Security of Identity-based Encryption Schemes from Quadratic Residues

Ferucio Laurenţiu Ţiplea, Sorin Iftene, George Teşeleanu, Anca-Maria Nica

Department of Computer Science, "Alexandru Ioan Cuza" University of Iaşi
700506 Iaşi, Romania
e-mail: ferucio.tiplea@uaic.ro, siftene@info.uaic.ro, george.teseleanu@info.uaic.ro, anca.nica@info.uaic.ro

Abstract. The aim of this paper is to provide an overview on the newest results regarding the security of identity-based encryption schemes from quadratic residuosity. It is shown that the only secure schemes are the Cocks and Boneh-Gentry-Hamburg schemes (except of anonymous variations of them).

1 Introduction

Identity-based cryptography (IBC) was proposed in 1984 by Adi Shamir [19] who formulated its basic principles but he was unable to provide a solution to it, except for an identity-based signature (IBS) scheme. A standard scenario on using identity-based encryption (IBE) is as follows. Whenever Alice wants to send a message m to Bob, she encrypts m by using Bob's identity $ID(B)$. In order to decrypt the message received from Alice, Bob asks the Private-Key Generator PKG to deliver him the private key associated to $ID(B)$.

In 2000, Sakai, Ohgishi and Kasahara [17] have proposed an identity-based key agreement (IBKM) scheme, and one year later, Cocks [7] and Boneh and Franklin [5] have proposed the first IBE schemes. Cocks' solution is based on quadratic residues. It encrypts a message bit by bit and requires $2\log n$ bits of cipher-text per bit of plain-text. The scheme is quite fast but its main disadvantage is the ciphertext expansion. The Boneh and Franklin's solution is based on bilinear maps. Moreover, Boneh and Franklin also proposed a formal security model for IBE, and proved that their scheme is secure under the Bilinear Diffie-Hellman (BDH) assumption.

The Cocks IBE scheme attracted the attention of many researchers. Of course, the main question raised by this scheme was about the space efficiency: how to extend it to encrypt arbitrarily large sequences of bits

by reasonable large ciphertexts. A very elegant solution to this question was proposed by Boneh, Gentry, and Hamburg [6]. Unfortunately, their solution suffers from a major deficiency: it makes use of a quartic deterministic time-complexity algorithm to compute solutions to some quadratic bi-variate congruences. Jhanwar and Barua tried to make a step further by proposing an efficient probabilistic algorithm [14] to replace the deterministic one. Unfortunately, their scheme, as well as some other variations, were recently shown insecure.

In this paper we review the newest security results on the IBE schemes based on quadratic residuosity assumption. We thus show that the only secure schemes are the Cocks and Boneh-Gentry-Hamburg schemes (due to space limitation we do not discuss on variations that provide anonymity). Our exposition starts with the Goldwasser-Micalli public-key encryption scheme as a warm-up, advances to the Cocks identity-based encryption scheme, and then to the Boneh-Gentry-Hamburg scheme. Finally, we focus on the insecurity of the Jhanwar-Barua scheme as well as variations of it.

2 Identity-based Encryption

An IBE scheme consists of four probabilistic polynomial-time (PPT) algorithms: *Setup*, *Extract*, *Encrypt*, and *Decrypt*. The first one takes as input a security parameter and outputs the system public parameters together with a master key. The *Extract* algorithm takes as input an identity ID together with the public parameters and the master key and outputs a private key associated to ID. The *Encrypt* algorithm, starting with a message m, an identity ID, and the public parameters, encrypts m into some ciphertext c (the encryption key is ID or some binary string derived from ID). The last algorithm decrypts c into m by using the private key associated to ID.

A natural way to define security models for IBE is to extend the ones for public key encryption (PKE). Recall that for PKE, security models are obtained by combining *security goals* and *attack models*. Three fundamental security goals for PKE are:

1. *indistinguishability* (IND) [13], which means that, given a ciphertext of one of two plaintexts, the adversary is not able to distinguish which of the two messages was encrypted;
2. *semantic security* (SS) [13], which means that the adversary is not able to obtain any information about the plaintext from a given ciphertext;

3. *non-malleability* (NM) [8], which means that, given a ciphertext of a plaintext, the adversary is not able to construct another ciphertext whose plaintext is meaningfully related to the initial one.

The attack models for PKE, considered so far, are:

1. *chosen plaintext attack* (CPA) [13] – under this attack, the adversary can obtain ciphertexts of plaintexts of its choice (in the public key setting, giving the adversary the public key suffices to capture these attacks);
2. *non-adaptive chosen ciphertext attack* (CCA1) [15] – under this attack, the adversary obtains, in addition to the public key, access to a decryption oracle. This oracle can be queried only for the period of time preceding its being given the challenge ciphertext. The term "non-adaptive" refers to the fact that the decryption queries do not depend on the challenge ciphertext;
3. *adaptive chosen ciphertext attack* (CCA2) [16] – under this attack, the adversary gets, in addition to what it gets under the CCA1 attack, access to the decryption oracle after obtaining the challenge ciphertext. The only restriction is that the adversary may not query the oracle for the decryption of the challenge ciphertext. The term "adaptive" refers to the fact that the adversary may adapt its queries after obtaining the challenge ciphertext.

By combining security goals and attack models we obtain nine security models for PKE. For instance, indistinguishability against adaptive chosen ciphertext attack, abbreviated IND-CCA2, is the inability of an adversary to distinguish between two ciphertexts arising out of two equal length messages, although the adversary can adaptively access a decryption oracle. Relationships between these security notions for PKE have been deeply studied [13,3,4,11,20].

The security models for PKE can be adapted to IBE, but some care is needed because in this case a coalition of valid users (of an IBE scheme) can launch an attack against another user (of the same scheme) by pulling together their decryption keys. This aspect is modeled by ensuring the adversary with access to a key-extraction oracle. As for PKE, combining the security goals with the attack models we obtain nine security models for IBE. They are abbreviated by X-ID-Y, where X is a security goal and Y is an attack model. The relationships between these security models are pictorially represented in Figure 2 [1]. As one can see, IND-ID-CCA2 is the strongest security model.

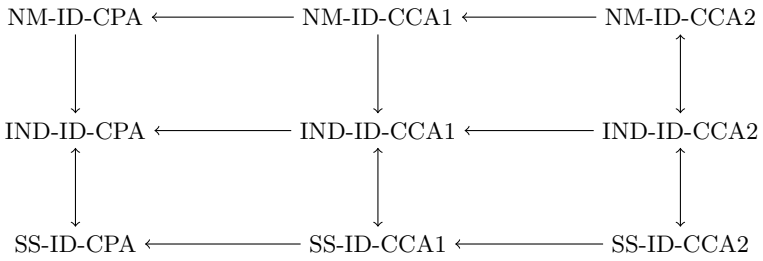

Fig. 1. Relationships between security models for IBE

Recall below the security models IND-IDCCA2 and IND-ID-CPA. For convenience, we will abbreviate IND-ID-CCA2 by IND-ID-CCA. These security models are best explained by means of a game played between the adversary $\mathcal{A}$ and a challenger.

IND-ID-CCA Game

Setup: The challenger takes a security parameter λ and runs $Setup(\lambda)$. It gives the adversary $\mathcal{A}$ the resulting system parameters PP, while keeping the master key msk to itself;

Phase 1: The adversary $\mathcal{A}$ issues a finite number of queries, where each query is of one of the following two forms:

- $Extraction\_query(ID)$: The adversary queries the challenger for the private key corresponding to the identity ID. The challenger runs the *Extract* algorithm to generate the private key corresponding to ID and sends it to $\mathcal{A}$;
- $Decryption\_query(ID, c)$: The adversary queries the challenger to decrypt the ciphertext c with the private key associated to ID. The challenger runs *Extract* to obtain the private key associated to ID and then runs *Decrypt* to decrypt c. Then, it sends the result to $\mathcal{A}$;

These queries may be asked adaptively, that is, each query may depends on the replies to the previous queries;

Challenge: Once the adversary decided that Phase 1 is over, it outputs two equal length plaintexts m_0 and m_1 and an identity ID^* which did not appear in any query in Phase 1 and on which it wishes to be challenged. The challenger picks a random bit $b \in \{0, 1\}$ and computes and sends $c^* = Encrypt(PP, ID^*, m_b)$ as a challenge to the adversary $\mathcal{A}$;

Phase 2: The adversary issues more queries just like in Phase 1, but with the following constraints: each $Extraction\_query(ID)$ must satisfy

$ID \neq ID^*$, and each $Decryption\_query(ID, c)$ must satisfy $(ID, c) \neq (ID^*, c^*)$;

Guess : The adversary outputs a guess $b' \in \{0, 1\}$ and wins the game if $b = b'$.

The *advantage* of an adversary as in the IND-ID-CCA game in attacking an IBE scheme $\mathcal{S}$ is defined as a function on the security parameter λ

$$Adv_{\mathcal{A},\mathcal{S}}(\lambda) = |P(b = b') - 1/2|,$$

where the probability is computed over the random bits used by the challenger and the adversary $\mathcal{A}$. An IBE scheme $\mathcal{S}$ is *IND-ID-CCA secure* if for any PPT adversary $\mathcal{A}$, the function $Adv_{\mathcal{A},\mathcal{S}}(\lambda)$ is negligible.

IND-ID-CPA security is defined similarly to IND-ID-CCA security except for the fact that the IND-ID-CPA game does not contain decryption queries.

3 IBE Schemes Based on Quadratic Residues

The first IBE scheme not using pairings was proposed by Clifford Cocks in December 2001 [7], shortly after Dan Boneh and Matthew Franklin announced their IBE scheme in August 2001 [5] [1]. The Cocks scheme is very elegant and *per se* revolutionary. It is based on the standard quadratic residuosity assumption modulo an RSA composite (in the random oracle model). In order to understand the Cocks' IBE scheme, as well as other IBE schemes based on the quadratic residuosity assumption, it is a good idea to start with the Goldwasser-Micali public key encryption (PKE) scheme [13]. But let us first recall a few concepts and notations on quadratic residues.

The Jacobi symbol of an integer a modulo an integer n is denoted by $\left(\frac{a}{n}\right)$. J_n stands for the set of integers in $\mathbb{Z}_n^*$ whose Jacobi symbol is 1, QR_n denotes the set of quadratic residues in $\mathbb{Z}_n^*$, and $SQRT_n(a)$ is the set of square roots modulo n of a. $\mathbb{Z}_n[x]$ is the ring of polynomials over $\mathbb{Z}_n$. The *QR advantage* of an adversary $\mathcal{A}$ against an RSA generator $RSAgen(\lambda)$ is denoted by $QRAdv_{\mathcal{A},RSAgen}(\lambda)$ (λ is a security parameter). If this advantage is negligible for all adversaries $\mathcal{A}$, we say that the *QR assumption holds for RSAgen*. Given a pseudorandom function (PRF) F, $PRFAdv_{\mathcal{A},F}$ stands for the *PRF advantage of $\mathcal{A}$ against F*. F is *secure* if $PRFAdv_{\mathcal{A},F}$ is negligible for all $\mathcal{A}$.

[1] It was revealed that Clifford Cocks, a mathematician in the United Kingdom's cryptography agency GCHQ, had years earlier devised his IBE scheme, but this was classified by the UK government.

3.1 The Goldwasser-Micali PKE Scheme

The main idea behind the Goldwasser-Micali PKE scheme is the following:

- each bit is viewed as one of the integers -1 or 1 (this can be simply done by encoding $b \in \{0,1\}$ by $(-1)^b$);
- sending the bit 1 is equivalent to sending a quadratic residue $c = r^2$ modulo a Blum integer $n = pq$, while sending the bit -1 is equivalent to sending $c = -r^2 \bmod n$;
- the decryption of c requires to decide whether c is a quadratic residue modulo n. This can efficiently be done if the factorization of n is known; otherwise, it is hard to distinguish between a quadratic residue and a quadratic non-residue (remark that the Jacobi symbol $\left(\frac{c}{n}\right)$ can efficiently be computed and it is always 1 due to the fact that n is a Blum integer).

Goldwasser-Micali PKE scheme [13]

Setup(λ)**:** Generate $(p,q) \leftarrow Blum\_gen(\lambda)$ and compute $n = pq$. Then, output the public key n, while the factorization (p,q) of n is the private key;

Encrypt(m,n)**:** To encrypt a bit $m \in \{-1,1\}$ by the public key n, choose at random $r \in \mathbb{Z}_n^*$ and output the ciphertext $c = r^2 \cdot m \bmod n$;

Decrypt$(c,(p,q))$**:** Return $m = 1$ if $c \in QR_n$, and -1, otherwise. This can efficiently be done by testing whether $\left(\frac{c}{p}\right) = 1$ and $\left(\frac{c}{q}\right) = 1$.

Theorem 1. *[13] The Goldwasser-Micali PKE scheme is IND-CPA secure under the QR assumption for Blum_gen.*

3.2 The Cocks PKE and IBE Schemes

The decryption in the Goldwasser-Micali scheme needs the factorization of n. The scheme below proposed by Cocks [7] is based on a similar idea but the decryption does not depend on the factorization of n. Moreover, n can be an RSA modulus and not necessarily a Blum integer as in the Goldwasser-Micali scheme.

Cocks PKE scheme [7]

Setup(λ)**:** Generate $(p,q) \leftarrow Blum\_gen(\lambda)$ and compute $n = pq$. Choose uniformly at random a private key $r \in \mathbb{Z}_n^*$ and output the public key (n,a), where $a = r^2 \bmod n$;

Encrypt$(m,(n,a))$**:** To encrypt a bit $m \in \{-1,1\}$ by the public key (n,a), choose at random $t \in \mathbb{Z}_n^*$ such that $\left(\frac{t}{n}\right) = m$ and output the ciphertext $c = t + at^{-1} \bmod n$;

Decrypt(c,r)**:** Output $\left(\frac{c+2r}{n}\right)$.

The generation of $t \in \mathbb{Z}_n^*$ with $\left(\frac{t}{n}\right) = m$ can be done by repetition because the probability of success for a random choice of t is $1/2$. The correctness of the Cocks public key encryption scheme simply follows from the congruence

$$c + 2r \equiv_n t(1 + 2rt^{-1} + (rt^{-1})^2) \equiv_n t(1 + rt^{-1})^2$$

which shows that $\left(\frac{c+2r}{n}\right) = \left(\frac{t}{n}\right) = m$.

Theorem 2. *[7] The Cocks PKE scheme is IND-CPA secure under the QR assumption for Blum_gen.*

The Cocks public key encryption scheme can now easily be transformed into an IBE scheme. Let $h : \{0,1\}^* \to J_n$ be a truly random function which maps identities into integers with the Jacoby symbol 1 modulo n. Now, the only subtlety is that we cannot detect whether the output of h is a quadratic residue modulo n or not (recall that the output of h is conceived as a public key). However, it can be easily seen that if $a = h(ID)$ is not a quadratic residue, then $-a$ is (recall that n is a Blum integer and, therefore, -1 is a quadratic non-residue). The solution is then to encrypt a bit $m \in \{-1,1\}$ both by a and $-a$. The private key of the decryptor will be a square root of a, if $a \in QR_n$, or of $-a$, if $-a \in QR_n$.

One may also remark that $-a$ can be replace by any product $e \cdot a \bmod n$ between a public quadratic non-residue e and a. Moreover, in this case n is not required to be a Blum integer. Thus, we arrive at the following general version of the Cocks IBE scheme.

Cocks IBE scheme [7]

Setup(λ)**:** Generate $(p,q) \leftarrow RSAgen(\lambda)$ and compute $n = pq$. Generate uniformly at random $e \in J_n \setminus QR_n$ and output the public parameters $PP = (n,e,h)$, where h is a hash function that maps identities to $J(n)$. The master key is the factorization of n, namely (p,q);

Extract(p,q,ID)**:** Let $a = h(ID)$. If $a \in QR(n)$, set the private key as a random square root r of a; otherwise set the private key as a random square root r of ea;

Encrypt(PP, ID, m)**:** Let $a = h(ID)$. To encrypt a bit $m \in \{-1, 1\}$, randomly choose $t_1, t_2 \in \mathbb{Z}_n^*$ such that $\left(\frac{t_1}{n}\right) = \left(\frac{t_2}{n}\right) = m$. Compute then $c_1 = t_1 + at_1^{-1} \bmod n$ and $c_2 = t_2 + eat_2^{-1} \bmod n$ and output the pair (c_1, c_2) as being the ciphertext associated to m;

Decrypt$((c_1, c_2), r)$**:** Set $c = c_1$ if $r^2 \equiv a \bmod n$, and $c = c_2$, otherwise. Then, $m = \left(\frac{c+2r}{n}\right)$.

The correctness of the Cocks IBE scheme follows in the same way as for the Cocks public key encryption scheme.

Theorem 3. *[7,12] The Cocks IBE scheme is IND-CPA secure in the random oracle model under the QR assumption for RSAgen.*

The Cocks IBE scheme encrypts a message bit by bit, and each bit is encrypted by $2 \log n$ bits, where n is the RSA integer used by the scheme. Therefore, the Cocks IBE scheme can be considered very bandwidth consuming. As Cocks remarked in his paper [7], the scheme can be used in practice to encrypt short session keys in which case it becomes very attractive.

3.3 The Boneh-Gentry-Hamburg IBE Scheme

In the Cocks IBE scheme, t_1 and t_2 are generated such that $\left(\frac{t_1}{n}\right) = \left(\frac{t_2}{n}\right) = m$. Therefore, we may say that t_1 and t_2 encrypt m, and they are transmitted to the recipient in a hidden way: t_1 and t_2 are encapsulated into c_1 and c_2, respectively. One may think to another way of encrypting the bit m. Namely, generate at random $t_1, t_2 \in \mathbb{Z}_n^*$ and encrypt m by (c_1, d_1, c_2, d_2), where $c_1 = m \cdot \left(\frac{t_1}{n}\right)$, $c_2 = m \cdot \left(\frac{t_2}{n}\right)$, $d_1 = t_1 + at_1^{-1} \bmod n$, and $d_2 = t_2 + eat_2^{-1} \bmod n$, where $e \in J_n \setminus QR_n$ is public. The decryption can be simply performed by computing $c_1 \cdot \left(\frac{d_1+2r}{n}\right)$ or $c_2 \cdot \left(\frac{d_2+2r}{n}\right)$, depending on whether a or ea is a quadratic residue modulo n. The scheme obtained in this way is less efficient than the Cocks IBE scheme but, a positive answer to the following question would change things: is there any way to (efficiently) compute, from the public parameters, two pairs of polynomials (f, g) and $(\bar{f}, \bar{g})$ such that the following property holds

$$\left(\frac{g(s)f(r)}{n}\right) = \left(\frac{\bar{g}(s)\bar{f}r}{n}\right) = 1$$

for some s known only by the encryptor and some r known only by the decryptor? If this question would have a positive answer, than one could encrypt the bit m by $(c, \bar{c})$, where $c = m \cdot \left(\frac{g(s)}{n}\right)$ and $\bar{c} = m \cdot \left(\frac{\bar{g}(s)}{n}\right)$. The

decryption would be obtained by multiplying c by $\left(\frac{f(r)}{n}\right)$ or $\bar{c}$ by $\left(\frac{\bar{f}(r)}{n}\right)$ (r would play the role of a private key).

The above idea was exploited by Boneh, Gentry, and Hamburg in [6].

Definition 1. *Let n be a positive integer, $a, S \in \mathbb{Z}_n^*$, and $f, g \in \mathbb{Z}_n[x]$. We say that (f, g) is a pair of* (a, S)-associated polynomials *if the following properties hold:*

1. *if $a, S \in QR_n$, then $f(r)g(s) \in QR_n$, for all $r \in SQRT_n(a)$ and $s \in SQRT_n(S)$;*
2. *if $a \in QR_n$, then $f(r)f(-r)S \in QR_n$, for all $r \in SQRT_n(a)$.*

Roughly speaking, the integer a will play the role of public key, while each $r \in SQRT_n(a)$ will be a private key. The square roots of S are used to randomize the encryption. Thus, the first condition in Definition 1, which is equivalent to $\left(\frac{g(s)}{n}\right) = \left(\frac{f(r)}{n}\right)$, guarantees the correctness of the decryption process: a bit m is encrypted by multiplying it by $\left(\frac{g(s)}{n}\right)$, and the result is decrypted by multiplying the ciphertext by $\left(\frac{f(r)}{n}\right)$. The second condition in Definition 1 is less intuitive: it is necessary to prove security.

The following IBE scheme, called $BasicIBE$, was proposed in [6].

$BasicIBE$ scheme [6]
% In this scheme, $\mathcal{D}$ is an unspecified deterministic algorithm that on
% input (n, a, S) outputs a pair (f, g) of (a, S)-associated polynomials,
% where n is a positive integer and $a, S \in \mathbb{Z}_n^*$.

Setup(λ)**:** Generate $(p, q) \leftarrow RSAgen(\lambda)$, compute $n = pq$, generate $e \in J_n \setminus QR_n$, and choose a hash function $h : \{0,1\}^* \times \{1, \ldots, \ell\} \to J_n$ for some integer $\ell \geq 1$. Output the public parameters $PP = (n, e, h)$; the master key $msk = (p, q, K)$ is the factorization of n together with a random key K of some pseudo-random function $F_K : \{0,1\}^* \times \{1, \ldots, \ell\} \to \{0, 1, 2, 3\}$ (F_K chooses one of the four square roots of $h(ID, i)$ or $eh(ID, i)$, depending on which of them is a quadratic residue);

Extract(msk, ID)**:** For each $j \in \{1, \ldots, \ell\}$, let $a_j = h(ID, j)$ and $i_j = F_K(ID, j)$. If r_0, r_1, r_2, r_3 is a fixed total ordering of the square roots of a_j or ea_j (depending on which of them is a quadratic residue), then the private key is $r = (r_{i_1}, \ldots, r_{i_\ell})$;

Encrypt(PP, ID, m)**:** Assume $m = m_1 \cdots m_\ell \in \{-1, 1\}^\ell$ is the ℓ-bit sequence to be encrypted. The encryption process is as follows:

– Generate at random $s \in \mathbb{Z}_n^*$ and set $S = s^2 \bmod n$;
– For $j := 1$ to ℓ do
  • Compute $a_j = h(ID, j)$;
  • Compute $(f_j, g_j) = \mathcal{D}(n, a_j, S)$ and $(\bar{f}_j, \bar{g}_j) = \mathcal{D}(n, ea_j, S)$;
  • Compute $c_j = m_j \cdot \left(\frac{g_j(s)}{n}\right)$ and $\bar{c}_j = m_j \cdot \left(\frac{\bar{g}_j(s)}{n}\right)$;
– Return $(c, \bar{c}, S)$, where $c = c_1 \cdots c_\ell$ and $\bar{c} = \bar{c}_1 \cdots \bar{c}_\ell$;

Decrypt$((c, \bar{c}, S), r)$**:** The decryption process is as follows:
– For $j := 1$ to ℓ do
  • Compute $a_j = h(ID, j)$;
  • If $a_j \in QR_n$ then $a'_j = a_j$ else $a'_j = ea_j$;
  • Compute $(f'_j, g'_j) = \mathcal{D}(n, a'_j, S)$;
  • Compute $m_j = c_j \cdot \left(\frac{f'_j(r_{i_j})}{n}\right)$;
– Return $m = m_1 \cdots m_\ell$.

The following theorem clarifies the security of the $BasicIBE$ scheme.

Theorem 4. *[6] For any efficient IND-ID-CPA adversary $\mathcal{A}$ attacking the $BasicIBE$ scheme, there exist two efficient algorithms $\mathcal{B}_1$ and $\mathcal{B}_2$, whose running time is about the same as that of $\mathcal{A}$, such that:*

$$IBEAdv_{\mathcal{A},BasicIBE}(\lambda) \leq 2 \cdot QRAdv_{\mathcal{B}_1,RSAgen}(\lambda) + PRFAdv_{\mathcal{B}_2,F}(\lambda),$$

provided that h is modeled as a random oracle, the QR assumption holds for $RSAgen$, and F is a secure pseudo-random function.

We emphasize that the $BasicIBE$ scheme is an abstract IBE scheme because no concrete algorithm $\mathcal{D}$ to compute (a, S)-associated polynomials is presented. In [6], the method proposed to construct such polynomials is based on the congruence $QC_n(a, S)$ given by

$$ax^2 + Sy^2 \equiv 1 \bmod n, \tag{1}$$

where $n = pq$ is an RSA modulus and $a, S \in \mathbb{Z}_n^*$. Any solution (x_0, y_0) to $QC_n(a, S)$ gives rise to two polynomials f and g

$$\begin{aligned} f(r) &= x_0 r + 1 \bmod n \\ g(s) &= 2(y_0 s + 1) \bmod n \end{aligned}$$

that are (a, S)-associated (see [6] for details).

The $BasicIBE$ scheme is more space efficient than the Cocks IBE scheme: ℓ bits are encrypted by $2\ell + \log n$ bits. The time complexity of the $BasicIBE$ scheme depends on the time complexity of the algorithm $\mathcal{D}$. If this implements the method described above, then the encryptor must solve 2ℓ equations of the form $QC_n(a_i, S)$ and $QC_n(ea_i, S)$, for all $1 \leq i \leq \ell$. The decryptor needs to solve only ℓ of these equations.

An improvement at the decryptor side can be obtained starting from the remark that if (x_1, y_1) is a solution to $QC_n(a, S)$ and (x_2, y_2) is a solution to $QC_n(e, S)$, then (x_3, y_3) is a solution to $QC_n(ea, S)$, where $x_3 = \frac{x_1 x_2}{S y_1 y_2 + 1} \bmod n$ and $y_3 = \frac{y_1 + y_2}{S y_1 y_2 + 1} \bmod n$.

Therefore, the encryptor only needs to solve the equations $QC_n(a_i, S)$ for all $1 \leq i \leq \ell$, and the equation $QC_n(e, S)$. This means $\ell + 1$ equations instead of 2ℓ equations.

The algorithm proposed in [6] to find solutions to $QC_n(a, S)$ is quartic in the security parameter, making thus the $BasicIBE$ scheme more expensive than all standard IBE and public key encryption schemes.

3.4 Jhanwar-Barua's IBE Scheme and Other Variations

A significant step in computing solutions to $QC_n(a, S)$ was made by Barua and Jhanwar [14,2] who have established the following characterization result for the solutions in $\mathbb{Z}_n^2$ to the congruence $QC_n(a, S)$.

Theorem 5. *[14,2] Let n be an RSA modulus and $a, S \in \mathbb{Z}_n^*$. The solutions to the congruence $QC_n(a, S)$ satisfy the following properties:*

1. *If $S \in QR_n$ then, for any $s \in SQRT_n(S)$ and any $t \in \mathbb{Z}_n^*$ with $(a + St^2, n) = 1$, the pair (x, y) of integers given by*

$$x = \frac{-2st}{a + St^2} \bmod n \quad \text{and} \quad y = \frac{a - St^2}{s(a + St^2)} \bmod n \tag{2}$$

   is a solution in $\mathbb{Z}_n^* \times \mathbb{Z}_n$ to the congruence $QC_n(a, S)$.
   Moreover, any solution $(x, y) \in \mathbb{Z}_n^* \times \mathbb{Z}_n$ to the congruence $QC_n(a, S)$ is as above, for some $s \in SQRT_n(S)$ and $t \in \mathbb{Z}_n^*$ with $(a + St^2, n) = 1$.
2. *If $a \in QR_n$ then, for any $r \in SQRT_n(a)$ and any $t \in \mathbb{Z}_n^*$ with $(S + at^2, n) = 1$, the pair (x, y) of integers given by*

$$x = \frac{S - at^2}{r(S + at^2)} \bmod n \quad \text{and} \quad y = \frac{-2rt}{S + at^2} \bmod n \tag{3}$$

   is a solution in $\mathbb{Z}_n \times \mathbb{Z}_n^*$ to the congruence $QC_n(a, S)$.
   Moreover, any solution $(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n^*$ to the congruence $QC_n(a, S)$ is as above, for some $r \in SQRT_n(a)$ and $t \in \mathbb{Z}_n^*$ with $(S + at^2, n) = 1$.

Theorem 5 leads to the following simple probabilistic algorithm $\mathcal{Q}(n, a, S)$ to compute solutions to the congruence $QC_n(a, S)$, when $S \in QR_n$ and a square root s of S is known (of course, the algorithm can be correspondingly rephrased for the case when $a \in QR_n$).

Scheme 1 : $\mathcal{Q}(n, a, S)$

Input: n, a, S, and s as above
Output: a solution (x_0, y_0) to $QC_n(a, S)$

1: randomly choose $t \in \mathbb{Z}_n^*$ such that $a + St^2 \in \mathbb{Z}_n^*$;
2: output $x_0 = -2st(a + St^2)^{-1} \bmod n$ and $y_0 = (tx_0 + s^{-1}) \bmod n$.

We emphasize that the probabilistic algorithm $\mathcal{Q}$ described above can not directly be used as an instantiation for the deterministic algorithm $\mathcal{D}$ in the BasicIBE scheme because it does not guarantee a correct decryption. Jhanwar and Barua have used it via a way to combine solutions differently than the one in [6].

Lemma 1. *[14] If $(x_1, y_1) \in \mathbb{Z}_n^2$ is a solution to the congruence $QC_n(a, S_1)$ and $(x_2, y_2) \in \mathbb{Z}_n^2$ is a solution to the congruence $QC_n(a, S_2)$, then $(x_{1,2}, y_{1,2}) \in \mathbb{Z}_n^2$ is a solution to the congruence $QC_n(a, S_1S_2)$, where*

$$x_{1,2} = \frac{x_1 + x_2}{ax_1x_2 + 1} \bmod n \quad \textit{and} \quad y_{1,2} = \frac{y_1y_2}{ax_1x_2 + 1} \bmod n, \tag{4}$$

provided that $(ax_0x_1 + 1, n) = 1$.

Moreover, $x_{1,2} \in \mathbb{Z}_n^*$ if and only if $(x_1 + x_2, n) = 1$.

Now we are able to describe the IBE scheme proposed by Jhanwar and Barua [14]. In this scheme, $\mathcal{Q}(n, a, S)$ is the probabilistic algorithm described above to find solutions to congruences $QC_n(a, S)$).

Jhanwar-Barua IBE (JB_IBE) scheme [14]

Setup(λ)**:** Generate $(p, q) \leftarrow RSAgen(\lambda)$, compute $n = pq$, generate $e \in J_n \setminus QR_n$, and choose a hash function $h : \{0,1\}^* \to J_n$. Output the public parameters $PP = (n, e, h)$; the master key $msk = (p, q, K)$ is the factorization of n together with a random key K of some pseudorandom function $F_K : \{0,1\}^* \to \{0,1,2,3\}$ (F_K chooses one of the four square roots of $h(ID)$ or $eh(ID)$);

Extract(msk, ID)**:** The private key is $r = r_j$, where $j = F_K(ID)$ and r_0, r_1, r_2, r_3 is an ordering of the square roots modulo n of $h(ID)$ or $eh(ID)$, depending on which of them is a quadratic residue modulo n;

Encrypt(PP, ID, m)**:** Assume $m = m_0 \cdots m_{\ell-1}$ is the ℓ-bit sequence to be encrypted. The encryption process is as follows:

- Compute $a = h(ID)$;
- Compute $k = \lceil \sqrt{\ell} \rceil$;
- For $i := 0$ to $k - 1$ do
  - Randomly choose $s_i \in \mathbb{Z}_n^*$ and compute $S_i = s_i^2 \bmod n$;
  - Compute $(x_i, y_i) \leftarrow \mathcal{Q}(n, a, S_i)$ and $(\bar{x}_i, \bar{y}_i) \leftarrow \mathcal{Q}(n, ea, S_i)$;
  - Compute $c_i = m_i \cdot \left(\frac{2s_i y_i + 2}{n}\right)$ and $\bar{c}_i = m_i \cdot \left(\frac{2s_i \bar{y}_i + 2}{n}\right)$;
- For $i := k$ to $\ell - 1$ do
  - Compute $1 \leq \alpha \leq k-1$ and $0 \leq \beta \leq k-1$ such that $i = \alpha \cdot k + \beta$;
  - Use Lemma 1 to compute y_i from (x_α, y_α) and (x_β, y_β), and $\bar{y}_i$ from $(\bar{x}_\alpha, \bar{y}_\alpha)$ and $(\bar{x}_\beta, \bar{y}_\beta)$;
  - Set $s_i = s_\alpha s_\beta \bmod n$;
  - Compute $c_i = m_i \cdot \left(\frac{2s_i y_i + 2}{n}\right)$ and $\bar{c}_i = m_i \cdot \left(\frac{2s_i \bar{y}_i + 2}{n}\right)$;
- Return $(c, \bar{c}, x, \bar{x})$, where $c = c_0 \cdots c_{\ell-1}$, $\bar{c} = \bar{c}_0 \cdots \bar{c}_{\ell-1}$, $x = (x_0, \ldots, x_{k-1})$, and $\bar{x} = (\bar{x}_0, \ldots, \bar{x}_{k-1})$;

Decrypt$((c, \bar{c}, x, \bar{x}), r)$**:** The decryption process is as follows:

- Compute $a = h(ID)$;
- Compute $k = \lceil \sqrt{\ell} \rceil$;
- For $i := 0$ to $k - 1$ do
  - If $a_i \in QR_n$ then $m_i = c_i \cdot \left(\frac{x_i r_j + 1}{n}\right)$ else $m_i = \bar{c}_i \cdot \left(\frac{\bar{x}_i r_j + 1}{n}\right)$;
- For $i := k$ to $\ell - 1$ do
  - Compute $1 \leq \alpha \leq k-1$ and $0 \leq \beta \leq k-1$ such that $i = \alpha \cdot k + \beta$;
  - Use Lemma 1 to compute either x_i from x_α and x_β, or $\bar{x}_i$ from $\bar{x}_\alpha$ and $\bar{x}_\beta$, depending on weather a or ea is a quadratic residue;
  - If $a_i \in QR_n$ then $m_i = c_i \cdot \left(\frac{x_i r_j + 1}{n}\right)$ else $m_i = \bar{c}_i \cdot \left(\frac{\bar{x}_i r_j + 1}{n}\right)$;
- Return $m = m_0 \cdots m_{\ell-1}$.

The soundness of JB_IBE scheme follows easily from how associated polynomials can be computed from solutions to congruences $QC_n(a, S)$ and from Lemma 1.

As one can see, in the JB_IBE scheme the encryptor needs to solve $2k$ congruences, where $k = \lceil\sqrt{\ell}\rceil$, while the decryptor solves none. The ciphertext length is $2\ell + 2k \log n$ bits for a plaintext of ℓ bits.

Regarding the security of the JB_IBE scheme, it was argued in [14] that the scheme is IND-ID-CPA secure. More precisely, it was shown the following.

Theorem 6. *[14] For any efficient IND-ID-CPA adversary $\mathcal{A}$ against the JB_IBE scheme there exist efficient algorithms $\mathcal{B}_1$ and $\mathcal{B}_2$, whose running time is about the same as that of $\mathcal{A}$, such that*

$$IBEAdv_{\mathcal{A},JB\_IBE}(\lambda) \leq PRFAdv_{\mathcal{B}_1,F}(\lambda) + 2 \cdot QRAdv_{\mathcal{B}_2,RSAgen}(\lambda) + \frac{1}{2^k},$$

provided that h is modeled as a random oracle, the QR assumption holds for $RSAgen$, and F is a secure pseudo-random function.

Unfortunately, the JB_IBE scheme is totally insecure. The first security flaw was remarked in [9] and it can simply described as follows. If $i = \alpha \cdot k + \beta$ and $j = \beta \cdot k + \alpha$, then $y_i = y_j$ (according to Lemma 1). Therefore, the bits m_i and m_j are encrypted by using the same Jacobi symbol. This allows an adversary to easily win the IND-ID-CPA security game (in the challenge phase, the adversary chooses two messages m^0 and m^1 such that m^0 has identical bits on the positions i and j, while m^1 has different bits on these positions). This security flaw can be overcame if we choose k larger than $\lceil\sqrt{\ell}\rceil$ and we combine (x_i, y_i) with (x_j, y_j) only for $i \leq j$ [9]. In fact, k should be the least integer satisfying $\frac{k(k+3)}{2} \geq \ell$.

Although we correct the JB_IBE scheme as above, the JB_IBE scheme is still insecure because from $x_0, \ldots, x_{k-1}$ one can compute $\left(\frac{2s_iy_i+2}{n}\right)$ for all i [18]. Indeed, let (x_1, y_1) be a solution to $QC_n(a, S_1)$ and (x_2, y_2) be a solution to $QC_n(a, S_2)$. By Lemma 1, $(x_{1,2}, y_{1,2})$ is a solution to $QC_n(a, S_1S_2)$, where $x_{1,2}$ and $y_{1,2}$ are as in the lemma. Then, if $a \in QR_n$ and $r \in SQRT_n(a)$ we obtain

$$(x_1r + 1)(x_2r + 1) \equiv_n ax_1x_2 + 1 + r(x_1 + x_2) \equiv_n (ax_1x_2 + 1)(x_{1,2}r + 1)$$

which leads to

$$\left(\frac{x_{1,2}r + 1}{n}\right) = \left(\frac{x_1r + 1}{n}\right)\left(\frac{x_2r + 1}{n}\right)\left(\frac{ax_1x_2 + 1}{n}\right) \tag{5}$$

Moreover, if $S_1, S_2 \in QR_n$, $s_1 \in SQRT_n(S_1)$, and $s_2 \in SQRT_n(S_2)$ we also have

$$\left(\frac{2s_1s_2y_{1,2} + 2}{n}\right) = \left(\frac{2s_1y_1 + 2}{n}\right)\left(\frac{2s_2y_2 + 2}{n}\right)\left(\frac{ax_1x_2 + 1}{n}\right) \tag{6}$$

no matter a is a quadratic residue or not (see [18] for more details).

Now, it is straightforward to show that the JB_IBE scheme is not IND-ID-CPA.

In [9], Elashry, Mu, and Susilo tried to improve the upper bound in Theorem 6 by dropping the factor $1/2^k$ by using Damgard's assumption. This assumption says that it is hard to predict the Jacobi symbol of the next integer of a polynomial length sequence of consecutive integers. More precisely, given a λ-bit RSA modulus n and an integer a, it is hard to predict $\left(\frac{a+poly(\lambda)+1}{n}\right)$ knowing

$$\left(\frac{a}{n}\right), \left(\frac{a+1}{n}\right), \ldots, \left(\frac{a+poly(\lambda)}{n}\right)$$

where *poly* is a polynomial.

In [9], Damgard's assumption is used as follows. Let (x_1, y_1) be a solution to $QC_n(a, S_1)$ and (x_2, y_2) be a solution to $QC_n(a, S_2)$. By using Lemma 1, these two solutions can be combined into a solution $(x_{1,2}, y_{1,2})$ to $QC_n(a, S_1S_2)$. Then, the authors claimed that, by Damgard's assumption, the probability of getting the Jacobi symbol

$$\left(\frac{2s_1s_2y_3+2}{n}\right) \tag{7}$$

from the sequence

$$\left(\frac{2s_1y_1+2}{n}\right), \left(\frac{2s_2y_2+2}{n}\right) \tag{8}$$

is $1/2$ (s_1 and s_2 are square roots of S_1 and S_2, resp.). Apart from the fact that the authors in [9] consider Damgard's assumption as a proved result (which is not the case), Damgard's assumption cannot be applied to this case because in between $2s_1y_1 + 2$ and $2s_2y_2 + 2$ may exist an exponential (in the security parameter λ) number of integers. Moreover, (6) shows clearly that the Jacobi symbol (7) can easily be obtained from the Jacobi symbols in (8) (recall that a can be publicly computed and x_1 and x_2 are known either from the ciphertext or can be computed from the ciphertext).

Later [10], the same authors (Elashry, Mu, and Susilo) tried to reduce more the number of congruences to be solved in order to get associated polynomials, and proposed a JB_IBE-like scheme. As they have used Lemma 1 to combine solutions, the flaw described above ([18]) still remains.

4 Conclusions

Designing an IBE scheme from quadratic residuosity, more space efficient than the Cocks scheme, is an interesting and valuable objective. The solution proposed by Boneh, Gentry, and Hamburg comes with a very elegant idea: associated polynomials. Unfortunately, their solution uses a quartic time-complexity deterministic algorithm to compute such polynomials from congruences of the form $ax^2 + Sy^2 \equiv 1 \bmod n$. The characterization proposed by Jhanwar and Barua for the solutions to such congruences is a valuable mathematical achievement that leads to efficient probabilistic algorithms to compute solutions. Unfortunately again, this probabilistic algorithm cannot be used in conjunction with the Boneh-Gentry-Hamburg scheme. The way it can be used to obtain IBE schemes, proposed by Jhanwar and Barua, leads to insecure schemes. The insecurity is generated by the fact that the Jacobi symbol of a solution obtained by combining two solutions can be derived from public elements from the Jacobi symbols of the corresponding solutions.

Summing up, the only secure IBE schemes from quadratic residuosity are the Cocks and Boneh-Gentry-Hamburg ($BasicIBE$) schemes (due to space limitation, our exposition did not take into consideration the anonymous variants of these schemes).

References

1. Nuttapong Attrapadung, Yang Cui, David Galindo, Goichiro Hanaoka, Ichiro Hasuo, Hideki Imai, Kanta Matsuura, Peng Yang, and Rui Zhang. Relations among notions of security for identity based encryption schemes. In *Proceedings of the 7th Latin American conference on Theoretical Informatics*, LATIN'06, pages 130–141, Berlin, Heidelberg, 2006. Springer-Verlag.
2. Rana Barua and Mahabir P. Jhanwar. On the number of solutions of the equation $Rx^2 + Sy^2 = 1 \ (\mathrm{mod} N)$. *The Indian Journal of Statistics*, 72-A:226–236, 2010.
3. Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. Relations among notions of security for public-key encryption schemes. In *Proceedings of the 18th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '98, pages 26–45, London, UK, UK, 1998. Springer-Verlag.
4. Mihir Bellare and Amit Sahai. Non-malleable encryption: Equivalence between two notions, and an indistinguishability-based characterization. In *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '99, pages 519–536, London, UK, UK, 1999. Springer-Verlag.
5. Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '01, pages 213–229, London, UK, UK, Aug. 2001. Springer-Verlag.

6. Dan Boneh, Craig Gentry, and Michael Hamburg. Space-efficient identity based encryptionwithout pairings. In *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '07, pages 647–657, Washington, DC, USA, 2007. IEEE Computer Society.
7. Clifford Cocks. An identity based encryption scheme based on quadratic residues. In *Proceedings of the 8th IMA International Conference on Cryptography and Coding*, pages 360–363, London, UK, UK, Dec. 2001. Springer-Verlag.
8. Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography. In *Proceedings of the twenty-third annual ACM symposium on Theory of computing*, STOC '91, pages 542–552, New York, NY, USA, 1991. ACM.
9. Ibrahim Elashry, Yi Mu, and Willy Susilo. Jhanwar-barua's identity-based encryption revisited. In ManHo Au, Barbara Carminati, and C.-C.Jay Kuo, editors, *Network and System Security*, volume 8792 of *Lecture Notes in Computer Science*, pages 271–284. Springer International Publishing, 2014.
10. Ibrahim Elashry, Yi Mu, and Willy Susilo. An efficient variant of boneh-gentry-hamburg's identity-based encryption without pairing. In Kyung-Hyune Rhee and Jeong Hyun Yi, editors, *Information Security Applications*, volume 8909 of *Lecture Notes in Computer Science*, pages 257–268. Springer International Publishing, 2015.
11. Oded Goldreich, Yoad Lustig, and Moni Naor. On chosen ciphertext security of multiple encryptions. *IACR Cryptology ePrint Archive*, 2002:89, 2002.
12. Shafi Goldwasser. Cocks' IBE scheme, bilinear maps. MIT Lecture Notes: "6876: Advanced Cryptography", 2004.
13. Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28:270–299, 1984.
14. Mahabir Prasad Jhanwar and Rana Barua. A variant of boneh-gentry-hamburg's pairing-free identity based encryption scheme. In *Inscrypt*, pages 314–331, 2008.
15. M. Naor and M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *Proceedings of the twenty-second annual ACM symposium on Theory of computing*, STOC '90, pages 427–437, New York, NY, USA, 1990. ACM.
16. Charles Rackoff and Daniel R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '91, pages 433–444, London, UK, UK, 1992. Springer-Verlag.
17. R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairings. In *Proceedings of Symposium on Cryptography and Information Security*, Okinawa, Japan, January 2000. Springer-Verlag.
18. Adrian Schipor. On the security of Jhanwar-Barua identity-based encryption scheme. Submitted, 2016. (personal communication).
19. Adi Shamir. Identity-based cryptosystems and signature schemes. In *Proceedings of CRYPTO 84 on Advances in cryptology*, pages 47–53, New York, NY, USA, 1985. Springer-Verlag New York, Inc.
20. Yodai Watanabe, Junji Shikata, and Hideki Imai. Equivalence between semantic security and indistinguishability against chosen ciphertext attacks. In *Proceedings of the 6th International Workshop on Theory and Practice in Public Key Cryptography: Public Key Cryptography*, PKC '03, pages 71–84, London, UK, UK, 2003. Springer-Verlag.