3,n} \right). \end{aligned}$$

\Rightarrow Computing $K = D_1 \cdot \prod_{i=1}^n K_i^{x_i}$ gives a pair

$$\begin{aligned} (K, D_2) &= \left(g^\alpha \cdot (h_0^{1+\vec{X} \cdot \vec{Y}} \cdot h_1^{x_1} \dots h_n^{x_n})^r \cdot \tilde{R}_3, g^r \cdot \tilde{R}'_3 \right) \\ &= \left(g^\alpha \cdot (h_0 \cdot h_1^{x_1} \dots h_n^{x_n})^r \cdot \tilde{R}_3, g^r \cdot \tilde{R}'_3 \right) \end{aligned}$$

To decrypt

$$(C_0, C_1, C_2) = \left(M \cdot e(g, g)^{\alpha \cdot s}, g^s, (h_0 \cdot h_1^{x_1} \dots h_n^{x_n})^s \right)$$

decryption computes $e(g, g)^{\alpha \cdot s} = \frac{e(C_1, K)}{e(C_2, D_2)}$.

Generalization to fully secure spatial encryption: [AL'10]

- Spatial encryption (Boneh-Hamburg, Asiacrypt'08):
 - Ciphertexts corresponds to a vector \vec{X} .
 - Private keys correspond to affine subspaces
 $V = \text{Aff}(M, \vec{c}) = \{M\vec{w} + \vec{c} \mid \vec{w} \in \mathbb{Z}_p^d\}$ for some $M \in \mathbb{Z}_p^{n \times d}$.
 - Decryption works iff $\vec{X} \in V$.
 - A private key SK_{V_1} for the subspace V_1 allows deriving SK_{V_2} for subspace V_2 iff $V_2 \subset V_1$.
- Boneh-Hamburg gave a selectively secure construction based on the Boneh-Boyen-Goh HIBE.
- Lewko-Waters makes it fully secure [AL10] in groups of composite order.
- Open problem: delegatable fully secure spatial encryption using simple assumptions in prime order groups.

Revocation with short ciphertexts: [AL'10]

- Revocation was suggested by Naor-Pinkas (FC'00) and improved by Lewko-Sahai-Waters (IEEE S&P 2010).
- Sender associates the ciphertext with a list $S = \{\text{ID}_1, \dots, \text{ID}_s\}$ of *revoked* identities.
- Decryption works using any SK_{ID} such that $\text{ID} \notin S$.
- [AL'10] also uses inner products: ciphertext and keys correspond to attribute vectors $\vec{X} = (x_1, \dots, x_n)$ and $\vec{Y} = (y_1, \dots, y_n)$. Decryption works when $\vec{X} \cdot \vec{Y} \neq 0$.
 $\Rightarrow O(1)$ -size ciphertexts and selective security.
- Gives revocation by defining $P[Z] = \prod_{\text{ID}_j \in S} (Z - \text{ID}_j)$ where $S = \{\text{ID}_1, \dots, \text{ID}_s\}$ is the revoked set. Then, $\vec{X} = (x_1, \dots, x_n)$ contains the coefficients of $P[Z]$ and SK_{ID} defines $\vec{Y} = (1, \text{ID}, \text{ID}^2, \dots, \text{ID}^{n-1})$.

Revocation with short ciphertexts: [AL'10]

- **Setup**(n): chooses groups $(\mathbb{G}, \mathbb{G}_T)$ of order $N = p_1 p_2 p_3$, $g \xleftarrow{R} \mathbb{G}_{p_1}$, $h_0, h_1, \dots, h_n \xleftarrow{R} \mathbb{G}_{p_1}$, $X_3 \xleftarrow{R} \mathbb{G}_{p_3}$, $\alpha \xleftarrow{R} \mathbb{Z}_N$ and sets

$$MPK = (g, \{h_i\}_{i=0}^n, e(g, g)^\alpha, X_3).$$

The master key is $MSK = g^\alpha$.

- **Encrypt**($MPK, \vec{X} = (x_1, \dots, x_n)$): picks $s \xleftarrow{R} \mathbb{Z}_N$ and sets

$$(C_0, C_1, C_2) = (M \cdot e(g, g)^{\alpha \cdot s}, g^s, (h_1^{x_1} \cdots h_n^{x_n})^s).$$

- **Extract**($MSK, \vec{Y} = (y_1, \dots, y_n)$): picks $r \xleftarrow{R} \mathbb{Z}_N$, $R_3, R'_3 \xleftarrow{R} \mathbb{G}_{p_3}$, $R_{3,1}, \dots, R_{3,n} \xleftarrow{R} \mathbb{G}_{p_3}$ and computes

$$SK_{\vec{Y}} = \left(g^\alpha \cdot h_0^r \cdot R_3, g^r \cdot R'_3, (h_0^{y_1} \cdot h_1)^r \cdot R_{3,1}, \dots, (h_0^{y_n} \cdot h_n)^r \cdot R_{3,n} \right).$$

Revocation with short ciphertexts: [AL'10]

- Private keys have the form

$$\begin{aligned} SK_{\vec{Y}} &= (D_1, D_2, K_1, \dots, K_n) \\ &= \left(g^\alpha \cdot h_0^r \cdot R_3, g^r \cdot R'_3, (h_0^{y_1} \cdot h_1)^r \cdot R_{3,1}, \dots, (h_0^{y_n} \cdot h_n)^r \cdot R_{3,n} \right). \end{aligned}$$

\Rightarrow Computing $K = \prod_{i=1}^n K_i^{x_i}$ gives

$$K = (h_0^{\vec{X} \cdot \vec{Y}} \cdot h_1^{x_1} \dots h_n^{x_n})^r.$$

To decrypt

$$(C_0, C_1, C_2) = (M \cdot e(g, g)^{\alpha \cdot s}, g^s, (h_1^{x_1} \dots h_n^{x_n})^s),$$

1. Compute $e(D_1, C_1) = e(g, g)^{\alpha s} \cdot e(g, h_0)^{rs}$
2. Compute $e(g, h_0)^{rs}$ thanks to $\gamma = \frac{e(C_1, K)}{e(C_2, D_2)} = e(g, h_0)^{rs \cdot \vec{X} \cdot \vec{Y}}$.

Conclusions

- Dual system encryption has proved quite powerful.
- Applications far beyond IBE (e.g. fully secure functional encryption, adaptively secure broadcast encryption, ...).
- Open problems remain
 - Fully secure HIBE with constant-size ciphertexts under simple assumptions using symmetric pairings
 - How about fully secure revocation with short ciphertext?
 - ... or fully secure ABE with short ciphertexts?
 - Is there a general recipe to get full security from selectively secure schemes?