Efficient Identity-based Encryption Without Random Oracles

Brent Waters

Weiwei Liu

School of Computer Science and Software Engineering

UNIVERSITY OF WOLLONGONG

Contents

UNIVERSITY OF WOLLONGONG

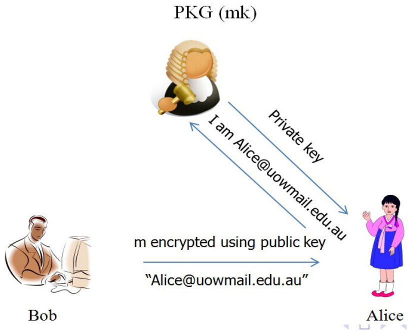
Outline

UNIVERSITY OF WOLLONGONG

Introduction

Identity-based Encryption:

- **Definition**: Essentially public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g., a user's email address, current date, physical IP address).



UNIVERSITY OF WOLLONGONG

Introduction

An identity-based encryption scheme **IBE** consists of four polynomial-time algorithms (**Setup**, **Extract**, **Encrypt**, **Decrypt**):

- **Setup**: Takes as input a security parameter 1^κ and returns the system parameters *params* and a master-key *mk*.
- **Extract**: Takes as input an arbitrary identity $ID \in \{0,1\}^*$ and master key *mk* and returns a private key $d_{ID} \leftarrow \textbf{Extract}(ID, mk, params)$.
- **Encryption**: Takes as input an *ID* and a message $m \in \mathcal{M}$, and returns a ciphertext $C \leftarrow \textbf{Enc}(ID, m, params)$.
- **Decryption**: Takes as input a private key d_{ID} and a cihpertext $C \in \mathcal{C}$, and returns $m \leftarrow \textbf{Dec}(d_{ID}, C)$.

UNIVERSITY OF WOLLONGONG

Introduction

Brief History of IBE:

- Shamir84' Identity-Based Cryptosystems and Signature Schemes.
- BB'04 Eurocrypt: Efficient Selective-ID Identity Based Encryption without Random Oracles.
- BB'04 Crypto: Secure Identity Based Encryption without Random Oracles.
- Waters'05 Eurocrypt: Efficient IBE system in full model without Random Oracles Mathematically similar to BB'04 (Crypto).
- Gentry'06 Eurocrpt: Practical Identity-Based Encryption without Random Oracles.

UNIVERSITY OF WOLLONGONG

Outline

1. Introduction
2. Security Model
3. Waters' Scheme
4. Security Proof

Security Model

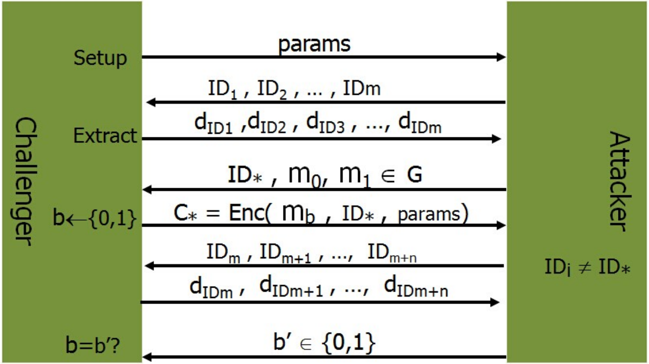


Figure : IBE Semantic Security

Security Model

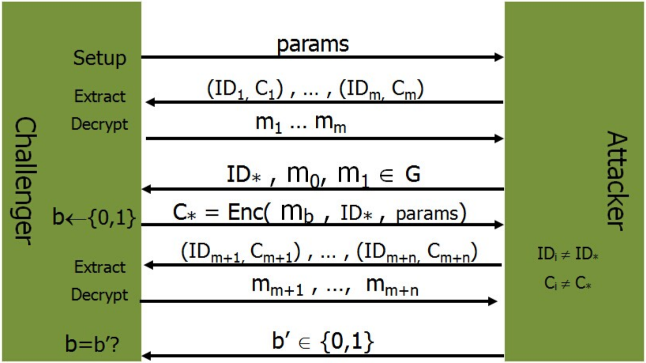


Figure : IBE CCA Security

Security Model

Definition

An IBE system is (t, q_{ID}, ϵ)-semantically secure if all t-time adversaries making at most q_{ID} private key queries have at most an ϵ in breaking the scheme.

Definition

An IBE system is $(t, q_{ID}, q_C, \epsilon)$-CCA secure if all t-time CCA adversaries making at most q_{ID} private key queries and q_C chosen ciphertext queries have at most an ϵ in breaking the scheme.

Security Model

Let $\mathbb{G}, \mathbb{G}_1$ be finite cyclic groups of prime order p and g be a generator of $\mathbb{G}$. We say $\mathbb{G}$ has admissible bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$ that satisfies:

1. **Bilinearity**: $e(g^a, g^b) = e(g, g)^{ab}$, $a, b \in_R \mathbb{Z}_p$ and $g \in \mathbb{G}$.
2. **Non-degenerate**: $e(g, g) \neq 1_{\mathbb{G}_1}$.
3. **Computability**: $e(g, g)$ is efficiently computable.

UNIVERSITY OF WOLLONGONG

Definition

Decisional Bilinear Diffie-Hellman (BDH) Assumption: Given two tuples $(g, A = g^a, B = g^b, C = g^c, Z = e(g,g)^{abc})$ and $(g, A = g^a, B = g^b, C = g^c, Z = e(g,g)^z)$ for some randomly $a, b, c, z \in \mathbb{Z}_p$, An adversary $\mathcal{B}$ has at least an ϵ advantage in solving the decisional BDH problem if
$|\Pr[\mathcal{B}(g, g^a, g^b, g^c, e(g,g)^{abc} = 1] - \Pr[\mathcal{B}(g, g^a, g^b, g^c, e(g,g)^z) = 1]| \geq \epsilon.$

Definition

Computational Diffie-Hellman (BDH) Assumption: Given $g, g^a, g^b \in \mathbb{G}$ for some random $a, b \in \mathbb{Z}_p$, An adversary $\mathcal{B}$ has at least an ϵ advantage in solving the decisional CDH problem if $|\Pr[\mathcal{B}(g, g^a, g^b) = g^{ab}] \geq \epsilon.$

Outline

Waters' Scheme

Let $\mathbb{G}$ be a group of prime order p. Let $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$ denote the bilinear map and g be the generator of $\mathbb{G}$.

- **Setup(1^κ)**: $params = (g, g_1, g_2, u', \vec{U})$, $mk = g_2^\alpha$.
- **KeyGen($v, mk, params$)**:
  $d_v = (d_1, d_2) = (g_2^\alpha (u' \prod_{i \in \mathcal{V}} u_i)^r, g^r)$.
- **Encryption($M, v, params$)**:
  $C = (C_1, C_2, C_3) = (e(g_1, g_2)^t M, g^t, (u' \prod_{i \in \mathcal{V}} u_i)^t))$
- **Decryption(C, d_v)**:
  $C_1 \frac{e(d_2, C_3)}{d_1, C_2} = (e(g_1, g_2)^t M) \frac{e(g^r, (u' \prod_{i \in \mathcal{V}} u_i)^t)}{e(g_2^\alpha (u' \prod_{i \in \mathcal{V}} u_i)^r, g^t)} = M$

BB' Scheme

Let $\mathbb{G}$ be a group of prime order p. Let $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$ denote the bilinear map and g be the generator of $\mathbb{G}$.

- **Setup(1^κ)**: $params = (g, g_1, g_2, h)$, $mk = g_2^\alpha$.
- **KeyGen($v, mk, params$)**: $d_v = (d_1, d_2) = (g_2^\alpha (g_1^v h)^r, g^r)$.
- **Encryption($M, v, params$)**:
  $C = (C_1, C_2, C_3) = (e(g_1, g_2)^t M, g^t, (g_1^v h)^t))$
- **Decryption(C, d_v)**:
  $C_1 \frac{e(d_2, C_3)}{e(d_1, C_2)} = (e(g_1, g_2)^t M) \frac{e(g^r, (g_1^v h)^t)}{e(g_2^\alpha (g_1^v h)^r, g^t)} = M$

Outline

Security Proof

Proof. Suppose there exists a (t, q, ϵ)-adversary $\mathcal{A}$ against the scheme. We construct a simulator $\mathcal{B}$ to play the decisional BDH game. The simulator will take BDH challenge $(g, A = g^a, B = g^b, C = g^c, Z)$ and outputs a guess β', as to whether the challenge is a BDH tuple. The simulator runs $\mathcal{A}$ executing the following steps.

Security Proof

Proof.

Setup: The simulator sets:

- $m = 4q, k \in (0, n)$,
- x' and $\vec{x} = (x_i)$ where $|\vec{x}| = n$ and $x', x_i \in (0, m-1)$.
- y' and $\vec{y} = (y_i)$ where $|\vec{y}| = n$ and $y', y_i \in_R \mathbb{Z}_p$.
- Let X^* denote the pair $(x', \vec{x})$.

Define three functions:

- $F(v) = (p - mk) + x' + \sum_{i \in \mathcal{V}} x_i$;
- $J(v) = y' + \sum_{i \in \mathcal{V}} y_i$;
- $$K(v) = \begin{cases} 0, & \text{if } x' + \sum_{i \in \mathcal{V}} x_i \equiv 0 \pmod{m} \\ 1, & \text{otherwise} \end{cases}$$

UNIVERSITY OF WOLLONGONG

Security Proof

Proof.

- $g_1 = A$, $g_2 = B$, $u' = g_2^{p-km+x'}$ and $u_i = g_2^{x_i} g^{y_i}$

Phase 1: Suppose the adversary issues a query for an identity v.

1. If $K(v) = 0$, the simulator aborts and randomly chooses its guess β' of the challenger's value β.
2. Otherwise, the simulator choose $r \in_R \mathbb{Z}_p$ and construct the key $d = (d_0, d_1)$.
   - $d_0 = g_1^{\frac{-J(v)}{F(v)}} (u' \prod_{i \in \mathcal{V}} u_i)^r$;
   - $d_1 = g_1^{\frac{-1}{F(v)}} g^r$;

Security Proof

Proof.

Let $\bar{r} = r - \frac{a}{F(v)}$, then

$$\begin{aligned} d_0 &= g_1^{\frac{-J(v)}{F(v)}} (u' \prod_{i \in \mathcal{V}} u_i)^r \\ &= g_1^{\frac{-J(v)}{F(v)}} (g_2^{F(v)} g^{J(v)})^r \\ &= g_2^a (g_2^{F(v)} g^{J(v)})^{-\frac{a}{F(v)}} (g_2^{F(v)} g^{J(v)})^r \\ &= g_2^a (u' \prod_{i \in \mathcal{V}} u_i)^{r - \frac{a}{F(v)}} \\ &= g_2^a (u' \prod_{i \in \mathcal{V}} u_i)^{\bar{r}} \end{aligned}$$

Security Proof

Proof.

$$\begin{aligned} d_1 &= g_1^{\frac{-1}{F(v)}} g^r \\ &= g^{r - \frac{a}{F(v)}} \\ &= g^{\bar{r}} \end{aligned}$$

The simulator will be able to perform this computation iff $F(v) \neq 0 \pmod{p}$. For ease of analysis the simulator will only continue (not abort) in the sufficient condition where $K(v) \neq 0$.

Security Proof

Proof. **Challenge**: The adversary submits two messages $M_0, M_1 \in \mathbb{G}_1$ and an identity v^*.

1. If $x' + \sum_{i \in \mathcal{V}^*} x_i \neq km$, the simulator aborts and submits a random guess for β'.
2. Otherwise, $F(v^*) \equiv 0 \pmod{p}$ and the simulator will flip a coin and construct the ciphertext $T = (ZM_\gamma, C, C^{J(v^*)})$.

Suppose that the simulator was given a BDH tuple, that is $Z = e(g,g)^{abc}$. Then we have

$$T = (e(g,g)^{abc} M_\gamma, g^c, g^{cJ(v^*)}) = (e(g_1, g_2)^c M_\gamma, g^c, (u' \prod_{i \in \mathcal{V}^*} u_i)^c)$$

Security Proof

Proof. We see that T is a valid encryption of M_γ. Otherwise, Z is a random element of $\mathbb{G}_1$. In that case the ciphertext will give no information about the simulator's choice of γ.

Phase 2: Same as in **Phase 1**.

Guess: The adversary $\mathcal{A}$ outputs a guess γ' of γ.

Artificial Abort: An adversary's probability of success could be correlated with the probability that the simulator needs to abort. Since two different sets of q private key queries may the cause the simulator to abort with different probabilities.

Security Proof

Proof. In the worst case, $\Pr[\gamma = \gamma' | \bar{abort}] - \frac{1}{2} = 0$ in the simulation even if $\Pr[\gamma = \gamma'] - \frac{1}{2} = \epsilon$ for some non-negligible ϵ. Let $\vec{v} = v_1, \ldots, v_q$ denote the private key queries made in phase 1 and phase 2 and let v^* denote the challenge identity. Define the function $\tau(X', \vec{v}, v*)$, where X' is a set of simulation values $x', x_1, \ldots, x_n$ as

$$\tau(X', \vec{v}, v*) = \begin{cases} 0, & \text{if } (\wedge_{i=1}^{q} K(v_i) = 1) \wedge (x' + \sum_{i \in \mathcal{V}^*} x_i) = km \\ 1, & \text{otherwise} \end{cases}$$

The function $\tau(X', \vec{v}, v*)$ will evaluate to 0 if the private key and challenge queries $\vec{v}, v^*$ will not cause an abort for a given choice of simulation values X'.

UNIVERSITY OF WOLLONGONG

Security Proof

Proof. Set $\eta = \Pr_{X'}[\tau(X', \vec{v}, v*) = 0]$. The simulator samples $O(\epsilon^{-2} ln(\epsilon^{-1})\lambda^{-1} ln(\lambda^{-1}))$ times the probability η by choosing a random X' and evaluating $\tau(X', \vec{v}, v*)$ to compute an estimate η'. We emphasize that the sampling does not involve running the adversary again. Let $\lambda = \frac{1}{8nq}$ be the lower bound on the probability of not aborting on any set of adversaries. Then if $\eta' \geq \lambda$ the simulator will abort with probability $\frac{\eta' - \lambda}{\eta'}$ and take a random guess. Otherwise, the simulator will not abort.
If the simulator has not aborted at this point it will take check to see if the adversary's guess $\gamma' = \gamma$. If $\gamma' = \gamma$, the simulator outputs a guess $\beta' = 1$; Otherwise, outputs $\beta = 0$.
This concludes the description of the simulator.

Security Proof

Proof. The first simulator is difficult to analyze directly since it might abort before all of the queries are made. The author present a second simulation to better describe the output distribution of the first simulation.

Setup: Set $mk = g_2^{\alpha}$, choose $X^*, \vec{y}$ as in the first simulation and derives u', U in the same way.

Phase 1: Use mk to respond to private key queries, in this way all queries can be answered.

Challenge: Upon receiving the challenge M_0, M_1, the simulator flips two coins β and γ. If $\beta = 0$, it encrypts a random message and if $\beta = 1$ it encrypts M_{γ}.

Security Proof

Proof.

Phase 2: Same as phase 1.

Guess: The simulator receives a guess γ' from the adversary. At this point the simulator has seen as the private key queries and the challenge query $(\vec{v}, v^*)$. It evaluates the function $\tau(X', \vec{v}, v*)$ and aborts if it evaluates to 1, outputting a random guess of β'.

Artificial Abort: The last step is same as the first simulation.

This ends the description.

Security Proof

Proof. The probabilities of the two simulators can be proved to be equal with the following claims.

Claim 1: The probabilities $\Pr[\beta' = \beta]$ are the same in both the first simulation and second simulation.

Claim 2: The probabilities of the simulation not aborting by the guess phase is at least $\lambda = \frac{1}{8(n+1)q}$.

Claim 3: If $\mathcal{A}$ has an probability ϵ in breaking the scheme, then $\mathcal{B}$ has at least a probability $\frac{\epsilon}{32(n+1)q}$ in breaking the BDH assumption.

A Signature Scheme

Setup: $pk = (g, g_1, g_2, u', U)$, $sk = g_2^{\alpha}$.
Signing: $\sigma_M = (\sigma_1, \sigma_2) = (g_2^{\alpha}(u' \prod_{i \in \mathcal{M}})^{r+\Delta}, g^{r+\Delta})$.
Verification: $e(\sigma_1, g) \stackrel{?}{=} e(g_1, g_2)e(\sigma_2, u' \prod_{i \in \mathcal{M}} u_i)$

Theorem

The signature scheme is (t, q, ϵ) existentially unforgeable assuming the decisional computational Diffie-Helman assumption holds.

Conclusion

1. The first efficient and practical Identity-based encryption that is secure in the full model without random oracles.
2. An efficient signature scheme.

Two interesting open problems remains to be solved:

1. How to construct an efficient IBE system that has short public parameters without random oracles.
2. How to construct an IBE system with a tight reduction in security.

References

Brent Waters.
Efficient identity-based encryption without random oracles.
In *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, pages 114–127, 2005.

UNIVERSITY OF WOLLONGONG

Thanks

Thank you