Journal of Ambient Intelligence and Humanized Computing (2019) 10:1561–1570
https://doi.org/10.1007/s12652-018-0756-9

ORIGINAL RESEARCH

New efficient identity based encryption without pairings

Jingang Liu[1] · **Lishan Ke**[1]

Received: 8 November 2017 / Accepted: 11 March 2018 / Published online: 15 March 2018

Abstract
Identity based encryption (IBE) schemes were first constructed with, and often have been since, bilinear mappings (a.k.a. pairings) on elliptic curves. But the multiply and exponent operation using pairings is slowly and inefficiency in implementation. There were, however, some successful attempts to construct IBE schemes based on more traditional number theoretic problems. Unfortunately, most of the proposed schemes are impractical as a result of bandwidth utilization or the time complexity of performance. By this work, we present a new efficient IBE scheme without pairings, which is inspired from the trapdoor technique rooted in composite residuosity class problem. Firstly, our converted basic IBE scheme is proven, in the random oracle model, secure against chosen-plaintext attacks (CPA) under the assumptions that the decision composite residuosity and decision partial discrete logarithm problems are intractable. Moreover, we employ the technique of Fujisaki–Okamoto to transform the basic scheme into enhanced one for resisting chosen-ciphertext attacks (CCA).

Keywords Identity based encryption · Composite degree residuosity · Provable security · Random oracle

1 Introduction

The idea of Identity based encryption scheme (IBE) was formulated by shamir in the early 1980s. Shamir's original motivation was to simplify certificate management in email systems. The intuitive flexibility and convenience of using an arbitrary string as a public key made many practical applications of IBE quickly apparent. An IBE scheme is an asymmetric system wherein the public key is effectively replaced by a user's publicly available identity information or any arbitrary string which derived from the user's identity. It enables any pair of users to communicate securely without exchanging public or private keys and without keeping any key directories. The service of a third party which we called private key generator (PKG) is needed whose sole purpose is to generate private key for the user. The private key is computed using the PKG's master-key and the identity of the user, and it's very useful in the field of cloud computing Shen et al. 2015; Wang et al. 2017b; Xu et al. 2018.

✉ Jingang Liu
xy07liu@126.com

Lishan Ke
keyao1986@163.com

[1] School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, People's Republic of China

Since the presentation of the idea from Shamir, several IBE schemes have emerged in the literature, based on various hard problems, for example in Desmedt and Quisquater 1986; Tanaka 1987. Unfortunately, most of the proposed schemes are impractical or insecure. However, it was not until 2001 that the Boneh–Franklin scheme Boneh and Franklin 2001 introduced the first working IBE system building on the progress in elliptic curves with bilinear pairings. Its publication was quickly gave rise to a number of follow-up works Waters 2005; Canetti et al. 2007; Li et al. 2015; Pan et al. 2016. Specifically, the system is based on bilinear maps between groups realized through the Weil pairing or Tate pairing, while the computational cost of the multiply and exponent operation using pairing is slowly and inefficiency in implementation.

Soon after the Boneh–Franklin scheme, a totally different approach was put forward by Cocks (2001) who introduced an elegant IBE scheme based on the standard quadratic residuosity (QR) problem. Cocks IBE scheme only requires elementary mathematics, encryption merely involves a couple of operations modulo an RSA modulus and the evaluation of Jacobi symbols. Its security rests on the standard quadratic residuosity assumption in the random oracle model. Cocks IBE, however, encrypts the message bit by bit and thus it is considered very bandwidth consuming. Despite its simplicity, Cocks' scheme received less attention

from the research community, compared to the pairing-based constructions.

1.1 Related works

A long standing open problem since Cocks (2001) is the construction of a space efficient IBE system without pairings. From efficiency considerations, and that motivates us to find alternative constructions.

Since Cocks' pioneering work, there has been a flurry of variants, aiming at dealing with the issue of bandwidth or offering extra properties. At FOCS'07, Boneh et al. (2007) made the first successful attempt to propose a space-efficient IBE scheme relied on the theory of ternary quadratic forms. Both use a RSA composite and while the Cocks scheme utilizes this concept in a bitwise encryption algorithm which encrypts each bit individually, thus expanding an ℓ-bit plaintext to a ciphertext of size $2\ell \log_2 N$, the latter scheme would only expand it to about a size of $\ell + \log_2 N$. Unfortunately, this scheme has short ciphertexts but rather large private keys, and both the encryption and decryption algorithms require non-trivial computational effort, observably slower than the Cocks system.

Subsequently, Cocks' cryptosystem was extended by Boneh et al. (2013) with multiple bit encryption. This scheme was shown to be secure under a modified higher power residuosity assumption (which generalizes the quadratic residuosity assumption). As explained in Boneh et al. 2013, these schemes are however less efficient, bandwidth-wise, than the original Cocks scheme. While it is currently inefficient, it shows that a generalization is possible, which may be able to be made efficient in the future.

Note that in 2009, Paterson and Srinivasan also proposed an IBE scheme from another direction, based on factorization assumption and discrete logarithm related assumptions simultaneously. It is reasonable both in space and in time-consuming, but the private key extracting algorithm is inefficient. Moreover, Meshram (2015) made a further improvement on the same intractable assumption, Thus, the scheme is in practice limited to the number of private key extraction queries. Other generalizations and extensions of the Cocks IBE scheme can be found in Ateniese and Gasti 2009; Clear et al. 2014.That is worth mentioning, an entirely different approach to IBE, based on lattices, was introduced by Gentry et al. (2008). Their IBE scheme enjoys efficient encryption and decryption, but has large public parameters and private keys. It also remains to be seen how parameters should be selected in practice for this scheme in order to attain a given level of security. Very recently, Döttling and Garg (2017) gave a beautiful construction of IBE using new primitives called chameleon encryption or one-time signatures with encryption.

1.2 Our contributions

In this study, we deal with the problem of constructing an IBE scheme without pairings, from Paillier's original scheme based on composite residuosity problem Paillier 1999, which is efficient and practical while meets a strong security requirement. Then we transform the basic scheme into enhanced one by applying the technique in Fujisaki and Okamoto 1999 to design a mediated IBE scheme secure against more powerful attacks (CCA). It should be noted that, our basic scheme is additively homomorphic and anonymous. In particular, it can now be used in applications where computing over ciphertexts is required. Typical applications include electronic voting, auction systems, private information retrieval, or cloud computing Liu et al. 2015; Chen et al. 2016; Wang et al. 2017a.

1.3 Outline of the paper

The rest of this paper is organized as follows: Some preliminaries such as basic facts, definitions and security models are given in next section. In Sect. 3, we present our proposed new efficient identity-based encryption scheme. Section 4 gives the security analysis as well as security proof. In Sect. 5, the enhanced scheme against chosen-ciphertext attacks is presented. The comparison of the previous ralated scheme is discussed in Sect. 6. Finally, some concluding remarks are made in Sect. 7.

2 Preliminaries

The Paillier encryption scheme Paillier 1999 is a probabilistic public key algorithm. The problem of computing N-th residue classes is believed to be computationally difficult. The decisional composite residuosity assumption is the intractability hypothesis upon which this cryptosystem is based.

In this section, we briefly describe some useful background knowledge. We first review the mathematical primitive that plays on central role in the previous scheme.

2.1 Definitions and notations

Let N be a positive integer, we write $\mathbb{Z}_N$ for the ring of residue classes modulo N, and $\mathbb{Z}_N^*$ for its multiplicative group. As usual, we say that a function f from the natural numbers to the non-negative real numbers is negligible if for every positive polynomial there is an N such that for all integers $n > N$ it holds that $f(n) < 1/poly(n)$. We typically denote an arbitrary negligible function by $negl(n)$. The probabilistic polynomial time is abbreviated as PPT.

2.2 Paillier encryption scheme

Let $N = pq$ be a safe-prime modulus, i.e. p and q are large primes of the form $p = 2p' + 1$ and $q = 2q' + 1$, where p' and q' are also different primes. We will denote by $\varphi(N)$ Euler's totient function and by $\lambda(N)$ Carmichael's function on N, i.e. $\varphi(N) = (p-1)(q-1)$ and $\lambda(N) = lcm(p-1, q-1)$, respectively. From now, we adopt λ instead of $\lambda(N)$ for visual comfort. And that $gcd(p-1, q-1) = 2$, which yields $\varphi(N) = 2\lambda$. Let $N = pq$ be a modulus chosen as above and $g \in \mathbb{Z}^*_{N^2}$. It is shown that the integer-valued function ε_g defined as follows:

$$\mathbb{Z}_N \times \mathbb{Z}^*_N \longrightarrow \mathbb{Z}^*_{N^2}$$

with

$$\varepsilon_g(x, y) = g^x y^N \pmod{N^2}$$

is a bijection if $ord(g) = \alpha N$, where $\alpha \geq 1$. Then given $\forall \omega \in \mathbb{Z}^*_{N^2}$, the unique $x \in \mathbb{Z}_N$ for which there exists some $y \in \mathbb{Z}^*_N$ such that $\omega = \varepsilon_g(x, y)$ is called the N-residuosity class of ω relative to g, denoted by g. Accordingly, the message is recovered by means of computing

$$m = \frac{L(c^\lambda \ mod \ N^2)}{L(g^\lambda \ mod \ N^2)} \pmod{N}$$

One can observe that the set $\mathbb{S} = \{u < N^2 | u \equiv 1 \pmod{N}\}$, over which the function L such that $\forall u \in \mathbb{S}$, $L(x) = \frac{x-1}{N}$ is clearly well-defined.

Lemma 1 *The Carmichael's theorem implies that* $\forall g \in \mathbb{Z}^*_{N^2}$, *we have*

$$\begin{cases} g^\lambda \equiv 1 & (\mathrm{mod}\, N) \\ g^{N\cdot\lambda} \equiv 1 & (\mathrm{mod}\, N^2) \end{cases} \tag{1}$$

Proof Since $\varphi(p) = (p-1)$, $\varphi(q) = (q-1)$. $gcd(p-1, q-1) = 2$ as well as $\varphi(N) = 2\lambda$, which yelds $\varphi(p), \varphi(q) | \lambda$. So we have

$$\begin{cases} g^\lambda \equiv 1 \pmod{p} \\ g^\lambda \equiv 1 \pmod{q} \end{cases}$$

From Chinese Remainder Theorem, implies $g^\lambda \equiv 1 \pmod{N}$. Futhermore, Carmichael function $\lambda(N^2) = N \cdot \lambda$, hence

$$g^{N\cdot\lambda} \equiv 1 \pmod{N^2}$$

□

2.3 Identity-based encryption model

A general study of the definition and security model of Identity Based Encryption has been driven from Boneh and Franklin (2001), we therefore refer the reader to this paper for more detail, concluding with a complete hierarchy.

3 A new identity-based encryption scheme

Motivated by Paillier 1999; Cramer and Shoup 2002; Bresson et al. 2003, we construct a new efficient IBE scheme without pairings.

For decreasing the decryption complexity, the ciphertext space was restricted to subgroup $\langle g \rangle$ of $\mathbb{Z}^*_{N^2}$ in the original Paillier scheme (see Paillier (1999), section 6). Accordingly, we define $\mathbb{G} = \{x \in \mathbb{Z}^*_{N^2} \ | x \equiv y^2 \ mod N^2, \exists y \in \mathbb{Z}_{N^2}\}$ is the cyclic subgroup of quadratic residues modulo N^2. For the order of group $\mathbb{G}$, denotes $ord(\mathbb{G})$, so we have

$$ord(\mathbb{G}) = \frac{\varphi(N^2)}{4} = \frac{N \cdot \varphi(N)}{4} = \frac{N \cdot \lambda}{2} \tag{2}$$

If one denotes by ν the inverse of 2 modulo N, according to Lemma 1, it can get the following corollaries:

Corollary 1 *In the cyclic group* $\mathbb{Z}^*_{N^2}$, *every element of order N, can be rewritten as the form* $\alpha = (1 + kN)$, *where* $k \in \{1, 2, \cdots, N\}$.

Corollary 2 *The elements of order N in* $\mathbb{Z}^*_{N^2}$, *also belong to the cyclic subgroup of quadratic residues modulo* N^2, i.e. $\alpha \in \mathbb{G}$ *which is* $2\nu \equiv 1 \bmod N$

$$\alpha = 1 + kN = (1 + \nu kN)^2 \pmod{N^2}$$

Corollary 3 *For every element* $s \in \mathbb{G}$, *there exists* $\varepsilon \in \mathbb{Z}_{\mathbb{N}}$, *i.e.*

$$s^{\frac{\lambda}{2}} = \left(1 + \varepsilon \cdot N\right) \pmod{N^2}$$

Proof Note that, from eq. 2, $ord(\mathbb{G}) = \frac{N\cdot\lambda}{2}$, in the cyclic group $\mathbb{G}$ we have

$$s^{\frac{\lambda\cdot N}{2}} = 1 \pmod{N^2}$$

that is

$$(s^{\frac{\lambda}{2}})^N = 1 \pmod{N^2}$$

with eq. 1, there exists $\varepsilon \in \mathbb{Z}_{\mathbb{N}}$, i.e.

$$s^{\frac{\lambda}{2}} = \left(1 + \varepsilon \cdot N\right) \pmod{N^2}$$

□

3.1 The intractable problems over $\mathbb{Z}^*_{N^2}$

In this subsection, we will follow the presentation of Paillier (1999). It defined the *Partial Discrete Logarithm*, abbreviated as *PDL*. Given g and $h \equiv g^x \bmod N^2$, computing x is infeasible.

Assumption 1 (PDL) For any probabilistic polynomial time algorithm $\mathcal{A}$, there exists a negligible function negl(n) such that

$$Adv^{PDL}_{\mathcal{A}} = Pr\left[(\mathcal{A}(g,h,N=x) \wedge (h \equiv g^x \bmod N^2)\right] \leq negl(n)$$

Assumption 2 (DDH) Given $N = pq$, $X = g^x \bmod N^2$, $Y = g^y \bmod N^2$ and $Z = g^z \bmod N^2$, to decide whether $z = xy \bmod (ord(\mathbb{G}))$ or not. For any probabilistic polynomial time algorithm $\mathcal{A}$, there exists a negligible function negl(n) such that

$$Adv^{DDH}_{\mathcal{A}} = \Big|Pr[\mathcal{A}(N,g,X,Y,g^{xy}) = 1] - Pr[\mathcal{A}(N,g,X,Y,Z) = 1]\Big| \leq negl(n)$$

For modulo N^2, it can be compute $Z(\bmod N)$ in line with $Z(\bmod N^2)$, similarly with the well known *CDH* problem, the *Modified computatial Diffie–Hellman* problem, denotes *MDH* assumption.

Assumption 3 (MDH) Given $N = pq$, $X = g^x \bmod N^2$, $Y = g^y \bmod N^2$ and $z = g^{xy} \bmod N$, to compute $Z = g^{xy} \bmod N^2$. For any probabilistic polynomial time algorithm $\mathcal{A}$, there exists a negligible function negl(n) such that

$$Adv^{MDH}_{\mathcal{A}} = Pr\left[\mathcal{A}(N,g,X,Y,z \bmod N) = Z \bmod N^2\right] \leq negl(n)$$

With the following theorem we make explicit the relation existing between the *PDL* problem and *MDH* problem.

Theorem 1 *If the PDL assumption is tenable then so is the MDH assumption.*

Proof Assume that the *MDH* problem can be easily solved, there exists a probabilistic polynomial time algorithm $\mathcal{B}$ requre the result $Z = g^{xy} (\bmod N^2)$, where it is given as input a random *MDH* three-tuple (X, Y, z). Then we can construct an *PPT* algorithm $\mathcal{A}$ that attempts to solve *PDL* problem using algorithm $\mathcal{B}$ as a subroutine.

Consider the *PDL* problem, that is given as input a value $h \equiv g^x (\bmod N^2)$ and tries to compute x. Since $x \in \left[1, ord(\mathbb{G})\right]$, there exists $x_1, x_2 \in \mathbb{Z}_N$, i.e. $x = x_1 + x_2 N$. That is to say, $\mathcal{A}$ try to find x_1, x_2 with $h \equiv g^{x_1 + x_2 N} (\bmod N^2)$.

For convenience, let g is a generator of cyclic group $\mathbb{G}$, then $ord(g) = \frac{N \cdot \lambda}{2}$. So a quadratic residue $c \in \mathbb{G}$ can be generated by g, there is $r_1 \in \mathbb{Z}_\lambda$ as well as $r_2 \in \mathbb{Z}_N$ that the equality $c \equiv g^{r_1 + \lambda r_2} (\bmod N^2)$ holds. Therefore

$$ord\left(g^\lambda\right) = \frac{ord(g)}{\left(\lambda, ord(g)\right)} = \frac{\frac{\lambda \cdot N}{2}}{\left(\lambda, \frac{\lambda \cdot N}{2}\right)} = N$$

Recall the Corollary 3, let $\varepsilon = 1$, we have

$$g^\lambda = (1 + N) \pmod{N^2}$$

The algorithm $\mathcal{A}$ call the algorithm $\mathcal{B}$ and make use of any values it outputs. Let $X = h, Y = c$ and $z = X^{r_1} (\bmod N)$, that is (X, Y, z) regard as input instantiation, plugged into algorithm $\mathcal{A}$. Now

$$\begin{aligned} Y &= g^{r_1 + \lambda r_2} = g^{r_1} \cdot g^{\lambda r_2} \\ &= g^{r_1} \cdot (1 + N)^{r_2} \\ &= g^{r_1} \cdot \left(1 + N \cdot r_2\right) \pmod{N^2} \end{aligned}$$

Suppose $t = \varepsilon^{-1} (\bmod N)$, then

$$\begin{aligned} Y &= g^{r_1}\left(1 + \varepsilon\varepsilon^{-1} N r_2\right) \\ &= g^{r_1}\left(1 + \varepsilon t N r_2\right) \\ &= g^{r_1}\left(1 + \varepsilon N\right)^{t r_2} \\ &= g^{\left(r_1 + \frac{\lambda t r_2}{2}\right)} \pmod{N^2} \end{aligned}$$

When $\mathcal{A}$ is given instance (X, Y, z), it can obtain the result Z^* from $\mathcal{B}$,

$$Z^* = g^{\left(x_1 + x_2 N\right)\left(r_1 + \frac{\lambda t r_2}{2}\right)} \pmod{N^2}$$

Since

$$\begin{aligned} &\left(x_1 + x_2 N\right)\left(r_1 + \frac{\lambda t r_2}{2}\right) \\ &= (x_1 + x_2 N) r_1 + \frac{\lambda t x_1 r_2}{2} + \frac{\lambda N t x_2 r_2}{2} \end{aligned}$$

For $ord(g) = \frac{N\lambda}{2}$, therefore

$$
\begin{aligned}
Z^* &= X^{r_1} \cdot \left(g^{\frac{\lambda}{2}}\right)^{tx_1 r_2} \\
&= X^{r_1} \cdot \left(1+\varepsilon N\right)^{tx_1 r_2} \\
&= X^{r_1} \cdot \left(1+x_1 r_2 N\right) \pmod{N^2}
\end{aligned}
$$

It follows that $\frac{Z^*}{X^{r_1}} = \left(1+x_1 r_2 N\right) \pmod{N^2}$.

To sum up, along with N is known, $x_1, x_2, r_2 \in \mathbb{Z}_N$. Hence, algorithm $\mathcal{A}$ can compute x_1, x_2 with non-negligible probability, it shows that the *PPT* algorithm $\mathcal{A}$ can solve *PDL* problem. This would contradict Assumption 1, and thus cannot happen. □

3.2 Description of the proposed scheme

In this section, we proposed an Identity Based Encryption scheme based on intractable *Partial Discrete Logarithm (DLP)* problem and *Modified computatial Diffie–Hellman (MDH)* problem over $\mathbb{Z}^*_{N^2}$. Our basic IBE scheme is defined to be a four-tuple of algorithms, *(Setup, Extract, Encrypt, Decrypt)* are constructed as follows.

1. **Setup:** PKG run the algorithm on input the security parameter 1^κ:
   - It generates the safe-prime modulus $N = pq$, i.e. p and q are large primes of the form $p = 2p' + 1$ and $q = 2q' + 1$.
   - Choose a secure cryptographic hash function $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}^*_{N^2}$.

2. **Extract:** For a given string $ID \in \{0,1\}^*$, the algorithm does:
   - Compute hash function $a = \mathcal{H}(ID)$, let $s = a^2 \pmod{N^2}$.
   - Pick a random $d \in [1, ord(\mathbb{G})]$ and set $h = s^d \pmod{N^2}$.
   - Send the private decrypt key d to user.
   - The public parameters $\{N, \mathcal{H}, h\}$, and keep the msk $\{p, q\}$ secret.

3. **Encrypt:** When sending an encrypted message $m \in \mathbb{Z}_N$ to a user with identity information *ID*,
   - Compute hash function $a = \mathcal{H}(ID)$, let $s = a^2 \pmod{N^2}$.
   - Pick a random $r \in \mathbb{Z}_{N^2}$, send the ciphertext $C = (c_1, c_2)$ where

$$
\begin{aligned}
c_1 &= s^r \pmod{N^2} \\
c_2 &= (1+N)^m \cdot h^r \pmod{N^2}
\end{aligned}
$$

4. **Decrypt:** To decrypt ciphertext $C = (c_1, c_2)$, with decrypt key d the recipient outputs plaintext

$$
m = \frac{\left(c_2 \cdot c_1^{-d} - 1\right) (\mathrm{mod}\ N^2)}{N}
$$

Correctness: Assuming the ciphertext is well-formed for *ID*, according to the Binomial Expansion $(a+b)^n = \sum_{i=0}^{n} C_n^i \cdot a^{n-i} \cdot b^i$, we have

$$
\begin{aligned}
(1+N)^m &= C_m^0 \cdot N^0 + C_m^1 \cdot N^1 + \cdots + C_m^{m-1} \cdot N^{m-1} + C_m^m \cdot N^m \\
&= (1+mN) \pmod{N^2}
\end{aligned}
$$

Then

$$
\begin{aligned}
\frac{\left(c_2 \cdot c_1^{-d} - 1\right) \bmod N^2}{N} &= \frac{(1+N)^m \cdot h^r \cdot (s^r)^{-d} - 1}{N} \\
&= \frac{(1+mN)(s^d)^r (s^r)^{-d} - 1}{N} \\
&= m
\end{aligned}
$$

Hence, it is easy to check that the decryption algorithm correctly recovers the plaintext m.

4 Security analysis

We now ready to study the security of our basic scheme. From Boneh and Franklin 2001, we do consider two security models that will be applied to our scheme. That is ID-OWE security and IND-ID-CPA security, respectively. In the following proving process, the idea is similarly to Boneh and Franklin 2001. Firstly, define a general PKE scheme associated with our scheme. Moreover, we prove that the attack on IBE scheme can be turned into the general PKE scheme. The idea behind the proof is that the adversary conducts private key extraction queries about *ID* do not increase more success advantage on the attack. Finally, our IBE scheme is proven security under reasonable assumption indirectly.

Theorem 2 Our proposed IBE scheme is IND-OWE security under the modified computatial Diffie–Hellman (MDH) assumption.

Motivated by Boneh and Franklin 2001; Huang et al. 2017, we formalize this via a proof by reduction, to prove

this theorem we need to construct a general PKE scheme $\mathcal{S}$ as follows.

Definition 1 (*General PKE*) The general PKE is constructed by $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$.

- KeyGen $\mathcal{K}$ Input security parameter 1^κ, algorithm $\mathcal{K}$ generates the safe-prime modulus $N = pq$, i.e. p and q are large primes of the form $p = 2p' + 1$ and $q = 2q' + 1$. Pick a random $s, d \in \mathbb{Z}_{N^2}$ and set $h = s^d \pmod{N^2}$. The public key is (N, s, h) and the private key is (p, q, d), respectively.
- Encrypt $\mathcal{E}$ Given the message $m \in \mathbb{Z}_N$, pick a random $r \in \mathbb{Z}_{N^2}$, send the ciphertext $C = (c_1, c_2)$ where

$$c_1 = s^r \pmod{N^2}$$
$$c_2 = (1+N)^m \cdot h^r \pmod{N^2}$$

- Decrypt $\mathcal{D}$ The user can decrypt ciphertext $C = (c_1, c_2)$ using the private key d as follows,

$$m = \frac{\left(c_2 \cdot c_1^{-d} - 1\right) (\mathrm{mod}\ N^2)}{N}$$

Lemma 2 *Suppose $\mathcal{B}$ be an ID-OWE adversary that has non-negligible advantage ϵ aganist the proposed IBE scheme. Let the secure cryptographic hash function $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}^*_{N^2}$ be an random oracle, and $\mathcal{B}$ makes at most q_E private key extraction queries. Then there exists a PPT adversary $\mathcal{A}$ succeeds in breaking the scheme $\mathcal{S}$ with at least $\left(1 - \frac{{q_E}^2}{N(p-1)(q-1)}\right) \cdot \frac{\epsilon}{q_E}$ probability.*

Proof Firstly, the challenger runs the system parameters about general PKE scheme $\mathcal{S}$, where the public key is (N, s, h) and the private key is (p, q, d), respectively. Pick a random message m, to generate the ciphertext $C = (c_1, c_2)$.

Given adversary $\mathcal{A}$ the public key (N, s, h) and the challenge ciphertext $C = (c_1, c_2)$, $\mathcal{A}$ attempts to recover the message m under ciphertext C. Moreover, the adversary $\mathcal{A}$ employs the given parameters to simulate for $\mathcal{B}$ an instance of the IBE scheme and then adversary $\mathcal{A}$ interacts with $\mathcal{B}$ as follows:

$\mathcal{H}$ queries: The adversary $\mathcal{A}$ acts as the simulator, random oracle, to respond to the *ID* queries of adversary $\mathcal{B}$. Suppose $\mathcal{B}$ does not make the same queries. In addition, it has conducted $\mathcal{H}(ID)$ queries before the private key extraction queries for *ID*. To answer the queries, the adversary $\mathcal{A}$ (simulator) creates a list of the queried ID_i and the output result $\mathcal{H}(ID_i)$. If the next queries have already appears on the list, then $\mathcal{A}$ replies with the recorded hash value $\mathcal{H}(ID_i)$, if not, outputs a random value. $\mathcal{A}$ maintains the above list, and the list is initially empty.
Responds: When given the $\mathcal{H}$ queries, the adversary $\mathcal{A}$ randomly chooses $a_i \in Z^*_{N^2}$, return $a_i = \mathcal{H}(ID)$ to the adversary $\mathcal{B}$. And obtain $s_i = a_i^2 \pmod{N^2}$. To respond the private key extraction queries queries, the adversary $\mathcal{A}$ randomly chooses $d_i \in Z^*_{N^2}$, computes $h_i = s_i^{d_i} \pmod{N^2}$.

From the constructions of our IBE scheme and the general PKE scheme $\mathcal{S}$, we observe that h_i is the valid ciphertext as the challenge to the adversary $\mathcal{B}$. With q_E queries and $\left|Z^*_{N^2}\right| = N(p-1)(q-1)$, then the success probability of every query is $1 - \frac{q_E}{N(p-1)(q-1)}$. That is, $\mathcal{B}$ makes q_E queries,

$$\left(1 - \frac{q_E}{N(p-1)(q-1)}\right)^{q_E} \geq \left(1 - \frac{{q_E}^2}{N(p-1)(q-1)}\right)$$

Hence, the probability of the adversary $\mathcal{A}$ succeeds in breaking the scheme $\mathcal{S}$ with at least

$$\left(1 - \frac{{q_E}^2}{N(p-1)(q-1)}\right) \cdot \frac{\epsilon}{q_E}$$

□

The above lemma shows that the ID-OWE security about the proposed basic IBE scheme rely on the OWE security of PKE scheme $\mathcal{S}$. Next, we show that scheme $\mathcal{S}$ is OWE security if the Assumption 3 holds.

Lemma 3 *The general PKE scheme $\mathcal{S}$ is OWE security under the modified computatial Diffie–Hellman (MDH) assumption.*

Proof If the OWE adversary $\mathcal{B}$ succeeds in breaking the scheme $\mathcal{S}$ within probabilistic polynomial time, then the *MDH* problem can be easily solved by adversary $\mathcal{A}$.

Given the instance of *MDH* problem (N, g, X, Y, z), where $N = pq, X = g^x \bmod N^2, Y = g^y \bmod N^2$ and $z = g^{xy} \bmod N$. the goal of $\mathcal{A}$ is to compute $Z = g^{xy} \bmod N^2$. The adversary $\mathcal{A}$ works as follows:

- $\mathcal{A}$ picks a random message m, exploit the given parameters to construct the valid ciphertext $C = (c_1, c_2)$.
- Simulate for $\mathcal{B}$ the public key of scheme $\mathcal{S}$, i.e. the triple (N, s, Y) be.
- Let $c_1 = X, c_2 = z \cdot (1+N)^m \pmod{N^2}$.
- Call the adversary $\mathcal{B}$ for attacking the scheme $\mathcal{S}$, input ciphertext C, obtain the output M.

– $\mathcal{A}$ computes $Z = z \cdot \left(1 + (m - M)N\right) \pmod{N^2}$.

From the construction of scheme $\mathcal{S}$ (Definition 1), we have

$$\begin{aligned} c_2 &= Z\big(1+N\big)^M \\ &= Z + (Z \bmod N)MN \\ &= (Z + zMN) \pmod{N^2} \end{aligned} \tag{3}$$

Moreover, by $\mathcal{C} = (c_1, c_2)$, obviously,

$$\begin{aligned} & z \cdot (1+N)^m \pmod{N^2} \\ &= z\big(1+mN\big) \\ &= (Z + zMN) \pmod{N^2} \end{aligned} \tag{4}$$

From the above two Eqs. (3, 4), the solution for *MDH* problem is

$$Z = z \cdot \left(1 + (m - M)N\right) \pmod{N^2}$$

This would contradict Assumption 3, and this cannot happen. Thus the general PKE scheme $\mathcal{S}$ is OWE security. □

To conclude, by Eqs. 2 and 3, our proposed basic IBE scheme is IND-OWE security under the modified computatial Diffie–Hellman (MDH) assumption, hence Theorem 2 is proved by reduction.

Next, we show that our proposed basic IBE scheme is IND-ID-CPA security.

Theorem 3 *The proposed basic IBE scheme is IND-ID-CPA security if the DDH assumption holds.*

Proof The following is analogous to Theorem 2 and is proved in the same way, i.e. the adversary conducts private key extraction queries about *ID* do not increase more success advantage on the attack. Then we show that scheme $\mathcal{S}$ is IND-CPA security if the Assumption 2 holds.

Concretely, suppose that there is an IND-CPA adversary $\mathcal{B}$ has non-negligible advantage ϵ against the proposed IBE scheme, we can construct a probabilistic polynomial time algorithm $\mathcal{A}$, with help of the adversary $\mathcal{B}$, which can solve the decisional Diffie–Hellman problem (DDH) over $Z^*_{N^2}$.

Given the instance of *DDH* problem quadruple (g, X, Y, Z), where $X = g^x \bmod N^2$, $Y = g^y \bmod N^2$ and $Z = g^z \bmod N^2$. the goal of $\mathcal{A}$ is to decide whether $z = xy \bmod (ord(\mathbb{G}))$ or not. The adversary $\mathcal{A}$ works as follows:

– $\mathcal{A}$ sets the public key (N, s, h), where $h = X = s^x \pmod{N^2}$.
– $\mathcal{A}$ tosses a coin $i \in \{0, 1\}$ randomly and encrypt m_i to return to $\mathcal{B}$.
– $\mathcal{A}$ exploits the given parameters to construct the ciphertext $\mathcal{C} = (c_1, c_2)$.

$$\begin{aligned} c_1 &= s^y \pmod{N^2} \\ c_2 &= (1+N)^{m_i} \cdot s^z \pmod{N^2} \end{aligned}$$

Obviously, if $z = xy \bmod (ord(\mathbb{G}))$, the above ciphertext $\mathcal{C} = (c_1, c_2)$ is valid for m_i, thus the adversary $\mathcal{A}$ can obtain the successful attack from adversary $\mathcal{B}$.

Otherwise, if $z \neq xy \bmod (ord(\mathbb{G}))$, there exists $\gamma \in [1, ord(\mathbb{G})]$ that the formula $z = xy + \gamma$ holds. From $ord(\mathbb{G}) = \dfrac{N \cdot \lambda}{2}$, we infer

$$\gamma = \gamma_1 + \frac{\lambda \cdot \gamma_2}{2}$$

where $\gamma_1, \gamma_2 \in \mathbb{Z}_N$. According to corollary 3

$$\begin{aligned} s^{\frac{\lambda}{2}} &= (1 + \varepsilon N) \pmod{N^2} \\ (1+N)^m &= (1 + mN) \pmod{N^2} \end{aligned}$$

Hence, we have

$$\begin{aligned} c_2 &= (1+N)^{m_i} \cdot s^{xy+\gamma} \\ &= \left(1 + Nm_i\right) \cdot s^{xy} \cdot s^{\gamma_1} \cdot s^{\frac{\lambda \cdot \gamma_2}{2}} \\ &= \left(1 + Nm_i\right) \cdot s^{xy+\gamma_1} \cdot \left(1 + \varepsilon N\right)^{\gamma_2} \\ &= \left(1 + (m_i + \varepsilon\gamma_2)N\right) \pmod{N^2} \end{aligned}$$

For the above formula we observe that m_i is hidden behind $\varepsilon\gamma_2$, hence the adversary is impossible to distinguish between encryptions of messages m_0 and m_1. If not, the adversary can solve the decisional Diffie–Hellman problem (DDH) over $Z^*_{N^2}$. To conclude, the proposed IBE scheme is IND-ID-CPA security if the DDH assumption holds. □

4.1 Properties

In this section, we study the properties of the basic IBE scheme. Concretely, these are called additively homomorphic and anonymity, respectively.

Proposition 1 (Additively Homomorphic) *Observe that, the proposed basic IBE scheme is additively homomorphic, i.e.*

$$Dec\Big(Enc(m_1)\cdot Enc(m_2)\Big) = m_1 + m_2$$

Proof Choose $r_1, r_2 \in \mathbb{Z}_{N^2}$ at random, on input plaintext m_1, m_2, and output the ciphertext C_1, C_2. For $C_1 \cdot C_2$

$$c_1 = s^{r_1+r_2} \pmod{N^2}$$
$$c_2 = (1+N)^{m_1+m_2}\cdot h^{r_1+r_2} \pmod{N^2}$$

therefore

$$\begin{aligned}\frac{\left(c_2\cdot c_1^{-d}-1\right) \bmod N^2}{N} &= \frac{(1+N)^{m_1+m_2}\cdot h^{r_1+r_2}\cdot (s^{r_1+r_2})^{-d}-1}{N}\\ &= \frac{\big(1+(m_1+m_2)N\big)(s^d)^{r_1+r_2}(s^{r_1+r_2})^{-d}-1}{N}\\ &= \frac{1+\big(m_1+m_2\big)N-1}{N}\\ &= m_1+m_2\end{aligned}$$

□

Remark 1 Because of the homomorphic properties, the proposed IBE scheme, however, is malleable and therefore does not protect against adaptive chosen-ciphertext attacks (IND-CCA). Usually in cryptography the notion of malleability is not seen as an advantage, but under certain applications such as secure electronic voting and threshold cryptosystems, this property may indeed be necessary. In the next section, we will present a enhanced IBE scheme with chosen ciphertext security.

Proposition 2 (Anonymity) *The proposed basic IBE scheme is anonymous, that is, the adversary cannot determine the identity under which an encryption is computed.*

The concept of anonymity (key-privacy) was first introduced by Bellare et al. (2001), subsequently, Boneh et al. (2001) extended the notion for Identity Based Encryption.

Notice that the above ciphertext C has two parts, namely

$$c_1 = s^r \pmod{N^2}$$
$$c_2 = (1+N)^m\cdot h^r \pmod{N^2}$$

Obviously, from the *Partial Discrete Logarithm* problem (Assumption 1) is intractable, any adversary cannot distinguish the receiver (i.e. *ID*) of a message, and more precisely, if an adversary who has two keys pk_1, pk_2 can not distinguish with which of these keys the message was encrypted. This property guarantee that the malicious adversaries are unable to acquire the intended recipient's *ID* from the intercepted ciphertext, thus they cannot issue extract queries, i.e. unable to possess the decryption secret key $sk_{ID} = d$.

5 Enhanced cryptosystems

The notion of security against an adaptive chosen-ciphertext attack (IND-CCA) was introduced by Rackoff and Simon (1992) as the property that a cryptosystem must have to resist active adversaries. It has been shown Boneh and Franklin 2001; Boneh and Katz 2005 that the stronger security notion for IBE is indistinguishability against adaptive chosen *ID* and adaptive chosen ciphertext attacks (IND-ID-CCA).

In Fujisaki and Okamoto 1999 Fujisaki–Okamoto (FO) put forward a method to transform a cryptosystem with IND-CPA security into one with IND-CCA security. They used a security hash function which was modeled as a random oracle in the security analysis. Moreover, Boneh and Franklin (2001) had shown such conversion instantiation. Here, we employ the general FO conversion technique to upgrade the basic IBE scheme to a scheme with IND-ID-CCA security.

1. **Setup:** As in the basic IBE scheme state. The only difference is we select a secure cryptographic hash function $\mathcal{H}_1 : \mathbb{Z}_{N^2} \to \{0,1\}^{\ell}\times\{0,1\}^{\kappa}$ additionally, where ℓ is the length of the message to be encrypted.
2. **Extract:** This phase is the same as the basic scheme.
3. **Encrypt:** To encrypt the message $m \in \{0,1\}^{\ell}$ to a user with identity *ID* do the following:
   - Compute hash function $a = \mathcal{H}(ID)$, let $s = a^2 \pmod{N^2}$.
   - Pick a random $\sigma \in \{0,1\}^{\kappa}$, compute $r = \mathcal{H}(m \parallel \sigma)$.
   - Send the ciphertext $C = (c_1, c_2)$ where

     $$c_1 = s^r \pmod{N^2}$$
     $$c_2 = \mathcal{H}_1(h^r \bmod N^2)\oplus(m\parallel\sigma)$$
4. **Decrypt:** To decrypt ciphertext $C = (c_1, c_2)$ using the decrypt key d under *ID*.
   - Compute $(m \parallel \sigma) = c_2 \oplus \mathcal{H}_1(c_1^d \bmod N^2)$.
   - Verify whether $c_1 = s^{\mathcal{H}_1(m\parallel\sigma)} \pmod{N^2}$ and output m if so. Otherwise, reject the ciphertext.

We say that the IND-ID-CCA security proof which is based on Fujisaki and Okamoto 1999 and our basic IBE scheme. Without going into details, we make the following theorem:

Table 1 Comparison of IBE schemes without Pairings

Schemes	KeyGen	Plaintext	Ciphertext	Homomorphic	Anonymity
Cocks (2001)	Yes	{0, 1}	$2\ell \log_2 N$	No	No
BGH (2007)	No	{0, 1}	$\ell + \log_2 N$	No	Yes
BLS (2013)	No	Z_k	$2^{\ell \log_2 N}$	No	Yes
Meshram (2015)	No	Z_N	$2 \log_2 N$	No	No
Our scheme	Yes	Z_N	$4 \log_2 N$	Additively	Yes

Theorem 4 *The proposed enhanced IBE scheme is IND-ID-CCA if the DDH assumption holds.*

6 Comparison

To the best of our knowledge, recent research on the construction of IBE scheme without pairings proceeds in the following main directions: quadratic residuosity problem Cocks 2001; Boneh et al. 2007, higher power residuosity problem Boneh et al. 2013, discrete logarithm problem Paterson and Srinivasan 2009; Meshram 2015. In this section we compare our basic IBE scheme with them.

Firstly, the procedure for key generation is efficient due to the random input, the encryption process requires 2 modular exponetiation and only require 1 in the decryption process. Moreover, the size of ciphertext is acceptable. Finally, our proposed basic IBE scheme have the properties of additively homomorphic and anonymity. The following table shows the comparison result (Table 1).

7 Conclusion

In this paper, we present a new efficient Identity-Based Encryption scheme without pairings, based on composite residuosity related problem, which may impel us to construct IBE scheme from a new direction.

Unfortunately, our scheme is provably secure under the random oracle. There is some doubt concerning the meaning of a proof of security in the random oracle model. As Canetti et al. (2004) shown, there exist cryptosystems that are provably secure in the random oracle, but insecure when the random oracle is instantiated with any hash function. Future work in attempting to modify our scheme which proven security in the stand model may also be an interesting problem. Finally, if we consider the IBE construction of Döttling and Garg (2017), maybe the chameleon function can also be instantiated by our assumption. It is beyond the scope of this paper, yet interested readers are referred to Döttling and Garg 2017 for a detailed description. However, in the current work we have not addressed the problem, and leave it for future.

Acknowledgements The authors would like to thank the anonymous referees for their fruitful comments that improved the presentation of this paper. This work has been partially supported by the Graduate Innovation Foundation of Guangzhou University Project (Project no. 2017GDJC-D04).

References

Ateniese G, Gasti P (2009) Universally anonymous ibe based on the quadratic residuosity assumption. In: Cryptographers' track at the RSA conference, Springer, pp 32–47. https://doi.org/10.1007/978-3-642-00862-7-3

Bellare M, Boldyreva A, Desai A, Pointcheval D (2001) Key-privacy in public-key encryption. In: International conference on the theory and application of cryptology and information security, Springer, pp 566–582. https://doi.org/10.1007/3-540-45682-1-33

Boneh D, Franklin M (2001) Identity-based encryption from the weil pairing. In: Annual international cryptology conference, Springer, pp 213–229. https://doi.org/10.1007/3-540-44647-8-13

Boneh D, Katz J (2005) Improved efficiency for cca-secure cryptosystems built using identity-based encryption. In: Cryptographers' track at the RSA conference, Springer, pp 87–103. https://doi.org/10.1007/2F978-3-540-30574

Boneh D, Di Crescenzo G, Ostrovsky R, Persiano G (2001) Public key encryption with keyword search. In: EUROCRYPT 2004, p 506. https://doi.org/10.1007/978-3-540-24676-3-30

Boneh D, Gentry C, Hamburg M (2007) Space-efficient identity based encryptionwithout pairings. In: 48th annual IEEE symposium on foundations of computer science, 2007, FOCS'07, IEEE, pp 647–657, https://doi.org/10.1109/FOCS.2007.64

Boneh D, LaVigne R, Sabin M (2013) Identity-based encryption with eth residuosity and its incompressibility. In: Autumn 2013 TRUST conference

Bresson E, Catalano D, Pointcheval D (2003) A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications. In: International conference on the theory and application of cryptology and information security, Springer, pp 37–54. https://doi.org/10.1007/978-3-540-40061-5-3

Canetti R, Goldreich O, Halevi S (2004) The random oracle methodology, revisited. J ACM 51(4):557–594. https://doi.org/10.1145/1008731.1008734

Canetti R, Halevi S, Katz J (2007) A forward-secure public-key encryption scheme. J Cryptol 20(3):265–294. https://doi.org/10.1007/s00145-006-0442-5

Chen X, Li J, Weng J, Ma J, Lou W (2016) Verifiable computation over large database with incremental updates. IEEE Trans Comput 65(10):3184–3195. https://doi.org/10.1007/978-3-319-11203-9-9

Clear M, Tewari H, McGoldrick C (2014) Anonymous ibe from quadratic residuosity with improved performance. In: International conference on cryptology in Africa, Springer, pp 377–397. https://doi.org/10.1007/978-3-319-06734-6-23

Cocks C (2001) An identity based encryption scheme based on quadratic residues. In: IMA international conference on cryptography and coding, Springer, pp 360–363. https://doi.org/10.1007/3-540-45325-3-32

Cramer R, Shoup V (2002) Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Advances in cryptology–EUROCRYPT 2002. https://doi.org/10.1007/3-540-46035-7-4

Desmedt Y, Quisquater JJ (1986) Public-key systems based on the difficulty of tampering (is there a difference between des and rsa?). In: Advances in cryptology–CRYPTO'86, Springer, pp 111–117. https://doi.org/10.1007/3-540-47721-7-9

Döttling N, Garg S (2017) Identity-based encryption from the diffie–hellman assumption. In: Annual international cryptology conference, Springer, pp 537–569. https://doi.org/10.1007/978-3-319-63688-7-18

Fujisaki E, Okamoto T (1999) How to enhance the security of public-key encryption at minimum cost. In: International workshop on public key cryptography, Springer, pp 53–68. https://doi.org/10.1007/3-540-49162-7-5

Gentry C, Peikert C, Vaikuntanathan V (2008) Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the fortieth annual ACM symposium on Theory of computing, ACM, pp 197–206. https://doi.org/10.1145/1374376.1374407

Huang Z, Liu S, Mao X, Chen K, Li J (2017) Insight of the protection for data security under selective opening attacks. Inf Sci 412:223–241. https://doi.org/10.1016/j.ins.2017.05.031

Li J, Li J, Chen X, Jia C, Lou W (2015) Identity-based encryption with outsourced revocation in cloud computing. IEEE Trans Comput 64(2):425–437. https://doi.org/10.1109/tc.2013.208

Liu D, Dai Y, Luan T, Yu S et al (2015) Personalized search over encrypted data with efficient and secure updates in mobile clouds. IEEE Trans Emerg Top Comput. https://doi.org/10.1109/TETC.2015.2511457

Meshram C (2015) An efficient id-based cryptographic encryption based on discrete logarithm problem and integer factorization problem. Inf Process Lett 115(2):351–358. https://doi.org/10.1016/j.ipl.2014.10.007

Paillier P (1999) Public-key cryptosystems based on composite degree residuosity classes. In: Advances in cryptology–EUROCRYPT'99, Springer, pp 223–238. https://doi.org/10.1007/3-540-48910-x-16

Pan G, Lei H, Deng Y, Fan L, Yang J, Chen Y, Ding Z (2016) On secrecy performance of miso swipt systems with tas and imperfect csi. IEEE Trans Commun 64(9):3831–3843. https://doi.org/10.1109/eusipco.2016.7760362

Paterson KG, Srinivasan S (2009) On the relations between non-interactive key distribution, identity-based encryption and trapdoor discrete log groups. Des Codes Cryptogr 52(2):219–241. https://doi.org/10.1007/s10623-009-9278-y

Rackoff C, Simon D (1992) Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In: Advances in cryptology–CRYPTO'91, Springer, pp 433–444. https://doi.org/10.1007/3-540-46766-1-35

Shamir A (1985) Identity-based cryptosystems and signature schemes. In: Advances in cryptology, Springer, pp 47–53. https://doi.org/10.1007/3-540-39568-7-5

Shen H, Gao C, He D, Wu L (2015) New biometrics-based authentication scheme for multi-server environment in critical systems. J Ambient Intell Hum Comput 6(6):825–834. https://doi.org/10.1007/s12652-015-0305-8

Tanaka H (1987) A realization scheme for the identity-based cryptosystem. In: Advances in cryptology–CRYPTO'87, Springer, pp 340–349. https://doi.org/10.1007/3-540-48184-2-29

Wang XA, Ma J, Xhafa F, Zhang M, Luo X (2017a) Cost-effective secure e-health cloud system using identity based cryptographic techniques. Future Gener Comput Syst 67:242–254. https://doi.org/10.1016/j.future.2016.08.008

Wang XA, Xhafa F, Ma J, Cao Y, Tang D (2017b) Reusable garbled gates for new fully homomorphic encryption service. Int J Web Grid Serv 13(1):25–48. https://doi.org/10.1504/ijwgs.2017.082061

Waters B (2005) Efficient identity-based encryption without random oracles. In: Advances in cryptology-EUROCRYPT 2005, pp 557–557. https://doi.org/10.1007/11426639-7

Xu J, Wei L, Zhang Y, Wang A, Zhou F, Gao CZ (2018) Dynamic fully homomorphic encryption-based merkle tree for lightweight streaming authenticated data structures. J Netw Comput Appl. https://doi.org/10.1016/j.jnca.2018.01.014