A New Identity Based Encryption Scheme From Pairing

Xianhui Lu, Dake He, Guomin Li
Southwest Jiaotong University
Email: lu_xianhui@sohu.com

December 28, 2006

Abstract

We construct an efficient identity based encryption scheme from pairing. The basic version of the new scheme is provably secure against chosen plaintext attack, and the full version of the new scheme is provably secure against adaptive chosen ciphertext attack. Our scheme is based on a new assumption (decision weak bilinear Diffie-Hellman assumption) which is no stronger than decision bilinear Diffie-Hellman assumption.

Keywords: IBE, IND-ID-CPA, IND-ID-CCA, standard model

1 Introduction

Identity Based Encryption (IBE) provides a public key encryption mechanism where a public key is an arbitrary string such as an email address or a telephone number. It is first proposed by Shamir in 1984 [1]. After that, it remained an open problem for almost two decades. In 2001, Boneh and Franklin [2] proposed formal security notions for IBE systems and designed a fully functional secure IBE scheme using bilinear maps. Cocks describes another construction using quadratic [3]. Both Boneh-Franklin and Cocks IBE schemes are provably secure against chosen ciphertext attack in random oracle model [4]. A proof in the random oracle model can only serve as a heuristic argument and has proved to possibly lead to insecure schemes when the random oracles are implemented in the standard model [5]. In [8] Boneh and Boyen proposed an efficient IBE scheme that is selective identity secure without random oracle model. Selective identity secure IBE is

a slightly weaker security model than the standard security model for IBE [6, 7]. After that Waters presents the first efficient IBE scheme that is chosen plaintext secure without random oracles. Hierarchical IBE(HIBE) is a generalization of IBE allowing for hierarchical delegation of decryption keys [11, 12]. The results from Canetti, Halevi, and Katz [7] , further improved upon by Boneh and Katz [10] show a generic and practical transformation from any chosen plaintext secure 2-level HIBE scheme to a chosen ciphertext secure IBE scheme. Since Water's IBE scheme can naturally be extended to a 2-level HIBE this implies the first efficient chosen ciphertext secure IBE in the standard model. The first direct chosen ciphertext IBE construction in the standard model was mentioned by Boyen, Mei, and Waters [10] and later improved by Galindo and Kiltz [15]. Both constructions are based on Waters' IBE and add one additional element to the ciphertext that is used for a consistency check in the decryption algorithm. Instead of providing the fully functionality of an IBE scheme, in many applications it is sufficient to just providing an identity-based encapsulation mechanism(IB-KEM). An IB-KEM can be updated to a full IBE scheme by adding a symmetric encryption scheme called data encapsulation scheme(DEM). The resulting IBE schemes are very efficient [18, 19]. In [19] Boyen classifies most of the known IBE schemes into four types as table1.

1.1 Our Contributions

We construct a IBE scheme based an assumption which is no stronger than DBDH(we call it weak decision bilinear Diffie-Hellman assumption). Our new scheme is provably secure in standard model and very efficient.The basic version of our scheme is secure against IND-ID-CPA , and the full version(a hybrid version) of our scheme is secure against IND-ID-CCA.

2 Preliminaries

We will review the definition of IBE system, decision bilinear Diffie-Hellman assumption. This is followed by the definition of One-time symmetric-key encryption and One-time message authentication code.

In describing probabilistic processes, we write $x \stackrel{R}{\leftarrow} X$ to denote the action of assigning to the variable x a value sampled according to the distribution X. If S is a finite set, we simply write $s \stackrel{R}{\leftarrow} S$ to denote assignment to s of an element sampled from uniform distribution on S. If A is a probabilistic algorithm and x an input, then $A(x)$ denotes the output distribution

Table 1: classification of IBE schemes

Type	Character	Schemes
Quadratic Residuosity	Relies on the hardness of the quadratic residuosity problem ,Requires $\log N$ bites of ciphertext per bit of plaintext, it is not known to be provably secure against adaptive identity attacks	Coc01[3]
Full Domain Hash	Relies on BDH assumption, Very efficient, Needs uniformly distributed hash functions with images in the pairing group restricts our choice of curves	BF01[2]
Exponent Inversion	Relies on q-BDHI assumption which is a very strong assumption,	SK03[20] BB2-04[8] Gen06[13]
Commutative Blinding	Relies on weak assumption , allowing identities to be encoded as integers rather than hashed on the curve, very flex to extend to threshold-IBE, Hierarchical-IBE and Forward-Security-IBE	BB1-04[8] Wat05[9] SW05[21] CS05[23] Nac05[22] BW06[24]

of A on in put x. Thus, we write $y \stackrel{R}{\leftarrow} A(x)$ to denote of running algorithm A on input x and assigning the output to the variable y.

We write

$$Pr[x_1 \stackrel{R}{\leftarrow} X_1, x_2 \stackrel{R}{\leftarrow} X_2, \ldots, x_n \stackrel{R}{\leftarrow} X_n : \phi(x_1, \ldots, x_n)]$$

to denote the probability that when x_1 is drawn from a certain distribution X_1, and x_2 is drawn from a certain distribution $X_2(x_1)$, possibly depending on the particular choice of x_1, and so on, all the way to x_n, the predicate $\phi(x_1, ..., x_n)$ is true. We allow the predicate ϕ to involve the execution of probabilistic algorithms.

2.1 Identity Based Encryption Scheme

An identity based encryption scheme IBE is specified by four randomized algorithms: **Setup, Extract, Encrypt, Decrypt**:

- **Setup**: takes a security parameter k and returns *params*(system parameters) and *master-key*. The system parameters include a description of a finite message space $\mathcal{M}$, and a description of a finite ciphertext space $\mathcal{C}$.

- **Extract**:takes as input $params$, $master\text{-}key$, and an arbitrary $ID \in \{0,1\}^*$, and returns a private key d. ID is an arbitrary string that will be used as a public key, and d is the corresponding private decryption key.

- **Encrypt**:takes as input $params$,ID, and $m \in \mathcal{M}$. It returns a cipher-text $C \in \mathcal{C}$

- **Decrypt**: takes as input $params$,$C \in \mathcal{C}$, and a private key d. It return $m \in \mathcal{M}$

We require that for all $params$, all $m \in \{0,1\}^*$ we have:

$$Decrypt(params, Encrypt(params, ID, m), d) = m$$

where $d = Extract(params, ID)$.

We recall the standard definition of security for identity based encryption schemes against adaptive chosen cipher-text attacks.

An identity based encryption scheme $\mathcal{E}$ is secure against an adaptive chosen ciphertext attack (IND-ID-CCA) if no polynomially bounded adversary A has a non-negligible advantage against the Challenger in the following IND-ID-CCA game:

1. **Setup:** The challenger takes a security parameter k and runs the **Setup** algorithm. It gives the adversary the resulting system parameters $params$. It keeps the $master\text{-}key$ to itself.

2. **Phase1**: The adversary issues queries $q_1, \cdots, q_m$ where query q_i is one of:

   - Extraction query $< ID_i >$. The challenger responds by running algorithm **Extract** to generate the private key d_i corresponding to the public key $< ID_i >$. It sends d_i to the adversary.
   - Decryption query $< ID_i, C_i >$. The challenger responds by running algorithm $Extract$ to generate the private key d_i corresponding to ID_i. It then runs algorithm **Decrypt** to decrypt the ciphertext C_i using the private key d_i. It sends the resulting plaintext to the adversary.

   These queries may be asked adaptively, that is, each query q_i may depend on the replies to $q_1, \cdots, q_{i-1}$.

3. **Challenge**: Once the adversary decides that Phase 1 is over it outputs two equal length plaintext $m_0, m_1 \in \mathcal{M}$ and an identity ID on which it wishes to be challenged. The only constraint is that ID did not appear in any private key extraction query in Phase 1. The challenger picks a random bit $b \in \{0,1\}$ and calculates $C = Encrypt(params, ID, m_b)$. It then sends C as the challenge to the adversary.

4. **Phase2**: The adversary issues more queries $q_{m+1}, \cdots, q_n$ where q_i is one of:

   - Extraction query $< ID_i >$ where $ID_i \neq ID$. Challenger responds as in Phase 1.
   - Decryption query $< ID_i, C_i > \neq < ID, C >$. Challenger responds as in Phase 1.

   These queries may be asked adaptively as in Phase 1.

5. **Guess**:Finally, A outputs a guess $b' \in \{0,1\}$. and wins the game if $b = b'$

The above adversary A is called an IND-ID-CCA adversary. The advantage of A in attacking $\mathcal{E}$ is define as:

$$AdvCCA_{\mathcal{E},A}(k) = |Pr[b = b'] - 1/2|$$

Definition 1 *We say that the IBE system $\mathcal{E}$ is secure against adaptive chosen ciphertext attack if for any polynomial time IND-ID-CCA adversary A the function $AdvCCA_{\mathcal{E},A}(k)$ is negligible. As shorted, we say that $\mathcal{E}$ is IND-ID-CCA secure.*

Removing the "Decrypt" queries in the IND-ID-CCA attack game above we get the IND-ID-CPA attack game. The adversary A in the IND-ID-CPA attack game is called an IND-ID-CPA adversary. The advantage of A in attacking $\mathcal{E}$ is define as follow:

$$AdvCPA_{\mathcal{E},A}(k) = |Pr[b = b'] - 1/2|$$

Definition 2 *We say that the IBE system $\mathcal{E}$ is secure against chosen plaintext attack if for any polynomial time IND-ID-CPA adversary A the function $AdvCPA_{\mathcal{E},A}(k)$ is negligible. As shorted, we say that $\mathcal{E}$ is IND-ID-CPA secure.*

2.2 The Decision Bilinear Diffie-Hellman Assumption

Let G be a bilinear group of prime order p. Let $e : G \times G \rightarrow G_T$ be the bilinear map.The bilinear Diffie-Hellman problem in G is as follow:

Given $g, g_a, g_b, g_c \in G$ as input, output $e(g,g)^{abc} \in G_T$, where a, b, c are random elements in Z_p, g is random elment in G. We say an algorithm A has advantage ϵ in solving the bilinear Diffie-Hellman problem in G if

$$|Pr[A(g, g^a, g^b, g^c) = e(g,g)^{abc}]| \geq \epsilon$$

The decisional bilinear Diffie-Hellman problem in G is as follow:

Given $g, g_a, g_b, g_c \in G$ and $T \in G_T$, where a, b, c are random elements in Z_p, g is random elment in G, T is random element in G_T. We say an algorithm A that outputs $b \in \{0,1\}$ has advantage ϵ in solving the decision bilinear Diffie-Hellman problem in G if

$$|Pr[A(g, g^a, g^b, g^c, e(g,g)^{abc}) = 0] - Pr[A(g, g^a, g^b, g^c, T) = 0]| \geq \epsilon$$

We refer to the distribution on the left as P_{BDH} and the distribution on the right as R_{BDH}.

2.3 One-time symmetric-key encryption

A one-time symmetric-key encryption scheme SKE consists of two algorithms:

- SKE.Encrypt(K, m): The deterministic, polynomial-time encryption algorithm takes as input a key K, and a message m, and outputs a cipher-text χ. We write $\chi \leftarrow SKE.Encrypt(K, m)$
- SKE.Decrypt(K, χ): The deterministic, polynomial-time decryption algorithm takes as input a key K, and a cipher-text χ, and outputs a message m or the special symbol $reject$. We write $m \leftarrow SKE.Decrypt(K, \chi)$

We require that for all $k \in Z$, for all $K \in \{0,1\}^{l(k)}$(where l(k) is the length of K), and for all $m \in \{0,1\}^*$,we have $SKE.Decrypt(K, SKE.Encrypt(K, m)) = m$.

We recall the standard definition of security for data encapsulation mechanisms against adaptive chosen cipher-text attacks and passive attacks.

Definition 3 *A SKE scheme is secure against adaptive chosen cipher-text attacks if the advantage of any PPT adversary A in the following game is negligible in the security parameter k:*

1. The challenger randomly generates an appropriately sized key K.
2. The adversary may make polynomial queries to a decryption oracle with cipher-text χ. The decryption oracle responds with SKE.Decrypt(K, χ).
3. At some point, A outputs two messages m_0, m_1 with $|m_0| = |m_1|$. A bit b is randomly chosen and the adversary is given a "challenge cipher-text" $\chi^* \leftarrow SKE.Encrypt(K, m)$.
4. A may continue to query its decryption oracle except that it may not request the decryption of χ^*. The decryption oracle responds with SKE.Decrypt(K, χ).
5. Finally, A outputs a guess b' .

We define $AdvCCA_{SKE,A}(k)$ to be $|Pr[b = b'] - 1/2|$ in the above attack game. We say that SKE is secure against adaptive chosen cipher-text attack if for all probabilistic polynomial-time oracle query machines A, the function $AdvCCA_{SKE,A}(k)$ grows negligibly in k.

We call the game above the IND-CCA game of SKE. If the adversary can only access the encryption oracle, then we get the IND-PA game of SKE.

Definition 4 *A SKE scheme is secure against passive attacks if the advantage of any PPT adversary A in the IND-PA game is negligible in the security parameter k:*

We define $AdvPA_{SKE,A}(k)$ to be $|Pr[b = b'] - 1/2|$ in the IND-PA game. We say that SKE is secure against passive attack if for all probabilistic, polynomial-time oracle query machines A, the function $AdvPA_{SKE,A}(k)$ grows negligibly in k.

2.4 One-time message authentication code

A one-time message authentication code scheme consists two algorithms:

- Parameter generation: The parameter generate algorithm takes as input 1^k, and outputs the key space K_V and the verification message space M_V. We write $(K_V, M_V) \leftarrow MAC.Gen(1^k)$

- Message authentication: The message authentication algorithm takes as input a key K, and a message α, and outputs a tag τ. We write $\tau \leftarrow MAC(K, \alpha)$

We define an attack game as follows:

1. MAC.Gen(1^k) outputs K_V, M_V.
2. The adversary chose a bit string α^*, and submits this to an oracle. The verification oracle generate a random key K then responds $\tau^* \leftarrow MAC(K, \alpha^*)$ to A.
3. A outputs a list:
$$((\alpha_1, \tau_1), \cdots, (\alpha_n, \tau_n))$$

We say that A has produced a forgery if for some $1 \leq i \leq n$ and $(\alpha_i, \tau_i) \neq (\alpha^*, \tau^*)$, we have $\tau_i \leftarrow MAC(K, \alpha_i)$. Define $AdvForge_{MAC,A}(k)$ to be the probability that A produces a forgery in the above game.

Definition 5 *A MAC scheme is secure against forgery attacks if the advantage of any PPT adversary A grows negligibly in k.*

Message authentication codes have been extensively studied. One can easily build secure one-time message authentication codes using an appropriate family of universal hash function, without relying one any intractability assumptions.

3 Weak BDH Assumption

Let G_1, G_2 be bilinear groups of prime order p. Let $e : G_1 \times G_2 \rightarrow G_T$ be the bilinear map.We define weak bilinear Diffie-Hellman problem as follow:

Given $(g, g^r \in G_1, Z \in G_T)$ as input, output $Z^r \in G_T$, where r is a random element in Z_p, g is random elment in G_1, $Z = e(g, g_1)$ and g_1 is a random element in G_2. We say an algorithm A has advantage ϵ in solving the weak bilinear Diffie-Hellman (WBDH) problem if

$$AdvWBDH = |Pr[A(g, g^r, Z) = Z^r]| \geq \epsilon$$

We define the decisional weak bilinear Diffie-Hellman(DWBDH) problem as follow:

Given $(g, g^r \in G_1, Z \in G_T)$ and $T \in G_T$, where r is a random element in Z_p, g is random elment in G_1, $Z = e(g, g_1)$ and g_1 is a random element

in G_2. We say an algorithm A that outputs $b \in \{0,1\}$ has advantage ϵ in solving the decision weak bilinear Diffie-Hellman problem in G if

$$AdvDWBDH = |Pr[A(g, g^r, Z, Z^r) = 0] - Pr[A(g, g^r, Z, T) = 0]| \geq \epsilon$$

We refer to the distribution on the left as D_{WBDH} and the distribution on the right as R_{WBDH}.

It is clear that if there is an algorithm A can resolve WBDH problem, we can construct another algorithm B to resolve BDH problem. While we don't know how to construct an algorithm to resolve WBDH if there is an algorithm can resolve BDH problem. So WBDH assumption is no stronger than BDH assumption. Similarly DWBDH assumption is no strong than DBDH assumption.

4 Basic Scheme

Our basic scheme is provably secure against IND-ID-CPA based on DWBDH assumption in standard model. Now we describe it as below:

- **Setup**: Let (G_1, G_2) be a bilinear group pair of prime order p, and let $e : G_1 \times G_2 \rightarrow G_T$ be a bilinear map in (G_1, G_2). The setup algorithm works as follow:

$$g \overset{R}{\leftarrow} G_1; g_1, g_2, g_3 \overset{R}{\leftarrow} G_2; H \overset{R}{\leftarrow} TCR$$

$$Z_1 \leftarrow e(g, g_1); Z_2 \leftarrow e(g, g_2);$$

$$params = (g, g_3, Z_1, Z_2, H); master\text{-}key = (g_1, g_2)$$

  Where H is TCR(target collision resistant) hash function [16].

- **Extract**:takes as input $params$, $master\text{-}key$, and an arbitrary $ID \in \{0,1\}^*$, the extract algorithm calculate the private key d as follow:

$$s \overset{R}{\leftarrow} Z_p; a \leftarrow H(ID);$$

$$d_1 \leftarrow g_3^s g_1^a g_2; d_2 \leftarrow g^s$$

$$d \leftarrow (d_1, d_2);$$

- **Encrypt**:takes as input $params$,ID, and $m \in \mathcal{M}$, the encrypt algorithm calculate the ciphertext C as follow:

$$r \overset{R}{\leftarrow} Z_p, a \leftarrow H(ID); c_1 \leftarrow g^r, c_2 \leftarrow g_3^r; c_3 \leftarrow Z_1^{ra} Z_2^r \cdot m$$

$$C \leftarrow (c_1, c_2, c_3)$$

- **Decrypt**: takes as input $params$,$C \in \mathcal{C}$, and a private key d, the decrypt algorithm calculate the plaintext m as follow:

$$m \leftarrow \frac{c_3 e(d_2, c_2)}{e(c_1, d_1)}$$

First we verify the consistence:

$$\frac{c_3 e(d_2, c_2)}{e(c_1, d_1)} = \frac{Z_1^{ra} Z_2^r \cdot m \cdot e(g^s, g_3^r)}{e(g^r, g_3^s g_1^a g_2)} = \frac{Z_1^{ra} Z_2^r \cdot m \cdot e(g, g_3)^{rs}}{e(g, g_3)^{rs} e(g, g_1^{ra}) e(g, g_2)^r}$$

$$= \frac{Z_1^{ra} Z_2^r \cdot m}{Z_1^{ra} Z_2^r} = m$$

Now we proved that the basic version of our IBE scheme is secure against IND-ID-CPA:

Theorem 1 *The basic IBE scheme is secure against chosen plain-text attack assuming that (1) the decision weak bilinear Diffie-Hellman problem is hard in group pair (G_1, G_2), (2) H is target collision resistant hash function[16].*

Let game G_0 be the original IND-ID-CPA game, let $b' \in \{0, 1\}$ denote the output of A, and let T_0 be the event that $b = b'$ in G_0, so that $AdvCPA_A = |Pr[T_0] - 1/2|$.

We will define a sequence $G_1, G_2, \ldots, G_l$ of modified attack games. Each of the games operates on the same underlying probability space. In particular, the public key and secret key of the cryptosystem, the coin tosses $Coins$ of A, and the hidden bit b take on identical values across all games. For any $1 \leq i \leq l$, we let T_i be the event that $b = b'$ in game G_i.

Game G_0

1. **Setup:**The challenger work as follow:

   I1: $g \overset{R}{\leftarrow} G_1; g_1, g_2, g_3 \overset{R}{\leftarrow} G_2; H \overset{R}{\leftarrow} TCR$

I2: $Z_1 \leftarrow e(g, g_1); Z_2 \leftarrow e(g, g_2);$

I3: $params = (g, g_3, Z_1, Z_2, H); master\text{-}key = (g_1, g_2)$

Finally $params$ is given to A.

2. **Phase1:** A make a sequence of extract queries with $ID_1, \cdots, ID_m$. The challenger computes:

Ex1: $s_i \overset{R}{\leftarrow} Z_p, a_i \leftarrow H(ID_i)$

Ex2: $d_i \leftarrow (g_3^{s_i} g_1^{a_i} g_2, g^{s_i})$

The challenger sends d_i to A.

3. **Challenge:**At some point, A makes an encryption query with two equal length plaintext $m_0, m_1 \in \mathcal{M}$ and an identity $ID \neq ID_i$. The challenger works as follow:

E1: $b \overset{R}{\leftarrow} \{0, 1\}$

E2: $r \overset{R}{\leftarrow} Z_p$

E3: $a \leftarrow H(ID)$

E4: $c_1 \leftarrow g^r, c_2 \leftarrow g_3^r$

E5: $c_3 \leftarrow Z_1^{ra} Z_2^r \cdot m_b$

E6: $C \leftarrow (c_1, c_2, c_3)$

The challenger sends C to A.

4. **Phase2:**A may continue to make extract queried with $ID_{m+1}, \cdots, ID_n (ID_i \neq ID)$, The challenger responds as phase 1.

5. **Guess:**Finally, A outputs a guess b'.

$b' \leftarrow A(Coins, params, \vec{ID}, \vec{d}, ID, C, m_0, m_1)$

where $\vec{ID} = (ID_1, \cdots, ID_n)$,$vecd = (d_1, \cdots, d_n)$

Game G_1 We modify the encryption oracle in game G_0 to obtain a new game G_1. Instead of using the original encryption algorithm, we modify the encryption algorithm, replacing step$E5$ with:

E5': $T \overset{R}{\leftarrow} G_T; c_2 \leftarrow T \cdot m_b$

Observe that, games $G0$ and $G1$ are the same except that in game $G0$, the quadruple $(g, Z_1^a Z_2, g^r, (Z_1^a Z_2)^r)$ is uniformly distributed in D_{WBDH}, and in game $G1$, the quadruple $(g, Z_1^a Z_2, g^r, T)$ is uniformly distributed in R_{WBDH}. Thus, any difference in behavior between these two games immediately yields a statistical test for distinguishing weak bilinear Diffie-Hellman quadruples from random quadruples. More precisely, we have

$$|Pr[T_1] - Pr[T_0]| \leq AdvDWBDH \tag{1}$$

Now let $g_1 = g_3^x, g_2 = g_3^y$, we get:

$$\log_{g_1}(d) = s + xa + y$$

$$\log_{g_1}(d_i) = s_i + xa_i + y$$

Since H is target collision resistant hash function, we get that$a \neq a_i$. So we have that the two equations are linear independent, and the probability of A get the private key d from d_i is $1/p$. And so we get that $(I\vec{D}, \vec{d}, m_0, m_1)$ are independent to b except a probability of:$(1/p) \times n + AdvTCR = n/p + AdvTCR$,where $AdvTCR_H$ is the advantage of attack on target collision resistant hash function(see [16] for detail),n is the times A queries extract oracle.

To complete the proof, we need to argue that b' is independent of b. First observe that by construction, b is independent of $(Conins, params)$. In the changed encryption oracle we get that b is independent to $(ID, C = (c_1, c_2))$(since T is random in G_T). We've showed that $(I\vec{D}, \vec{d}, m_0, m_1)$ are independent to b except a probability of $n/p + AdvTCR$. That's to say b is independent to $b' \leftarrow A(Coins, params, I\vec{D}, \vec{d}, ID, C, m_0, m_1)$ except with a negligible probability . And we have

$$|Pr[T_1] - 1/2| \leq n/p + AdvTCR \tag{2}$$

From $(1), (2)$ we have

$$AdvCPA_A = |Pr[T_0] - 1/2| \leq AdvDWBDH + n/p + AdvTCR \tag{3}$$

Now we've proved theorem 1.

5 Full Security Scheme

Based on our basic IBE scheme we construct a IND-ID-CCA secure IBE scheme. Our full security scheme is a hybrid scheme using our basic scheme

as the key encapsulation mechanism(KEM). Now we describe the full security scheme.

- **Setup**: Let (G_1, G_2) be a bilinear group pair of prime order p, and let $e : G_1 \times G_2 \to G_T$ be a bilinear map in (G_1, G_2). Constructs one-time symmetric-key encryption scheme SKE and one-time authentication code scheme MAC as in [16]. Choose target collision resist hash functions H_1, H_2, The setup algorithm works as follow:

$$g \overset{R}{\leftarrow} G_1; g_1, g_2, g_3 \overset{R}{\leftarrow} G_2;$$

$$Z_1 \leftarrow e(g, g_1); Z_2 \leftarrow e(g, g_2);$$

$$params = (g, g_3, Z_1, Z_2, H_1, H_2, SKE, MAC); master\text{-}key = (g_1, g_2)$$

- **Extract**:takes as input $params$, $master\text{-}key$, and an arbitrary $ID \in \{0,1\}^*$, the extract algorithm calculate the private key d as follow:

$$s \overset{R}{\leftarrow} Z_p; a \leftarrow H_1(ID);$$

$$d_1 \leftarrow g_3^s g_1^a g_2; d_2 \leftarrow g^s$$

$$d \leftarrow (d_1, d_2);$$

- **Encrypt**:takes as input $params$,ID, and $m \in \mathcal{M}$, the encrypt algorithm calculate the ciphertext C as follow:

$$r \overset{R}{\leftarrow} Z_p, a \leftarrow H_1(ID);$$

$$u_1 \leftarrow g^r, u_2 \leftarrow g_3^r$$

$$K \leftarrow H_2(Z_1^{ra} Z_2^r)$$

$$\chi \leftarrow SKE.Encrypt(K, m)$$

$$\tau \leftarrow MAC(K, \chi)$$

$$C \leftarrow (u_1, u_2, \chi, \tau)$$

- **Decrypt**: takes as input $params$,$C \in \mathcal{C}$, and a private key d, the decrypt algorithm calculate the plaintext m as follow:

$$K \leftarrow H_2(\frac{e(u_1, d_1)}{e(d_2, u_2)})$$

$$m \leftarrow SKE.Decrypt(K, \chi)$$

$$if\ \tau = MAC(K, \chi)\ return\ m; elsereturn\ \perp$$

SKE is secure against passive attack, MAC is secure against forge attack. We will prove that the scheme above is IND-ID-CCA secure in standard model.

Theorem 2 *The hybrid IBE scheme is secure against adaptive chosen cipher-text attack assuming that (1) the decision weak bilinear Diffie-Hellman problem is hard in (G_1, G_2), (2) SKE is secure against passive attack, and (3)MAC is secure against forgery attack, (4) H_1, H_2 are two target collision resistant hash functions.*

Let game G_0 be the original IND-ID-CCA game, let $b' \in \{0,1\}$ denote the output of A, and let T_0 be the event that $b = b'$ in G_0, so that $AdvCCA_A = |Pr[T_0] - 1/2|$.

We will define a sequence $G_1, G_2, \ldots, G_l$ of modified attack games. Each of the games operates on the same underlying probability space. In particular, the public key and secret key of the cryptosystem, the coin tosses $Coins$ of A, and the hidden bit b take on identical values across all games. For any $1 \leq i \leq l$, we let T_i be the event that $b = b'$ in game G_i.

Game G_0

1. The challenger work as follow:

   I1: $g \overset{R}{\leftarrow} G_1; g_1, g_2, g_3 \overset{R}{\leftarrow} G_2$

   I2: $Z_1 \leftarrow e(g, g_1); Z_2 \leftarrow e(g, g_2);$

   I3: $params = (g, g_3, Z_1, Z_2, H_1, H_2, SKE, MAC); master\text{-}key = (g_1, g_2)$

   Where SKE is symmetric-key encryption scheme, MAC is one-time authentication code scheme, H_1, H_2 are two TCR hash functions. Finally $params$ is given to A.

2. **Phase1:** The adversary issues queries $q_1, \cdots, q_m$ where query q_i is one of:

   - Extraction query $< ID_i >$. The challenger responds by running algorithm:

   Ex1: $s_i \overset{R}{\leftarrow} Z_p, a_i \leftarrow H_1(ID_i)$

   Ex2: $d_i \leftarrow (g_3^{s_i} g_1^{a_i} g_2, g^{s_i})$

   The challenger sends d_i to A.

   - Decryption query $< ID_i, C_i >$. The challenger calculates:

D1: $s_i \overset{R}{\leftarrow} Z_p, a_i \leftarrow H_1(ID_i)$
D2: $d_1 i \leftarrow g_3^{s_i} g_1^{a_i} g_2; d_2 i \leftarrow g^{s_i}$
D2: $K_i \leftarrow H_2(\frac{e(u_{1i}, d_{1i})}{e(d_{2i}, u_{2i})})$
D3: $m_i \leftarrow SKE.Decrypt(K_i, \chi_i)$
D4: $if\ \tau_i = MAC(K_i, \chi_i)\ return\ m_i; elsereturn\ \perp$

The challenger sends m_i or $\perp$ to A.

3. **Challenge:**At some point, A makes an encryption query with two equal length plaintext $M_0, M_1 \in \mathcal{M}$ and an identity $ID \neq ID_i$. The challenger works as follow:

E1: $b \overset{R}{\leftarrow} \{0, 1\}$
E2: $r \overset{R}{\leftarrow} Z_p$
E3: $a \leftarrow H_1(ID)$
E4: $u_1 \leftarrow g^r, u_2 \leftarrow g_3^r$
E5: $K \leftarrow H_2(Z_1^{ra} Z_2)$
E6: $\chi \leftarrow SKE.Encrypt(K, M_b)$
E7: $\tau \leftarrow MAC(K, \chi)$
E8: $C \leftarrow (u_1, u_2, \chi, \tau)$

The challenger sends C to A.

4. **Phase2:**A may continue issues queries $q_m + 1, \cdots, q_n$ where query q_i is one of:

   - Extraction query $< ID_i > \neq < ID >$. The challenger responds as phase 1.
   - Decryption query $< ID_i, C_i > \neq < ID, C >$. The challenger responds as phase 1.

5. **Guess:**Finally, A outputs a guess b'.

   $b' \leftarrow A(Coins, params, \vec{ID}, \vec{d}, \vec{C}, \vec{m}, ID, C, M_0, M_1)$
   where $\vec{ID} = (ID_1, \cdots, ID_n)$,$\vec{d} = (d_1, \cdots, d_n)$,$\vec{C} = (C_1, \cdots, C_n)$,$\vec{m} = (m_1, \cdots, m_n)$

Game G_1 We modify the encryption oracle in game G_0 to obtain a new game G_1. Instead of using the original encryption algorithm, we modify the encryption algorithm, replacing step$E5$ with:

E5': $T \stackrel{R}{\leftarrow} G_T; K \leftarrow H_2(T)$

Observe that, games $G0$ and $G1$ are the same except that in game $G0$, the quadruple $(g, Z_1^a Z_2, g^r, (Z_1^a Z_2)^r)$ is uniformly distributed in D_{WBDH}, and in game $G1$, the quadruple $(g, Z_1^a Z_2, g^r, T)$ is uniformly distributed in R_{WBDH}. Thus, any difference in behavior between these two games immediately yields a statistical test for distinguishing weak bilinear Diffie-Hellman quadruples from random quadruples. More precisely, we have

$$|Pr[T_1] - Pr[T_0]| \leq AdvDWBDH \tag{4}$$

Similarly to the proof of the basic scheme, we get that $(\vec{ID}, \vec{d})$ are independent to b except a probability of:$n/p + AdvTCR$

Now we will show that the decryption oracle in game $G1$ leaks nothing about the plaintext except a negligible probability $AdvForge_{MAC}$. If A tries to get a ciphertext $C_i = (u_{1i}, u_{2i}, \chi_i, \tau_i)$ from a legal ciphertext $C = (u_1, u_2, \chi, \tau)$ such that $C_i \neq C$, then the probability of $Pr[\tau_i = MAC(K_i, \chi_i)]$ is $AdvForge_{MAC}$. So, if $\tau_i = MAC(K_i, \chi_i)$, it must be the case that A knows m_i and constructs the ciphertext by $Encrypt(params, ID, m_i)$ except a negligible probability $AdvForge_{MAC}$. Now we have that no further information about the plaintext will be leaked by the decryption oracle in game $G1$ except with a negligible probability $AdvForge_{MAC}$.

To complete the proof, we need to argue that b' is independent of b. First observe that by construction, b is independent of $(Conins, params)$. In the changed encryption oracle we get that b is independent to $(ID, C = (u_1, u_2, \chi, \tau))$, except a negligible property of $AdvPA_{SEK}$. We've showed that the decryption oracle won't leak any further information about the according plaintext. That's to say b is independent to $(\vec{C}, \vec{m}, M_0, M_1)$ except a negligible probability $AdvForge_{MAC}$. Now we have that b is independent to $b' \leftarrow A(Coins, params, \vec{C}, \vec{m}, M_0, M_1)$ except with a negligible probability . And we have

$$|Pr[T_1] - 1/2| \leq AdvForge_{MAC} + AdvPA_{SEK} + AdvTCR + n/p \tag{5}$$

From (4), (5) we have

$$AdvCCA_A = |Pr[T_0] - 1/2|$$

$$\leq AdvDWBDH + AdvForge_{MAC} + AdvPA_{SEK} + AdvTCR + n/p \tag{6}$$

Now we've proved theorem 2.

6 Efficiency Analysis

The efficiency of our basic scheme and full scheme ,BB1,Wat05 and EK06 is list in table2.

Table 2: Efficiency comparison(1 unit = general exponent in G_1, G_2)

	Extract	Encrypt	Decrypt	Ciphertext over-head(bit)	Assumption	Security
BB1	0.5	1.3	24	$2\|p\|$	DBDH	IND-sID-CPA
Wat05	1.4	2	24	$2\|p\|$	DBDH	IND-ID-CPA
EK06	1.6	2.3	24	$2\|p\|$	mDBDH	IND-ID-CCA(IB-KEM)
Basic	0.5	2	24	$2\|p\|$	WDBDH	IND-ID-CPA
Full	0.5	2	24	$2\|p\| + \|t\|$	WDBDH	IND-ID-CCA

Table 3: Timing value of different operations(1 unit = general exponent in G_1, G_2)[19]

operation	time(exp)
fix-base exponent in G_1, G_2	0.2
general exponent in G_1, G_2	1
general multi-exponent in G_1, G_2	1.5
hashing to G_1, G_2	1
fix-base exponent in G_T	0.8
general exponent in G_T	4
general multi-exponent in G_T	6
single pairing	20
ratio of pairing	24

Where "BB1" is the first IBE scheme in [8],"Wat05" is the IBE scheme in [9], "EK06" is the IB-KEM in [15], "Basic" is the basic version of our scheme, "Full" is the full security version of our scheme. When tabulating computational efficiency hash function(to Z_p) and block cipher evaluations are ignored. See table-3 for the timing value of different operations. Cipher-text overhead represents the difference between the cipher-text length and the message length, and $|p|$ is the length of a group element in G_1 or G_2, $|t|$ is the length of MAC. It is clear that our schemes are efficient in both

computation and ciphertext overhead.

7 Conclusion

Based on a new assumption in bilinear group we construct a new IBE scheme which is efficient in both computation and ciphertext length. The new assumption is named as weak bilinear Diffie-Hellman assumption. It is no stronger than the bilinear Diffie-Hellman assumption. We proved our scheme in standard model. The basic version of our IBE scheme is provably secure against chosen plaintext attack(IND-ID-CPA) and the full version of our IBE scheme which is a hybrid IBE scheme is provably secure against adaptive chosen ciphertext attack(IND-ID-CCA).

References

[1] Adi Shamir. Identity-based cryptosystems and signature schemes. In Advances in CryptologyCRYPTO 1984, volume 196 of LNCS, pages 47C53. Springer-Verlag, 1984.

[2] Dan Boneh and Matt Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, Advances in CryptologyCRYPTO 2001, volume 2139 of LNCS, pages 213C29. Springer-Verlag, 2001.

[3] Clifford Cocks. An identity based encryption scheme based on quadratic residues. In Proceedings of the 8th IMA International Conference on Cryptography and Coding, pages 26C8, 2001.

[4] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In ACM CCS 93, pages 62-73. ACM Press, Nov. 1993.

[5] R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited. In 30th ACM STOC, pages 209-218. ACM Press, May 1998.

[6] Ran Canetti, Shai Halevi, and Jonathan Katz. A forward-secure public-key encryption scheme. In Advances in CryptologyEUROCRYPT 2003, volume 2656 of Lecture Notes in Computer Science. Springer-Verlag, 2003.

[7] Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identitybased encryption. In Advances in CryptologyEURO-

CRYPT 2004, volume 3027 of LNCS, pages 207C22. Springer-Verlag, 2004.

[8] Dan Boneh and Xavier Boyen. Efficient selective-ID secure identity based encryption without random oracles. In Advances in CryptologyEUROCRYPT 2004, volume 3027 of Lecture Notes in Computer Science, pages 223C38. Springer-Verlag, 2004. http://www.cs.stanford.edu/ xb/eurocrypt04b/.

[9] Brent Waters. Efficient identity-based encryption without random oracles. In Advances in CryptologyEUROCRYPT 2005, volume 3494 of Lecture Notes in Computer Science. Springer- Verlag, 2005.

[10] Xavier Boyen, Qixiang Mei, and Brent Waters. Direct chosen ciphertext security from identitybased techniques. In ACM Conference on Computer and Communications SecurityCCS 2005. ACM Press, 2005. http://www.cs.stanford.edu/ xb/ccs05/.

[11] J. Horwitz and B. Lynn. Toward hierarchical identity-based encryption. In L. R. Knudsen, editor, EUROCRYPT 2002, volume 2332 of LNCS, pages 466-481. Springer-Verlag, Apr. 2002.

[12] C. Gentry and A. Silverberg. Hierarchical ID-based cryptography. In Y. Zheng, editor, ASI- ACRYPT 2002, volume 2501 of LNCS, pages 548-566. Springer-Verlag, Dec. 2002.

[13] Craig Gentry. Practical identity-based encryption without random oracles. In Advances in CryptologyEUROCRYPT 2006, Lecture Notes in Computer Science. Springer-Verlag, 2006.

[14] D. Boneh and J. Katz. Improved eciency for CCA-secure cryptosystems built using identity- based encryption. In A. Menezes, editor, CT-RSA 2005, volume 3376 of LNCS, pages 87-103. Springer-Verlag, Feb. 2005.

[15] E. Kiltz and D. Galindo. Direct chosen-ciphertext secure identity-based encryption without ran- dom oracles. Cryptology ePrint Archive, Report 2006/034, 2006. http://eprint.iacr.org/.

[16] R. Cramer and V. Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM Journal on Computing, 33(1):167-226, 2003.

[17] K. Bentahar, P. Farshim, J. Malone-Lee, and N. Smart. Generic constructions of identity- based and certicateless KEMs. Cryptology ePrint Archive, Report 2005/058, 2005. http://eprint.iacr.org/.

[18] M. Barbosa,L. Chen, Z. Cheng, M. Chimley, A. Dent, P. Farshim, K. Harrison, J. Malone-Lee, N. P.Smart, F.Vercauteren,SK-KEM: An Identity-Based KEM , http://grouper.ieee.org/groups/1363/IBC/submissions/index.html, Submitted 2006-06-07.

[19] X.Boyen,The BB1 Identity-based cryptosystem:A standard for Encryption and Key Encapsulation,http://grouper.ieee.org/groups/1363/IBC/submissions/index.html, Submitted 2006-08-14.

[20] Ryuichi Sakai and Masao Kasahara. ID based cryptosystems with pairing over elliptic curve. Cryptology ePrint Archive, Report 2003/054, 2003. http://eprint.iacr.org/2003/054/.

[21] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In Advances in Cryptology EUROCRYPT 2005, volume 3494 of Lecture Notes in Computer Science. Springer-Verlag, 2005.

[22] David Naccache. Secure and practical identity-based encryption. Cryptology ePrint Archive, Report 2005/369, 2005. http://eprint.iacr.org/2005/369/.

[23] Sanjit Chatterjee and Palash Sarkar. Trading time for space: Towards an efficient IBE scheme with short(er) public parameters in the standard model. In Proceedings of ICISC 2005, 2005.

[24] Xavier Boyen and Brent Waters. Anonymous hierarchical identity-based encryption (without random oracles). In Advances in CryptologyCRYPTO 2006, volume 4117 of Lecture Notes in Computer Science. Springer-Verlag, 2006. http://www.cs.stanford.edu/ xb/crypto06a/.