

## Lecture 13

Lecturer: Victor Shoup

Scribe: Kristiyan Haralambiev

Last time, we studied the Boneh-Franklin IBE scheme which is semantically secure and, using the Fujisaki-Okamoto transformation, CCA secure; both in the random oracle model. We continue our discussion by presenting a semantically secure IBE scheme in a weaker (selective-ID) model, but without using random oracles. Also, we study the Canetti-Halevi-Katz transformation,  $(l + 1)$ -level semantically secure HIBE to  $l$ -level CCA HIBE, by applying it to the Boneh-Boyen scheme to obtain a CCA public key encryption.

## 1 Selective-ID Secure IBE Without Random Oracles

We review our notation from the last time:

### 1.1 Bilinear Pairings and Related Intractability Assumption

Let  $(\mathbb{G}_1, +)$  and  $(\mathbb{G}_2, \cdot)$  be two cyclic groups of prime order  $q$ . The bilinear pairing is given as  $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ , which satisfies the following properties:

- Bilinearity: For all  $P, Q, R \in \mathbb{G}_1$ ,  $e(P + Q, R) = e(P, R)e(Q, R)$  and  $e(P, Q + R) = e(P, Q)e(P, R)$ ;
- Non-degeneracy: There exists  $P, Q \in \mathbb{G}_1$  such that  $e(P, Q) \neq 1$ ;
- Computability: It is efficient to compute  $e(P, Q) \forall P, Q \in \mathbb{G}_1$ .

**Assumption 1 (Decisional Bilinear Diffie-Hellman Assumption)** *The DBDH assumption is defined as follows: for a given generator  $P \in \mathbb{G}_1$ , randomly chosen  $a, b, c \in_R \mathbb{Z}_q$  and  $T \in_R \mathbb{G}_2$ , any PPT algorithm  $\mathcal{A}$  has negligible advantage in distinguishing  $e(P, P)^{abc}$  from  $T$ , i.e.*

$$|Pr[\mathcal{A}(P, aP, bP, cP, e(P, P)^{abc}) = 1] - Pr[\mathcal{A}(P, aP, bP, cP, T) = 1]| \leq \epsilon, \text{ for a negligible } \epsilon$$

### 1.2 Boneh-Boyen sID Semantically Secure IBE

The original paper presents a Hierarchical IBE (HIBE) scheme which is a direct generalization of the IBE scheme presented below. In a HIBE scheme, identities are vectors, i.e.  $ID = (I_1, I_2, \dots, I_l) \in \mathbb{Z}_q^l$  represents an identity at depth  $l$ . The *KeyGen* algorithm takes as input an identity  $ID$  at depth  $l$  and the private key  $K_{ID|_{l-1}}$  of the parent identity  $ID|_{l-1} = (I_1, \dots, I_{l-1})$  at depth  $l - 1$ , and outputs the private key  $K_{ID}$  for identity  $ID$ . The *MSK* is considered to be the private key at depth 0. (Note that any IBE scheme is a HIBE for which all identities have depth 1.)

We assume identities to be elements of  $\mathbb{Z}_q$ ; if necessary, one could use a CRHF:  $\{0, 1\}^* \rightarrow \mathbb{Z}_q$ . Plaintexts and ciphertexts are elements of  $\mathbb{G}_2$ .

- KeyGen():  $\langle P \rangle = \mathbb{G}_1$ ,  $x, y \in_R \mathbb{Z}_q$ ,  $MPK = (P, xP, yP, Q)$  and  $MSK = (xyP)$
- SKEExtract( $MSK, ID = u$ ) =  $(\underbrace{xyP + r\mathcal{F}(u)}_{D_0}, \underbrace{rP}_{D_1})$ , where  $\mathcal{F}(u) = u(xP) + Q$  and  $r \in_R \mathbb{Z}_q$
- Encrypt( $ID = u, M$ ) =  $(\underbrace{zP}_{C_0 \in \mathbb{G}_1}, \underbrace{z\mathcal{F}(u)}_{C_1 \in \mathbb{G}_1}, \underbrace{e(xP, yP)^z M}_{C_2 \in \mathbb{G}_2})$ , where  $z \in_R \mathbb{Z}_q$
- Decrypt( $K_{ID} = (D_0, D_1), C = (C_0, C_1, C_2)$ ): output  $C_2 \cdot e(C_1, D_1) / e(C_0, D_0) = M$

Correctness:

$$C_2 \frac{e(C_1, D_1)}{e(C_0, D_0)} = \frac{C_2 \cdot e(z\mathcal{F}(u), rP)}{e(zP, xyP + r\mathcal{F}(u))} = \frac{C_2 \cdot e(\mathcal{F}(u), P)^{rz}}{e(P, P)^{xyz} e(\mathcal{F}(u), P)^{rz}} = \frac{C_2}{e(P, P)^{xyz}} = M$$

Security:

direct reduction to DBDH: the input is  $(P, X = xP, Y = yP, Z = zP, T)$ , where  $T$  is random or  $e(P, P)^{xyz}$

After the adversary  $\mathcal{A}$  outputs the target  $ID = u^*$ , the challenger sets  $Q = -u^*(xP) + vP$ , for randomly chosen  $v \in \mathbb{Z}_q$ . Then,  $MPK = (P, X, Y, Q)$ ,  $MSK$  is unknown, and  $\mathcal{F}(u) = u(xP) + Q = (x(u - u^*) + v)P$ .

Although the challenger doesn't know  $MSK$ , he would be able to answer secret key queries for  $ID = u \neq u^*$ :

- set  $\Delta = u - u^* \neq 0 \in \mathbb{Z}_q$  and select  $t \in_R \mathbb{Z}_q$
- $D_0 \leftarrow -\frac{v}{\Delta}(yP) + t\mathcal{F}(u)$
- $D_1 \leftarrow -\frac{1}{\Delta}(yP) + tP$

Verify:

$$\begin{aligned} D_0 &= xyP + r\mathcal{F}(u) = xyP + \left(\frac{-y}{\Delta} + t\right)\mathcal{F}(u) \\ &= xyP - \frac{y}{\Delta}\mathcal{F}(u) + t\mathcal{F}(u) \\ &= xyP - \frac{y}{\Delta}(x\Delta + v)P + t\mathcal{F}(u) \\ &= -\frac{v}{\Delta}(yP) + t\mathcal{F}(u) \\ D_1 &= \underbrace{\left(\frac{-y}{\Delta} + t\right)}_{=r} P \end{aligned}$$

Therefore, that would be a perfect simulation of extraction queries. Now, recall that in the semantic security game  $\mathcal{A}$  sends two messages  $M_0, M_1$  to the challenger who selects a random bit  $b \in \{0, 1\}$ , encrypts  $M_b$ , and sends back  $Encrypt(u^*, M_b)$  to  $\mathcal{A}$ . The simulator will encrypt  $M_b$  as  $(Z = zP, vZ, TM_b)$ . If  $T$  is random,  $TM_b$  is "perfectly hidden". Whereas if  $T = e(P, P)^{xyz}$ ,  $c_1 = z\mathcal{F}(u^*) = z(x \cdot 0 + v)P = zvP = vZ$  is correct, and so the simulator computes an encryption as a real challenger would.

$\Rightarrow$  If  $\mathcal{A}$  has a non-negligible advantage of breaking the semantic security of the scheme, one could construct an algorithm breaking the DBDH assumption.

## 2 The Canetti-Halevi-Katz Transformation

We briefly discuss the idea behind the transformation for  $l = 0$ , i.e. from semantically secure selective-ID IBE to chosen-ciphertext secure encryption, and refer to the corresponding paper about the general case (from  $(l + 1)$ -level semantically secure HIBE to  $l$ -level CCA HIBE).

Given a semantically secure selective-ID IBE scheme  $(KeyGen_{IBE}, SKExtract, E, D)$  and a one-time signature scheme with strong unforgeability  $(KeyGen_{Sgn}, S, V)$ , we construct  $(KeyGen', E', D')$  as follows:

- $KeyGen'$ : run  $KeyGen_{IBE}$  and set  $(PK, SK) \leftarrow (MPK, MSK)$
- $E'(PK, M)$ :  $(spk, ssk) \leftarrow KeyGen_{Sgn}()$   
 $c_0 = spk$   
 $c_1 = E(MPK, ID = spk, M)$   
 $c_2 = S(ssk, c_1)$   
output  $C = (c_0, c_1, c_2)$
- $D'(SK, C)$ :
  - verify signature
  - extract  $K_{ID}$  for  $ID = spk$
  - decrypt

Pf of security idea:  $c_0$  is acting as  $u^*$  (the target ID)

Clearly, the adversary should make use of the decryption queries in order to break the security. If the challenge ciphertext is  $(c_0, c_1, c_2)$  and adversary submits a "relevant" but different ciphertext  $(\tilde{c}_0, \tilde{c}_1, \tilde{c}_2)$ , either  $\tilde{c}_0 = c_0$  or  $\tilde{c}_0 \neq c_0$ . In the former case,  $(\tilde{c}_1, \tilde{c}_2) \neq (c_1, c_2)$ , so the signature verification must fail (if not, break the signature scheme). In the latter case, if  $\mathcal{A}$  has non-negligible advantage in breaking the scheme, then there is another  $\mathcal{A}'$  breaking the IBE scheme with same advantage.