Full Title of the Talk

John Smith

University of California

john@smith.com

January 1, 2020

Overview

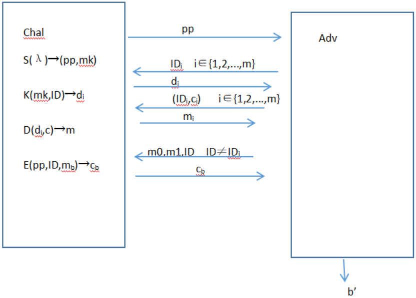
1. First Section
    - Subsection Example
    - Revocation of Public Keys

Applications for Identity-Based Encryption

1. Revocation of Public Keys
   Public key certificates are valid, an IBE system key expiration can be done by having Alice encrypt e-mail sent to Bob using the public key: “bob@company.com k current-year”.This approach makes key revocation very simple.In addition, it can be used to manage user credentials.
2. Delegation of Decryption Keys
   Delegation to a laptop: Suppose Alice wants Bob to send the message and uses the current date as the encryption key.When using IBE system, Bob can install several private keys corresponding to the leaving days of travel on his laptop.If the notebook is stolen the master key is not compromised.
   Delegation of duties:IBE can simplify the management of a large number of public key security system by using the master key to generate private keys corresponding to different functions.

CCA Security

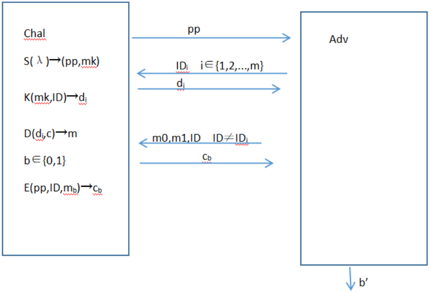
definition 2.1. We say that the IBE system E is semantically secure against an adaptive chosen ciphertext attack if for any polynomial time IND-ID-CCA adversary A the function AdvE,A(k) is negligible.As shorthand, we say that E is IND-ID-CCA secure.



$$\text{Adv}\,\varepsilon,\mathcal{A}(k) = \left|\Pr\left[b = b'\right] - \frac{1}{2}\right|$$

CPA Security

Definition 2.2. We say that the IBE system E is semantically secure if for any polynomial time IND-ID-CPA adversary A the function AdvE,A(k) is negligible. As shorthand, we say that E is IND-ID-CPA secure.



Chal

$S(\lambda)\rightarrow(pp,mk)$

$K(mk,ID)\rightarrow d_i$

$D(d_i,c)\rightarrow m$

$b\in\{0,1\}$

$E(pp,ID,m_b)\rightarrow c_b$

pp

$ID_i \quad i\in\{1,2,\dots,m\}$

d_i

$m0,m1,ID \quad ID\neq ID_i$

c_b

Adv

b'

$$\mathrm{Adv}\,\varepsilon,\mathcal{A}(k)=\left|\Pr\left[b=b'\right]-\tfrac{1}{2}\right|$$

Bilinear maps and the Bilinear Diffie-Hellman Assumption

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two groups of order q for some large prime q. Our IBE system makes use of a bilinear map$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ between these two groups. The map must satisfy the following properties:

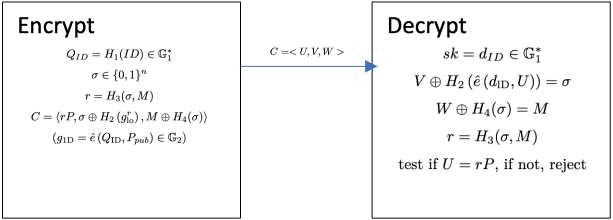
1. Bilinear
2. Non-degenerate
3. Computable

Decision Diffie-Hellman is Easy: The Decision Diffie-Hellman problem (DDH) in $\mathbb{G}_1$ is to distinguish between the distributions $\langle P, aP, bP, abP \rangle$ and $\langle P, aP, bP, cP \rangle$ where a, b, c are random in $\mathbb{Z}_q^*$ and P is random in $\mathbb{G}_1^*$. Joux and Nguyen point out that DDH in $\mathbb{G}_1$ is easy. To see this, observe that given P, aP, bP, cP $\in \mathbb{G}_1^*$ we have

$$c = ab \bmod q \quad \Longleftrightarrow \quad \hat{e}(P, cP) = \hat{e}(aP, bP)$$

CCA secure IBE

Figure: FullIdent Schema



Encrypt

$$Q_{ID} = H_1(ID) \in \mathbb{G}_1^*$$

$$\sigma \in \{0,1\}^n$$

$$r = H_3(\sigma, M)$$

$$C = \langle rP, \sigma \oplus H_2\left(g_{\mathrm{lo}}^r\right), M \oplus H_4(\sigma)\rangle$$

$$\left(g_{\mathrm{1D}} = \hat{e}\left(Q_{\mathrm{ID}}, P_{pub}\right) \in \mathbb{G}_2\right)$$

$C =< U, V, W >$

Decrypt

$$sk = d_{ID} \in \mathbb{G}_1^*$$

$$V \oplus H_2\left(\hat{e}\left(d_{\mathrm{lD}}, U\right)\right) = \sigma$$

$$W \oplus H_4(\sigma) = M$$

$$r = H_3(\sigma, M)$$

test if $U = rP$, if not, reject

FullIdent is a chosen cipher text secure IBE (IND-ID-CCA), under the assumption of hard BDH. [1, 3]

$$Adv_{\mathcal{G},\mathcal{B}}(k) \geq 2FO_{adv}\left(\frac{\epsilon(k)}{e\left(1 + q_E + q_D\right)}, q_{H_4}, q_{H_3}, q_D\right) / q_{H_2}$$

Relaxing the hashing requirements

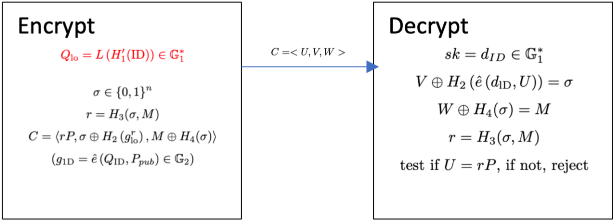


Figure: Modified FullIdent

Encrypt

$Q_{\mathrm{lo}} = L\left(H_1'(\mathrm{ID})\right) \in \mathbb{G}_1^*$

$\sigma \in \{0,1\}^n$

$r = H_3(\sigma, M)$

$C = \langle rP, \sigma \oplus H_2\left(g_{\mathrm{lo}}^r\right), M \oplus H_4(\sigma)\rangle$

$\left(g_{\mathrm{1D}} = \hat{e}\left(Q_{\mathrm{ID}}, P_{pub}\right) \in \mathbb{G}_2\right)$

$C =< U,V,W >$

Decrypt

$sk = d_{ID} \in \mathbb{G}_1^*$

$V \oplus H_2\left(\hat{e}\left(d_{\mathrm{ID}}, U\right)\right) = \sigma$

$W \oplus H_4(\sigma) = M$

$r = H_3(\sigma, M)$

test if $U = rP$, if not, reject

Using a deterministic encoding function to map $\mathcal{A}$ onto $\mathbb{G}_1^*$. This modified FullIdent is IND-ID-CCA secure. [5]

References

John Smith (2012)
Title of the publication
Journal Name 12(3), 45 – 678.

Paulo SLM Barreto, Hae Y Kim, Ben Lynn, and Michael Scott.
Efficient algorithms for pairing-based cryptosystems.
In *Annual international cryptology conference*, pages 354–369. Springer, 2002.

Mihir Bellare and Phillip Rogaway.
Random oracles are practical: A paradigm for designing efficient protocols.
In *Proceedings of the 1st ACM conference on Computer and communications security*, pages 62–73. ACM, 1993.

Dan Boneh.
The decision diffie-hellman problem.
In *International Algorithmic Number Theory Symposium*, pages 48–63. Springer, 1998.

Dan Boneh and Matt Franklin.
Identity-based encryption from the weil pairing.
In *Annual international cryptology conference*, pages 213–229. Springer, 2001.

The End