Practical IBE Secure under CBDH - Encrypting Without Pairing

S. Sree Vivek[1], S. Sharmila Deva Selvi[2], Aanchal Malhotra[3] and C. Pandu Rangan[4]
[1]*Samsung R&D Institute, Bangalore, India*
[2]*Microsoft Research India, Bangalore, India*
[3]*Boston University, Boston, MA, U.S.A.*
[4]*IIT-Madras, Chennai, India*

Keywords: Identity based Cryptography, Encryption without Bilinear Pairing, Without Full Domain Hash, Provable Security, Random Oracle Model.

Abstract: Since the discovery of identity based cryptography, a number of identity based encryption schemes were reported in the literature. Although a few schemes were proposed after its introduction, the first efficient identity based encryption scheme was proposed by Dan Boneh and Matthew K. Franklin in 2001. This encryption scheme uses Weil pairing on elliptic curves during both encryption and decryption process. In this paper, we propose a new identity based encryption scheme and prove its security in the random oracle model. There are two highlighting features in our scheme. First, it does not employ bilinear pairing computation during the encryption process. Second, our scheme does not require full domain hashing, which makes our scheme more practical and efficiently implementable. Moreover, we prove the security of our scheme by reducing it to the well known Computational Bilinear Diffie-Hellman problem. We first prove the security of our scheme in weaker security notion i.e. we prove our scheme to be IND-CPA secure. Then using Fujisaki Okamoto transformation, we convert our scheme to IND-CCA secure version.

1 INTRODUCTION

Identity-based (from now on, ID-based) cryptography was introduced by Adi Shamir (Shamir, 1984) in his seminal paper as an alternative to traditional public key cryptography. Traditional public key cryptography makes use of Public Key Infrastructures (PKI). In PKI-based system, each user generates on his own his private and public key. The certification authority of the PKI provides a digital certificate which links the identity of the user and his public key. The validity of this certificate must be checked before using the public key of the user, when encrypting a message to him or when verifying a signature from him. Obviously, the management of digital certificates degrades the efficiency of public key cryptosystems in practice. The idea of ID-based cryptography is to use the identity of a user (e-mail address, telephone number, etc.) as the public key. The user contacts a trusted entity, Private Key Generator (PKG), to obtain the private key corresponding to his identity. The PKG typically uses a secret information called *master secret* to compute the private key corresponding to the identity of the user. This private key is then distributed to the authorised user through a secure channel.

ID-based cryptography has been the object of a lot of research during the last decade. ID-based encryption is an interesting technology because other public-key algorithms have encountered difficulty in practical use. It provides an easy solution that provides for the confidentiality of data. A number of ID-based encryption schemes have been proposed in both standard model (Boneh and Boyen, 2011)(Agrawal et al., 2010)(Kiltz, 2006)(Gentry, 2006)(Waters, 2005) and random oracle model (Boneh and Franklin, 2005)(Attrapadung et al., 2007)(Sakai and Kasahara, 2003). The most efficient ID-based encryption schemes are currently based on bilinear pairings on elliptic curves, such as the Weil or Tate pairings. The first of these schemes was developed by Dan Boneh and Matthew K. Franklin (Boneh and Franklin, 2005) and performs probabilistic encryption of arbitrary ciphertexts using an Elgamal-like approach. Many ID-based encryption schemes have been proposed since then, adopting many different strategies, thereby reducing the computational cost and the ciphertext size.

Table 1 recollects the complete bibliography of different ID-based Key constructs used till date.

Sree Vivek S., Sharmila Deva Selvi S., Malhotra A. and Pandu Rangan C..
Practical IBE Secure under CBDH - Encrypting Without Pairing.
DOI: 10.5220/0005541802510258
In *Proceedings of the 12th International Conference on Security and Cryptography* (SECRYPT-2015), pages 251-258
ISBN: 978-989-758-117-5

Table 1: Properties of existing ID-based Key constructs.

Scheme	**ID-based Key Constructs**	**IBE**	**Pairing**		**Assumption**	**FDH**
			Enc	Dec		
BLS (Boneh et al., 2004)	$D_A = sQ_A \in \mathbb{G}_1$ $Q_A = \hat{H}(ID_A) \in \mathbb{G}_1$	Y	Y	Y	CBDH	Y
Barreto (Barreto et al., 2005)	$D_A = \frac{1}{s+q_A}P \in \mathbb{G}_1$ $q_A = \hat{H}(ID_A) \in \mathbb{Z}_q^*$	Y	N	Y	q-SBDH	N
Galindo (Galindo and Garcia, 2009)	$d_A = (x_A + s_1 q_A) \bmod q \in \mathbb{Z}_q^*$ $X_A = x_A P \in \mathbb{G}_1$ $q_A = \hat{H}(ID_A) \in \mathbb{Z}_q^*$	N	-	-	-	-
Selvi (Selvi et al., 2011)	$d_A = (s_1 q_A + s_2 x_A) \in \mathbb{Z}_q^*$ $X_A = x_A P \in \mathbb{G}_1, Y_A = y_A P \in \mathbb{G}_1$ $q_A = \hat{H}(ID_A) \in \mathbb{Z}_q^*$	N	-	-	-	-
Ours	$d_A = (sq_A + r_A) \in \mathbb{Z}_p$ $X_A = r_A Q+$ $\bar{r}_A(u_o + \sum_{i=1}^{k} q_A[i]u_i) \in \mathbb{G}_1$ $Y_A = \bar{r}_A P \in \mathbb{G}_1$ $q_A = \hat{H}(ID_A) \in \{0,1\}^k$	Y	N	Y	CBDH	N

Motivation. Typically, the computationally most expensive part of implementing ID-based encryption algorithms is execution of bilinear pairings. Thus, our main concern in this paper is to avoid bilinear pairing during encryption. Till now, all but one scheme by Sakai-Kasahara (Sakai and Kasahara, 2003) use bilinear pairing during the encryption process. This scheme is quite efficient, in terms of computational complexity when compared with other ID-based encryption schemes. Later, the security of this scheme was proved by Chen and Cheng (Chen and Cheng, 2005) under q-SBDH assumption, which is a stronger assumption. Our attempt was to construct a scheme which reduces to a weaker and well known assumption.

Secondly, in practice it is difficult to build a Full Domain Hash (FDH) which hashes directly onto a group of points on an elliptic curve (Boneh and Franklin, 2005). However with a slightly reduced cost in computation, it is achieved by hashing onto some arbitrary set, and then using some deterministic admissible encoding function to map onto the elliptic curve group. In our scheme, instead of FDH we make use of a computation similar to Waters' hash (Waters, 2005) and hence our scheme can be easily and efficiently realized in practice.

Our Contribution. Our first interesting contribution is a novel probabilistic PKI based signature scheme (and this is of specific interest) described in section 3. The novelty of this signature scheme is; it is based on Schnorr's signature (Schnorr, 1989) but does not take the randomness used to generate the signature as an input to the message hash. In an ID-based scheme, the private key of the user is constructed using a PKI based signature scheme. While randomized signature schemes such as Schnorr (Schnorr, 1989),(Selvi et al., 2011),(Galindo and Garcia, 2009),(Herranz, 2006) are used to extract the private key of the user in ID-based signatures, they can not be used for extracting the private key of a user for an ID-based encryption scheme. This is because the randomness used to extract the private key should also be a component of the public key of the ID-based scheme. While in an ID-based signature scheme, this randomness can be sent along with the signature for verification, it can not be done in IBE scheme, since in an IBE scheme, the public key of the user must be the identity alone. Thus, in our IBE scheme we use a construction similar to Waters' hash (Waters, 2005), which helps us to achieve binding between the identity of the user and the private key, without including the randomness in the message hash. In addition, this helps us in avoiding the use of full domain hashes in the design of the ID-based encryption scheme. Next we show the construction of the novel ID-based encryption scheme in section 4 which does not use pairing during encryption process. However, during the decryption process we require pairing computation. The significant advantage of our scheme is that it does not compromise on security and is proven secure under the well known CBDH assumption.

Table 2 compares different ID-based encryption schemes in random oracle model in terms of underly-

Table 2: Properties of ID-based Encryption Schemes in Random Oracle Model.

Scheme	**Hard Problem Assumption**	**Encryption Complexity**	**Decryption Complexity**	**Cipher Text Size**
Boneh Franklin (Boneh and Franklin, 2005)	CBDH	1P+2EM	1P	$\|\|\mathbb{G}\|\|+\|m\|$
Katz and Wang (Katz and Wang, 2003) (Attrapadung et al., 2007)	GBDH	2P+4EM	1P	$2\|\|\mathbb{G}\|\|+2\|m\|$
Attrapadung *et al* (Attrapadung et al., 2007)	LBDH	2P+2EM+1SKE	2P+2EM	$\|\|\mathbb{G}\|\|+\|m\|+2\rho$
Sakai and Kasahara (Sakai and Kasahara, 2003)	q-SBDH	3EM	1P+1EM	$\|\|\mathbb{G}\|\|+\|m\|+\rho$
Ours (Γ' scheme)	CBDH	ρEA+3EM	2P+1EM	$2\|\|\mathbb{G}\|\|+\|m\|+\rho$

P - Pairing, EM - Elliptic curve scalar point multiplication, EA - Addition of two elliptic curve points, SKE - Complexity of CCA-2 secure Symmetric Key Encryption, $||\mathbb{G}||$ - Size of one group element, $|m|$ - Size of message, ρ - Number typically of size 128 bits. CBDH - Computational Bilinear Diffie-Hellman, GBDH - Gap Bilinear Diffie-Hellman, LBDH - List Bilinear Diffie-Hellman, q-SBDH - q- Strong Bilinear Diffie-Hellman.

ing hard problem assumption, computation complexity of encryption and decryption processes, and size of generated ciphertext. Our scheme involves the computation of elliptic curve point additions and avoids the use of bilinear pairing during encryption. However, the time complexity for executing one bilinear pairing is roughly four times the time complexity for executing upto 160 elliptic curve point additions (Islam and Biswas, 2012). From table 2, it is clear that compared to other schemes, we have reduced the computation cost during encryption process to a great extent in our scheme by avoiding bilinear pairing. There is one other scheme by Sakai and Kasahara (Sakai and Kasahara, 2003) that does not involve pairing computation during encryption. Although the decryption cost of our scheme is higher than that of (Sakai and Kasahara, 2003), we argue that our scheme is better than the scheme in (Sakai and Kasahara, 2003). This is because the security of our scheme is reduced to the well known CBDH problem whereas the scheme in (Sakai and Kasahara, 2003) has a security reduction to the stronger q-SBDH assumption. Similarly, the decryption cost of our scheme is higher when compared with (Boneh and Franklin, 2005) but our scheme offers two advantages over (Boneh and Franklin, 2005). First our scheme does not involve bilinear pairing computation during encryption, and second it does not use Full Domain Hash, thus making it efficiently implementable.

2 PRELIMINARIES

In this section, we briefly recall the basics and security models.

2.1 Bilinear Pairing

Let $\mathbb{G}_1$ be a cyclic additive group generated by P, with prime order q, and $\mathbb{G}_2$ be a cyclic multiplicative group of the same order q. A bilinear pairing is a map $\hat{e}$: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ with the following properties.

Bilinearity. For all $P, Q, R \in \mathbb{G}_1$,

$\hat{e}(P, Q+R) = \hat{e}(P, Q)\hat{e}(P, R)$.

$\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ $[Where\, a, b \in_R \mathbb{Z}_p]$.

Non-degeneracy. There exist $P, Q \in \mathbb{G}_1$ such that $\hat{e}(P, Q) \neq \mathbb{I}_{\mathbb{G}_2}$, where $\mathbb{I}_{\mathbb{G}_2}$ is the identity element of $\mathbb{G}_2$.

Computability. There exists an efficient algorithm to compute $\hat{e}$(P,Q) for all $P, Q \in \mathbb{G}_1$.

2.2 Computational Assumptions

In this section, we review the computational assumptions related to bilinear maps that are relevant to the protocol we discuss.

Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be a bilinear map. Let P be a generator of $\mathbb{G}_1$, whose order is a large prime q. Let a, b, c be elements of $\mathbb{Z}_p$.

Definition 1 (Computational Diffie-Hellman Problem (CDHP))**.** Given $(P, aP, bP) \in \mathbb{G}_1^3$ for unknown a, b $\in \mathbb{Z}_p$, the CDH problem in $\mathbb{G}_1$ is to compute *abP*. The advantage of any probabilistic polynomial time algorithm $\mathcal{A}$ in solving the CDH problem in $\mathbb{G}_1$ is defined as:

$$Adv_{\mathcal{A}}^{CDH} = Pr[\mathcal{A}(P, aP, bP) = abP | a, b \in \mathbb{Z}_p]$$

The CDH assumption is that, for any probabilistic polynomial time algorithm $\mathcal{A}$, the $Adv_{\mathcal{A}}^{CDH}$ is negligibly small.

Definition 2 (Computational Bilinear Diffie-Hellman Problem (CBDH))**.** Given $(P, aP, bP, cP) \in \mathbb{G}_1^4$ for unknown a, b, c $\in \mathbb{Z}_p$, the CBDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$ is to compute $\hat{e}(P,P)^{abc} \in \mathbb{G}_2$. The advantage of any probabilistic polynomial time algorithm $\mathcal{A}$ in solving the CBDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$ is defined as:

$$Adv_{\mathcal{A}}^{CBDH} = Pr[\mathcal{A}(P, aP, bP, cP) = \hat{e}(P,P)^{abc} \,|\, a, b, c \in \mathbb{Z}_p]$$

The CBDH assumption is that, for any probabilistic polynomial time algorithm $\mathcal{A}$, the $Adv_{\mathcal{A}}^{CBDH}$ is negligibly small.

2.3 Generic Framework for PKI-based Signature Scheme

The framework for a PKI based signature scheme consists of the algorithms **KeyGen**, **Sign**, **and Verify**. The algorithms are defined below:

KeyGen: takes a security parameter κ as input, and outputs a *private key sk* and the corresponding public key *pk*.

Sign: takes private key *sk*, public key *pk* and the message $m \in \mathcal{M}$ as input. It outputs the signature σ.

Verify: takes signature σ, message $m \in \mathcal{M}$ and the public key *pk* as input. It either accepts or rejects the message claim to authenticity.

These algorithms must meet the standard consistency constraint. For all $(pk, sk) \leftarrow$***KeyGen*** and all $m \in \mathcal{M}$, we have ***Verify*** = $(pk, m,$ ***Sign*** $(pk, sk, m)) = accept$.

2.4 Security Model for PKI-based Signature Scheme

Existential unforgeability is a standard acceptable notion of security for signature schemes. We say that any signature scheme is existentially unforgeable under adaptive chosen message attacks if any polynomially bounded adversary $\mathcal{A}$ has negligible advantage in the following game with the challenger $\mathcal{C}$.

KeyGen: $\mathcal{C}$ runs the KeyGen algorithm and generates the system parameters *params* and the secret key *sk*. It gives *params* to $\mathcal{A}$ and keeps *sk* secret.

Training Phase: After the KeyGen phase is over, $\mathcal{A}$ starts interacting with $\mathcal{C}$ by querying various oracles provided by $\mathcal{C}$ in the following way:

- ***Random Oracle:*** $\mathcal{A}$ queries hash function listed in *params* for any arguments, and $\mathcal{C}$ responds by treating the hash function as a random function.
- ***Sign Oracle:*** $\mathcal{A}$ issues signature queries on message m. Using *sk*, $\mathcal{C}$ runs the signing algorithm and returns a resulting signature σ as response. Additionally, $\mathcal{C}$ maintains a set W ($W = \{\phi\}$ initially) and when m is queried by $\mathcal{A}$ to the sign oracle, $\mathcal{C}$ updates W as $W = W \cup \{m\}$.

Sign Forgery: On obtaining sufficient training, $\mathcal{A}$ outputs a valid message-signature (m^*, σ^*) pair such that the following two conditions hold: 1. ***Verify*** (pk, m^*, σ^*) = accept, and 2. $(m^*) \notin W$ where W is set of all messages queried by $\mathcal{A}$ in ***Sign Oracle***.

The advantage of an adversary $\mathcal{A}$ in breaking the chosen plaintext security of signature scheme is defined as:

$$Adv_{\mathcal{A}}^{EUF-CMA} = \Pr[\mathcal{A} \rightarrow (m^*, \sigma^*) : \textbf{\textit{Verify}}\ (pk, m^*, \sigma^*) = accept \bigwedge (m^*) \notin W].$$

2.5 Generic Framework for ID-based Encryption Scheme

An ID-based encryption scheme can be defined as a tuple $\langle \mathcal{S}, \mathcal{K}, \mathcal{E}, \mathcal{D} \rangle$, where $\mathcal{S}$ is the setup algorithm, $\mathcal{K}$ is the key extract algorithm, $\mathcal{E}$ is the encryption algorithm, and $\mathcal{D}$ is the decryption algorithm. The algorithms are defined as shown below:

Setup: takes a security parameter κ and returns params (system parameters) and master key. Params include a definition of finite message space $\mathcal{M}$, and a description of a finite ciphertext space $\mathcal{C}$. Intuitively, params will be publicly known, while the master key will be known only to the “Private Key Generator”(PKG).

Key Extract: takes params, master-key, and an arbitrary ID as input, and returns a private key d. Here ID is the identity string that is used as a public key, and d is the corresponding private decryption key. $\mathcal{K}$ extracts a private key from the given public key.

Encrypt: takes params, ID, and $M \in \mathcal{M}$ as input. It returns a ciphertext $C \in \mathcal{C}$.

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

These algorithms must satisfy the standard consistency constraint. When d is the private key generated by the ***Key Extract*** algorithm and corresponds to the identity *ID*, the following should hold.

$$\forall M \in \mathcal{M} : \textbf{\textit{Decrypt:}}\ (params, C, d) = M,\ where\ C = \textbf{\textit{Encrypt:}}\ (params, ID, M).$$

2.6 Security Model for ID-based Encryption Scheme

Chosen plaintext security (IND-CPA) is the standard acceptable notion of security for encryption schemes. We say that an ID-based encryption scheme is semantically secure against adaptive chosen plaintext attack (IND-CPA) if any polynomially bounded adversary $\mathcal{A}$ has negligible advantage in the following game with the challenger $\mathcal{C}$:

Setup: *Challenger $\mathcal{C}$ runs the Setup algorithm. It gives $\mathcal{A}$ the resulting system parameters params. It keeps the master key msk to itself.*

Phase I: *$\mathcal{A}$ issues queries $q_1, q_2, \ldots, q_m$ where q_i is* as follows:

KeyExtract Query $\langle ID_i \rangle$: $\mathcal{C}$ corresponds by running KeyGen algorithm to generate the private key d_i. It sends d_i to $\mathcal{A}$. These queries may be asked adaptively i.e. each query q_i may depend on the replies to $q_1, q_2, \ldots, q_{i-1}$.

Challenge: *$\mathcal{A}$ after getting sufficient training gives two messages (m_0, m_1) of equal length, and an identity ID^* on which it wishes to be challenged to $\mathcal{C}$. $\mathcal{C}$ picks a random bit $b \in \{0,1\}$ and sets the challenge ciphertext to $C^* = Encrypt\,(params, ID^*, m_b)$. It sends C^* as a challenge to $\mathcal{A}$.*

Phase II: *$\mathcal{A}$ is again allowed to get training after getting the challenge ciphertext C^*.* The only restriction is that the private key of ID^* should not be queried to the key extract oracle.

Guess: *Finally, after getting training in* ***Phase II****, $\mathcal{A}$ produces an educated guess $b' \in \{0,1\}$. $\mathcal{A}$ wins if $b' = b$. The advantage of $\mathcal{A}$ in breaking the chosen plaintext security of an ID-based encryption system is given by,*

$$Adv_{\mathcal{A}}^{IND-CPA} = \left| Pr[b' = b] - \frac{1}{2} \right|.$$

3 BASIC SIGNATURE SCHEME ($Basic_{Sign}$)

We will now construct a secure public key signature scheme in the random oracle model under the CDH assumption. This signature scheme is weakly unforgeable, i.e. the adversary is not allowed to submit as forgery a message signature pair for which message it has already queried the signature oracle. This is a PKI based signature scheme and this will be used by the PKG to generate the private key for the users of an ID-based encryption scheme.

User KeyGen: Let κ be the security parameter and $\mathbb{G}_1, \mathbb{G}_2$ be cyclic prime order groups of order p, where $\mathbb{G}_1$ is an additive group and $\mathbb{G}_2$ is a multiplicative group. Choose $P, Q \in_R \mathbb{G}_1$, and let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be a bilinear map. To generate the key, user chooses $s \in_R \mathbb{Z}_p$ and computes the public key $P_{pub} = sP$. The user also chooses random values $u_0, u_1 \ldots\ldots u_k \in \mathbb{G}_1$ and a cryptographic hash function $H_1(.)$ defined by,

$$H_1 : \{0,1\}^n \rightarrow \{0,1\}^k$$

Here k is a number typically of size 128 bits, to ensure collision resistance against birthday attack. And n is the size of message. The public key is $\langle \mathbb{G}_1, \mathbb{G}_2, P, Q, p, \hat{e}, H_1, P_{pub}, u_0, u_1 \ldots.. u_k \rangle$. The private key of the user is $\langle s \rangle$.

Sign: For generating the signature on message $m \in \{0,1\}^n$ by the user, this algorithm uses the private key of the user and performs the following:

- Computes $q_m = H_1(m) \in \{0,1\}^k$. Here, q_m represents a k-bit number. Let $q_m[i]$ represent the i^{th} bit of q_m.
- Chooses random $r_m, \bar{r}_m \in \mathbb{Z}_p$.
- Sets $d_m = sq_m + r_m \in \mathbb{Z}_p$.
- Sets $Y_m = \bar{r}_m P \in \mathbb{G}_1$.
- Sets $X_m = r_m Q + \bar{r}_m(u_o + \sum_{i=1}^{k} q_m[i]u_i) \in \mathbb{G}_1$.
- Outputs the signature $\sigma = \langle d_m, Y_m, X_m \rangle$.

Verify: Now, the generated signature can be verified as follows:

- On receiving $\sigma = \langle d_m, Y_m, X_m \rangle$, compute $q_m = H_1(m)$ and $r_m P = d_m P - q_m(sP) = d_m P - q_m(P_{pub})$.
- Check if $\hat{e}(P, X_m) \overset{?}{=} \hat{e}(Y_m, (u_0 + \sum_{i=1}^{k} q_m[i]u_i))$ $\hat{e}(r_m P, Q)$.
  If the above check holds, return the signature as "*Valid*" else return "*Invalid*".

<u>**Correctness:**</u> If the signature is generated correctly, then it will pass the verification test. In fact,

$$\begin{aligned} LHS = \hat{e}(P, X_m) &= \hat{e}(P,\, r_m Q + \bar{r}_m(u_0 + \sum_{i=1}^{k} q_m[i]u_i)) \\ &= \hat{e}(P,\, r_m Q)\; \hat{e}(P,\, \bar{r}_m(u_0 + \sum_{i=1}^{k} q_m[i]u_i)) \\ &= \hat{e}(r_m P,\, Q)\; \hat{e}(\bar{r}_m P,\, (u_0 + \sum_{i=1}^{k} q_m[i]u_i)) \\ &= \hat{e}(r_m P,\, Q)\; \hat{e}(Y_m,\, (u_0 + \sum_{i=1}^{k} q_m[i]u_i)) \\ &= RHS \end{aligned}$$

Remark. For generating the private keys of the users of an ID-based system, a PKI based signature scheme will be used by the PKG of the ID-based system. We want our PKI based signature scheme to have the following properties:

- In the signature scheme, the message hash should not take any other parameters as input. Hence Schnorr (Schnorr, 1989) type signature schemes cannot be used for the purpose. In order to offer existential unforgeability, Schnorr type signature schemes will always use hash functions of the type $H(message, randomness, ...)$. In fact, if the hash function uses only the message as the parameter, the signature scheme becomes forgeable. Hence the hash function uses additional randomness as an input parameter. However such schemes if used by a PKG, leads to inefficient ID-based encryption schemes.
- Our second goal is to avoid Full Domain Hash function and hence we make use of a computation similar to Waters' hash function. Hence the BLS (Boneh et al., 2004) type signatures which use FDH cannot be used for our purpose.

Since none of the existing key constructs are suitable for our purpose, we have come up with a novel key construct. Although, unlike Schnorr signature scheme, our scheme uses only message as the input to the hash, still our scheme is secure because we have bound the randomness r_m and hash H_1 in other components of the signature through a computation similar to Waters' hash.

Theorem 1: *If there exists an EUF-CMA adversary for our $Basic_{Sign}$ scheme with a non-negligible probability, then we show that there exists a challenger $\mathcal{C}$ who can solve the Computational Diffie-Hellman problem $(CDHP)$ on $\mathbb{G}_1$ with almost the same probability.*

4 CONSTRUCTION OF A CPA SECURE ENCRYPTION SCHEME

In this section we propose a novel ID-based encryption scheme without using bilinear pairing during encryption and prove the security in random oracle model, assuming the hardness of Computational Bilinear Diffie-Hellman Problem (CBDHP). The PKG of this scheme uses $Basic_{Sign}$ signature scheme explained in the previous section to generate private key of the user. The details of the new scheme and the formal proof is given below.

4.1 The Scheme (Γ-Scheme)

Setup: Let κ be the security parameter and $\mathbb{G}_1$, $\mathbb{G}_2$ be cyclic prime order groups of order p, where $\mathbb{G}_1$ is an additive group and $\mathbb{G}_2$ is a multiplicative group. Let $P, Q \in_R \mathbb{G}_1$ be the elements of $\mathbb{G}_1$, and $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be a bilinear map. PKG chooses $s \in_R \mathbb{Z}_p$ and computes the public key $P_{pub} = sP$. PKG also sets $\alpha = \hat{e}(P,Q)$, $\alpha_1 = \hat{e}(P,Q)^s$. Additionally, PKG chooses random values $u_0, u_1 ....u_k \in \mathbb{G}_1$ and picks two cryptographic hash functions $H_1(.)$, and $H_2(.)$ defined by,

$$H_1\text{: } \{0,1\}^n \rightarrow \{0,1\}^k, \text{ and } H_2\text{: } \mathbb{G}_2 \rightarrow \{0,1\}^n$$

Here k is a number typically of size 128 bits, to ensure collision resistance against birthday attacks. And n is the size of identity. The system parameters *params* are $\langle \mathbb{G}_1, \mathbb{G}_2, P, Q, p, \hat{e}, H_1, H_2, P_{pub}, \alpha, \alpha_1, u_0, u_1 .....u_k \rangle$. The master private key is $\langle s \rangle$.

Key Extract. Given the master private key s, and the user identity $ID_A \in \{0,1\}^n$, the algorithm does the following:

1. Computes $q_A = H_1(ID_A) \in \{0,1\}^k$. Here, q_A represents a k-bit number. Let $q_A[i]$ represent the i^{th} bit of q_A.
2. Chooses random $r_A, \bar{r}_A \in \mathbb{Z}_p$.
3. Sets $d_A = sq_A + r_A \in \mathbb{Z}_p$.
4. Sets $Y_A = \bar{r}_A P \in \mathbb{G}_1$.
5. Sets $X_A = r_A Q + \bar{r}_A(u_o + \sum_{i=1}^{k} q_A[i]u_i) \in \mathbb{G}_1$.
6. Outputs the private key of the user as $D_A = \langle d_A, Y_A, X_A \rangle$.

Note. The Key Extract algorithm is a probabilistic polynomial time (PPT) algorithm. However, this algorithm can be made deterministic by generating the random coins $r_A, \bar{r}_A$ through a pseudo random function with the identity and the master private key as the seeds (Pornin, 2012).

Encryption. On input of a message $m \in \mathcal{M}$ and identity $ID_A \in \{0,1\}^n$, the encrypt algorithm works as follows:

- Chooses $r \in_R \mathbb{Z}_p$.
- Computes c_1= rP and $\beta = \alpha_1^{rq_A}$.
- Computes $c_2 = r(u_o + \sum_{i=1}^{k} q_A[i]u_i)$.
- Computes $c_3 = H_2(\beta) \oplus m$.
- Outputs the ciphertext $C = \langle c_1, c_2, c_3 \rangle$.

Decryption. Let $C = \langle c_1, c_2, c_3 \rangle$ be a valid encryption of m under the identity ID_A. Then C can be decrypted using the private key D_A as follows:

1. Compute $\beta' = \hat{e}(c_1, d_A Q - X_A)\,\hat{e}(Y_A, c_2)$.

2. Compute $m = H_2\left(\beta'\right) \oplus c_3$.

Correctness: It can be shown that $\beta' = \beta$ as follows:

$$
\begin{aligned}
\beta &= \alpha_1^{rq_A} \\
\beta' &= \hat{e}(c_1, d_A Q - X_A)\,\hat{e}(Y_A, c_2) \\
&= \hat{e}(c_1, d_A Q)\,\hat{e}(c_1, -X_A)\,\hat{e}(\bar{r}_A P, r(u_0 + \sum_{i=1}^{k} q_A[i]u_i)) \\
&= \hat{e}\,(rP, (sq_A + r_A)Q)\;\hat{e}(rP, r_A Q + \bar{r}_A(u_0 + \sum_{i=1}^{k} q_A[i]u_i))^{-1} \\
&\quad\ \hat{e}(\bar{r}_A P, r(u_0 + \sum_{i=1}^{k} q_A[i]u_i)) \\
&= \hat{e}(rP, sq_A Q)\hat{e}(rP, r_A Q)\,\hat{e}(rP, r_A Q)^{-1} \\
&\quad\ \hat{e}(rP, \bar{r}_A(u_0 + \sum_{i=1}^{k} q_A[i]u_i))^{-1} \\
&\quad\ \hat{e}(\bar{r}_A P, r(u_0 + \sum_{i=1}^{k} q_A[i]u_i)) \\
&= \hat{e}(P, Q)^{srq_A} \\
&= \alpha_1^{rq_A} = \beta
\end{aligned}
$$

Theorem 2. If there exists an IND-CPA adversary for our scheme Γ with a non-negligible probability then it is possible to construct another algorithm which can solve the Computational Bilinear Diffie-Hellman problem (CBDHP) with almost the same probability.

5 IND-CCA SECURE SCHEME

We apply the Fujisaki Okamoto Transformation (Fujisaki and Okamoto, 2013) to convert the IND-CPA secure Γ scheme of the previous section into an adaptive chosen ciphertext secure ID-based scheme in the random oracle model. We obtain the following IBE scheme which we call the Γ' scheme.

5.1 The Scheme $\left(\Gamma' - scheme\right)$

Setup : The Setup is similar to Γ scheme. In addition, we pick a hash function $H_3(.)$ defined as, $H_3 : \{0,1\}^n \times \{0,1\}^\rho \to \mathbb{Z}_p$. And, redefine the hash function $H_2(.)$, as $H_2 : \mathbb{G}_2 \to \{0,1\}^{n+\rho}$. Remember that ρ is a number typically of size 128 bits.

Key Extract. As in Γ scheme.

Encryption. On input of a message $m \in \{0,1\}^n$ and identity ID_A, the encrypt algorithm works as follows:

- Chooses $\omega \in \{0,1\}^\rho$ and computes $r = H_3(m||\omega) \in \mathbb{Z}_p$.
- Computes $c_1 = rP \in \mathbb{G}_1$ and $\beta = \alpha_1^{rq_A}$.
- Computes $c_2 = r(u_o + \sum_{i=1}^{k} q_A[i]u_i) \in \mathbb{G}_1$.
- Computes $c_3 = H_2(\beta) \oplus (m||\omega)$.
- Output the ciphertext $C = \langle c_1, c_2, c_3 \rangle$.

Decryption. Let $C = \langle c_1, c_2, c_3 \rangle$ be a valid encryption of m under the identity ID_A. Then C can be decrypted by the user as follows:

- Computes $\beta' = \hat{e}(c_1, d_A Q - X_A)\,\hat{e}(Y_A, c_2)$.
- Computes $(m'||\omega') = H_2\left(\beta'\right) \oplus c_3$.
- Compute $r' = H_3(m'||\omega')$.
- Test that $c_1 = r'P$ and $c_2 = r'(u_0 + \sum_{i=1}^{k} q_A[i]u_i)$.

If the above two tests hold, output m' as the decryption of C.

Correctness: It can be easily shown that $m' = m$ since $\beta' = \beta$. The proof of correctness follows from that of Γ scheme.

Remark. Let Γ be an IND-CPA secure ID-based encryption scheme. Then after applying Fujisaki Okamoto transformation (Fujisaki and Okamoto, 2013) to Γ, we get an IND-CCA secure ID-based encryption scheme Γ' under the same assumption that CBDH is hard to solve in $(\mathbb{G}_1, \mathbb{G}_2)$. This statement follows from the proof of standard transformation due to Fujisaki Okamoto for converting an IND-CPA secure scheme to IND-CCA secure scheme.

6 CONCLUSION

In this paper, we have designed a novel identity based encryption scheme in random oracle model which reduces to the well known CBDH problem. Our scheme differs from all existing schemes because it does not use full domain hash and it does not employ pairing computation during encryption process, thus making it more efficient. In order to achieve these properties, we have proposed a novel PKI based signature scheme, which is used to extract the private key of the identity based encryption scheme. We have first proved the security of our scheme in CPA security notion, and then using Fujisaki Okamoto transformation we have proposed the CCA secure version of our scheme. Ours is the only scheme which does not use bilinear pairing during encryption without compromising on security. Our scheme is proven secure under the well known CBDH problem.

REFERENCES

Agrawal, S., Boneh, D., and Boyen, X. (2010). Efficient lattice (h)ibe in the standard model. In *Advances in*

Cryptology - EUROCRYPT, volume 6110 of *Lecture Notes in Computer Science*, pages 553–572. Springer.

Attrapadung, N., Furukawa, J., Gomi, T., Hanaoka, G., Imai, H., and Zhang, R. (2007). Efficient identity-based encryption with tight security reduction. *IEICE Transactions*, 90-A(9):1803–1813.

Barreto, P. S. L. M., Libert, B., McCullagh, N., and Quisquater, J.-J. (2005). Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In *Advances in Cryptology - ASIACRYPT*, volume 3788 of *Lecture Notes in Computer Science*, pages 515–532. Springer.

Boneh, D. and Boyen, X. (2011). Efficient selective identity-based encryption without random oracles. *Journal of Cryptology*, Vol 24(No 4):659–693.

Boneh, D. and Franklin, M. K. (2005). Identity-based encryption from the weil pairing. In *Advances in Cryptology - CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer.

Boneh, D., Lynn, B., and Shacham, H. (2004). Short signatures from the weil pairing. *Journal of Cryptology*, Vol 17(No 4):297–319.

Chen, L. and Cheng, Z. (2005). Security proof of sakai-kasahara's identity-based encryption scheme. In *IMA Int. Conf.*, pages 442–459.

Fujisaki, E. and Okamoto, T. (2013). Secure integration of asymmetric and symmetric encryption schemes. *J. Cryptology*, 26(1):80–101.

Galindo, D. and Garcia, F. D. (2009). A schnorr-like lightweight identity-based signature scheme. In *Progress in Cryptology - AFRICACRYPT*, volume 5580 of *Lecture Notes in Computer Science*, pages 135–148. Springer.

Gentry, C. (2006). Practical identity-based encryption without random oracles. In *Advances in Cryptology - EUROCRYPT*, volume 4004 of *Lecture Notes in Computer Science*, pages 445–464. Springer.

Herranz, J. (2006). Deterministic identity-based signatures for partial aggregation. *Comput. J.*, 49(3):322–330.

Islam, S. K. H. and Biswas, G. P. (2012). A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks. *Annales des Télécommunications*, 67(11-12):547–558.

Katz, J. and Wang, N. (2003). Efficiency improvements for signature schemes with tight security reductions. In *ACM Conference on Computer and Communications Security*, pages 155–164.

Kiltz, E. (2006). Chosen-ciphertext secure identity-based encryption in the standard model with short ciphertexts. *IACR Cryptology ePrint Archive*, 2006:122.

Pornin, T. (2012). Deterministic Usage of DSA and ECDSA Digital Signature Algorithms. urlhttp://tools.ietf.org/id/draft-pornin-deterministic-dsa-01.html#rfc.section.3.

Sakai, R. and Kasahara, M. (2003). Id based cryptosystems with pairing on elliptic curve. *IACR Cryptology ePrint Archive*, 2003:54.

Schnorr, C.-P. (1989). Efficient identification and signatures for smart cards. In *Advances in Cryptology - CRYPTO*, volume 435 of *Lecture Notes in Computer Science*, pages 239–252. Springer.

Selvi, S. S. D., Vivek, S. S., and Rangan, C. P. (2011). Identity-based deterministic signature scheme without forking-lemma. In *Advances in Information and Computer Security - IWSEC*, volume 7038 of *Lecture Notes in Computer Science*, pages 79–95. Springer.

Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In *CRYPTO - 84*, Lecture Notes in Computer Science, pages 47–53. Springer.

Waters, B. (2005). Efficient identity-based encryption without random oracles. In *Advances in Cryptology - EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127. Springer.