On the security of Jhanwar-Barua Identity-Based Encryption Scheme

Adrian G. Schipor
aschipor@info.uaic.ro[1]

[†]Department of Computer Science
"Al. I. Cuza" University of Iași
Iași 700506, Romania

Abstract

In [3], Jhanwar and Barua presented an improvement of the Boneh-Gentry-Hamburg (BGH) scheme. In addition to reducing the time complexity of the algorithm to find a solution of the equation $ax^2 + Sy^2 \equiv 1 \bmod n$, their scheme reduces the number of equations to be solved by combining existing solutions. In [2], Susilo et al. extended the Jhanwar-Barua scheme, reducing more the number of equations to be solved. This paper presents a security flaw that appears in both schemes and shows that they are not IND-ID-CPA secure.

1 Intoduction

Identity Based Encryption (IBE) is a type of public key encryption in which the public key can be any arbitrary string. It has been proposed in 1984 by Adi Shamir [6]. Although the idea was presented a long time ago, the first IBE scheme was proposed relatively recently, in 2001, when Boneh and Franklin developed an IBE scheme based on elliptic curves [4]. Soon after, Clifford Cocks developed another IBE scheme [7], based on Quadratic Residuosity Problem (QRA). However, the Cocks scheme is impractical to use because it encrypts one bit by $2 \log n$ bits.

In [1], Boneh, Gentry and Hamburg proposed an IBE scheme (BGH) that encrypts a bit by multiplying it by a random Jacobi symbol, so the ciphertext expansion is much smaller than the ciphertext expansion of the Cocks scheme. However, the time complexity is not as good. In order to encrypt or decrypt a bit, a solution of the equation $ax^2 + Sy^2 \equiv 1 \bmod n$ is needed, where a represents the hashed identity and S is a quadratic residue *modulo* n. Two polynomials, f and g, that satisfies the property that $g(s) = 2y + 2$ and $f(r) = rx + 1$ has the same Jacobi symbol, for every square root s of S and every square root r of a, are used: the Jacobi symbol of $g(s)$ is used for encryption and the Jacobi symbol of $f(r)$ is used for decryption. The main bottleneck of the BGH scheme is the complexity of the algorithm that finds a solution of the equation $ax^2 + Sy^2 \equiv 1 \bmod n$.

Jhanwar and Barua proposed in [3] an efficient algorithm for finding such a solution, together with a modified version of the BGH scheme that uses that algorithm. The resulting scheme is more time efficient than the BGH scheme, but the ciphertext expansion is bigger. This is because the algorithm for finding a solution is probabilistic, so it is not guaranteed that it will find the same solution on both encryption and decryption of a bit. Also, their scheme reduces the number of equations to be solved at encryption and doesn't need to solve any equation at decryption. However, this introduces a security flaw, as it will be seen in section 4.

In [2], Susilo et. al presents an improvement of the Jhanwar-Barua scheme, reducing more the number of equation needed to be solved at encryption. Like the Jhanwar-Barua scheme, their scheme is vulnerable.

2 Definitions

2.1 IBE Scheme

An IBE scheme $\mathcal{E}$ consists of four randomized algorithms [3]:

- **Setup(λ)**: takes as input a security parameter λ and returns the system public parameters PP and the master secret key msk. The system public parameters PP are publicly known, and the master secret key msk is known only to a third party, "Private Key Generator" (PKG).

- **Keygen(PP, msk, id)**: takes as input the system public parameters PP, the master secret key msk and an arbitrary identity $id \in \{0,1\}^*$

and returns the private key d associated with the identity id.

- **Encrypt**(PP, id, m): takes as input the system public parameters PP, an identity id and a message $m \in \{0,1\}^*$ and returns the ciphertext c, that represents the encryption of the message m.
- **Decrypt**(PP, c, d): takes as input the system public parameters PP, a ciphertext $c \in \{0,1\}^*$ and a private key d and returns the decrypted message m, or $\perp$ if the ciphertext is not valid.

2.2 The IND-ID-CPA security model

Boneh and Franklin extended the security notion of indistinguishability against chosen plaintext attack (IND-CPA) to identity-based encryption schemes [4]. The resulting security model (IND-ID-CPA) is defined as the following game between a challenger $\mathcal{C}$ and a PPT adversary $\mathcal{A}$.

IND-ID-CPA game:

1. The challenger $\mathcal{C}$ runs the **Setup** algorithm with a security parameter λ. It publishes the public system parameters PP to the adversary $\mathcal{A}$ and keeps the master secret key msk for itself.
2. The adversary performs (adaptively) private key extraction queries for the identities $id_1, ..., id_k$. The challenger runs the **Extraction** algorithm and sends to the adversary the private keys $d_{id_1}, ..., d_{id_k}$ corresponding to the received identities.
3. The adversary makes one challenge query. It selects two equal length messages m_0, m_1 and a public key id_{Ch} (that didn't appeared in the previous phase) and sends them to the challenger.
4. The challenger picks a random bit $b \in \{0,1\}$ and sends $c = m_b$ as a challenge to the adversary.
5. The adversary performs more private key extraction queries for the identities $id_{k+1}, ..., id_n$ and receives from the challenger the corresponding private keys $d_{id_{k+1}}, ..., d_{id_n}$. The only constraint is that id_i $(k+1 \leq i \leq n)$ is not equal to id_{Ch}.
6. Finally, the adversary outputs a guess $b' \in \{0,1\}$ for the value of b.

The advantage of the adversary $\mathcal{A}$ against an IBE scheme is defined as the following function of the security parameter λ:

$$Adv_{\mathrm{IBE},\mathcal{A}}^{\mathrm{IND-ID-CPA}}(\lambda) = Pr[b' = b] - \frac{1}{2}$$

Definition 1 *An IBE scheme is IND-ID-CPA secure if* $Adv_{\mathrm{IBE},\mathcal{A}}^{\mathrm{IND-ID-CPA}}(\lambda)$ *is a negligible function for all PPT adversaries* $\mathcal{A}$.

2.3 Jacobi Symbols and the QR assumption

Let p be an odd prime. For any integer a, the Legendre symbol $\left(\frac{a}{p}\right)$ is defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } a \equiv 0 \bmod p \\ 1, & \text{if } a \text{ is a quadratic residue mod } p \\ -1, & \text{if } a \text{ is a quadratic non-residue mod } p. \end{cases}$$

Let $N = p_1 p_2 ... p_k$ be the product of k odd primes (not necessarily distinct). For any integer a, the Jacobi symbol $\left(\frac{a}{N}\right)$ is defined as the product of the Legendre symbols corresponding to the prime factors of N:

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right) ... \left(\frac{a}{p_k}\right).$$

For a positive integer N, let $J(N)$ be the following set:

$$J(N) = \{a \in \mathbb{Z}_N \mid \left(\frac{a}{N}\right) = 1\},$$

where $\left(\frac{a}{N}\right)$ is a Jacobi symbol.

The set of quadratic residues *modulo* N $QR(N)$ is defined as:

$$QR(N) = \{a \in \mathbb{Z}_N \mid gcd(a, N) = 1 \wedge x^2 \equiv a \bmod N \text{ has a solution}\}.$$

Definition 2 *Let* $RSAgen(\lambda)$ *be a PPT algorithm that generates two equal size primes* p *and* q. *The Quadratic Residuosity (QR) Assumption holds for* $RSAgen(\lambda)$ *if given a tuple* (N, V), *where* $N = pq$ *and* $V \in J(N)$, *there is no polynomial time algorithm which can determine if* $V \in QR(N)$ *or* $V \in J(N) \setminus QR(N)$ *with non-negligible probability.*

3 The Jhanwar-Barua Scheme

3.1 Preliminaries

The scheme uses the following probabilistic algorithm for finding a solution of the equation $ax^2 + Sy^2 \equiv 1 \bmod N$, where S is a quadratic residue *modulo* N [3]:

1. Randomly choose $t \in \mathbb{Z}_N^*$ such that $a + St^2 \in \mathbb{Z}_N^*$.
2. Output $x_0 = \frac{-2st}{a+St^2}$, $y_0 = \frac{a-St^2}{s(a+St^2)}$.

In addition to this algorithm, the following product formula is used [3]:

Lemma 1 *Let (x_i, y_i) be a solution to $ax^2 + S_i y^2 \equiv 1 \bmod N$ for $i = 1, 2$. Then (x_3, y_3) is a solution to*

$$ax^2 + S_1 S_2 y^2 \equiv 1 \bmod N$$

where $x_3 = \frac{x_1 + x_2}{a x_1 x_2 + 1}$ and $y_3 = \frac{y_1 y_2}{a x_1 x_2 + 1}$.

Also, the scheme uses two functions $f(r) = rx + 1$ and $g(s) = 2sy + 2$ that satisfies the property that the Jacobi symbol of $f(r)$ equals the Jacobi symbol of $g(s)$ for every square root s of S and every square root r of a.

3.2 Structure

The JB scheme is detailed below:

- **Setup(λ)**: Generate two primes, p and q, and let $N = pq$. Choose a random element $u \in J(N) \setminus QR(N)$ and a hash function $H : \mathcal{ID} \mapsto J(N)$. The system public parameters PP are (N, u, H). The master secret key msk is the factorization of N and a secret key K for a pseudorandom function $F_K : \mathcal{ID} \mapsto \{0, 1, 2, 3\}$.
- **Keygen(PP, msk, id)**: Set $R = H(id) \in J(N)$ and $w = F_K(id) \in \{0, 1, 2, 3\}$. Choose $a \in \{0, 1\}$ such that $u^a R \in QR(N)$. Let $\{z_0, z_1, z_2, z_3\}$ be the four square roots of $u^a R \in \mathbb{Z}_N$. Outputs the private key $r = z_w (= d_{id})$.

- **Encrypt(PP, id, m)**: The following algorithm is used to encrypt a message $m \in \{-1, 1\}^l$:

  $k \leftarrow \sqrt{l}$, $R \leftarrow H(id) \in J(N)$
  for $i \in [1, l]$ **do**
    if $i \leq k$ **then**
      $s_i \in \mathbb{Z}_N^*$, $S = s_i^2 \bmod N$
      $(x_i, y_i) \leftarrow Rx_i^2 + S_i y_i^2 \equiv 1 \bmod N$
      $(\bar{x}_i, \bar{y}_i) \leftarrow uR\bar{x}_i^2 + S_i \bar{y}_i^2 \equiv 1 \bmod N$
      $c_i \leftarrow m_i \cdot \left(\frac{2y_i s_i + 2}{N}\right)$
      $\bar{c}_i \leftarrow m_i \cdot \left(\frac{2\bar{y}_i s_i + 2}{N}\right)$
    else
      $(j_1, j_2) \leftarrow i = k \cdot j_1 + j_2$
      $y_{j_1,j_2} \leftarrow \frac{y_{j_1} y_{j_2}}{Rx_{j_1} x_{j_2} + 1}$, $\bar{y}_{j_1,j_2} \leftarrow \frac{\bar{y}_{j_1} \bar{y}_{j_2}}{uR\bar{x}_{j_1} \bar{x}_{j_2} + 1}$
      $c_i \leftarrow m_i \cdot \left(\frac{2y_{j_1,j_2} s_{j_1} s_{j_2} + 2}{N}\right)$
      $\bar{c}_i \leftarrow m_i \cdot \left(\frac{2\bar{y}_{j_1,j_2} s_{j_1} s_{j_2} + 2}{N}\right)$
    end if
    $c \leftarrow [c_1, c_2, ..., c_l]$, $\bar{c} \leftarrow [\bar{c}_1, \bar{c}_2, ..., \bar{c}_l]$
    $x \leftarrow [x_1, x_2, ..., x_k]$, $\bar{x} \leftarrow [\bar{x}_1, \bar{x}_2, ..., \bar{x}_k]$
  end for

  The resulted ciphertext is $C \leftarrow (c, \bar{c}, x, \bar{x})$.

- **Decrypt(PP, C, d_{id})**: To decrypt the ciphertext C using the private key d_{id}, the following algorithm is used:

  for $i \in [1, l]$ **do**
    if $r^2 = R$ **then**
      if $i > k$ **then**
        $(j_1, j_2) \leftarrow i = k \cdot j_1 + j_2$
        $x_i \leftarrow \frac{x_{j_1} + x_{j_2}}{Rx_{j_1} x_{j_2} + 1}$
      end if
      $m_i \leftarrow c_i \cdot \left(\frac{x_i r + 1}{N}\right)$
    end if
    if $r^2 = uR$ **then**
      if $i > k$ **then**
        $(j_1, j_2) \leftarrow i = k \cdot j_1 + j_2$
        $\bar{x}_i \leftarrow \frac{\bar{x}_{j_1} + \bar{x}_{j_2}}{uR\bar{x}_{j_1} \bar{x}_{j_2} + 1}$

end if
$m_i \leftarrow \bar{c}_i \cdot \left(\frac{\bar{x}_i r+1}{N}\right)$
end if
end for

Susilo et al. extended the Jhanwar-Barua scheme, reducing the number of equations needed to be solved. They claim that having the Jacobi symbols $\left(\frac{2y_{j_1}s_{j_1}+2}{N}\right)$ and $\left(\frac{2y_{j_2}s_{j_2}+2}{N}\right)$ is hard to find the value of $\left(\frac{2y_{j_1,j_2}s_{j_1}s_{j_2}+2}{N}\right)$ [2], saying that Damgård proved that [5]. However, because some values are publicly known, this is not a hard problem, as it will be seen in the next section.

4 The security flaw

Because the algorithm used for solving the equations is probabilistic, $(x_i, ..., x_k)$ and $(\bar{x_i}, ..., \bar{x_k})$ are added to the ciphertext so they are publicly known. Thus, if R is a quadratic residue *modulo* N, the following property holds:

$$\left(\frac{rx_{j_1,j_2}+1}{N}\right) = \left(\frac{rx_{j_1}+1}{N}\right)\left(\frac{rx_{j_2}+1}{N}\right)(Rx_{j_1}x_{j_2}+1)^{-1} \tag{1}$$

Because x_{j_1,j_2} is composed we have:

$$rx_{j_1,j_2}+1 = r(x_{j_1}+x_{j_2})(Rx_{j_1}x_{j_2}+1)^{-1}+1.$$

But

$$\begin{aligned}(rx_{j_1}+1)(rx_{j_2}+1) &= r^2x_{j_1}x_{j_2}+rx_{j_1}+rx_{j_2}\\ &= Rx_{j_1}x_{j_2}+1+r(x_{j_1}+x_{j_2})\end{aligned}$$

and if we multiply this with $(Rx_{j_1}x_{j_2}+1)^{-1}$ we obtain

$$(rx_{j_1}+1)(rx_{j_2}+1)(Rx_{j_1}x_{j_2}+1)^{-1} = r(x_{j_1}+x_{j_2})(Rx_{j_1}x_{j_2}+1)^{-1}+1,$$

so the Jacobi symbol $\left(\frac{(rx_{j_1}+1)(rx_{j_2}+1)(Rx_{j_1}x_{j_2}+1)^{-1}}{N}\right)$ equals the Jacobi symbol $\left(\frac{rx_{j_1,j_2}+1}{N}\right)$. x_{j_1} and x_{j_2} are publicly known, so anyone can compute this Jacobi symbol. This proves the property (1).

We know that the Jacobi symbol $\left(\frac{g(s)}{N}\right)$ equals the Jacobi symbol $\left(\frac{f(r)}{N}\right)$, so $\left(\frac{2y_{j_1}s_{j_1}+2}{N}\right)$ equals $\left(\frac{rx_{j_1}+1}{N}\right)$, $\left(\frac{2y_{j_2}s_{j_2}+2}{N}\right)$ equals $\left(\frac{rx_{j_2}+1}{N}\right)$ and $\left(\frac{2y_{j_1,j_2}s_{j_1}s_{j_2}+2}{N}\right)$ equals $\left(\frac{rx_{j_1,j_2}+1}{N}\right)$, so when R is a quadratic residue, we have:

$$\left(\frac{2y_{j_1,j_2}s_{j_1}s_{j_2}+2}{N}\right)=\left(\frac{2y_{j_1}s_{j_1}+2}{N}\right)\left(\frac{2y_{j_2}s_{j_2}+2}{N}\right)(Rx_{j_1}x_{j_2}+1)^{-1} \quad (2)$$

But what happens when R is not a quadratic residue? The property (2) holds even if R is not a quadratic residue *modulo* N:

$$\begin{aligned}
2y_{j_1,j_2}s_{j_1}s_{j_2}+2 &= 2y_{j_1}s_{j_1}y_{j_2}s_{j_2}(Rx_{j_1}x_{j_2}+1)^{-1}+2\\
&= 2\frac{R-S_{j_1}t_{j_1}^2}{s_{j_1}(R+S_{j_1}t_{j_1}^2)}s_{j_1}\frac{R-S_{j_2}t_{j_2}^2}{s_{j_2}(R+S_{j_2}t_{j_2}^2)}s_{j_2}(Rx_{j_1}x_{j_2}+1)^{-1}+2\\
&= \frac{2(R-S_{j_1}t_{j_1}^2)(R-S_{j_2}t_{j_2}^2)}{(R+S_{j_1}t_{j_1}^2)(R+S_{j_2}t_{j_2}^2)(Rx_{j_1}x_{j_2}+1)}+2\\
&= \frac{2(R-S_{j_1}t_{j_1}^2)(R-S_{j_2}t_{j_2}^2)}{(R+S_{j_1}t_{j_1}^2)(R+S_{j_2}t_{j_2}^2)(Rx_{j_1}x_{j_2}+1)}+\\
&\quad+\frac{2(R+S_{j_1}t_{j_1}^2)(R+S_{j_2}t_{j_2}^2)(R\frac{-2s_{j_1}t_{j_1}}{R+S_{j_1}t_{j_1}^2}\frac{-2s_{j_2}t_{j_2}}{R+S_{j_2}t_{j_2}^2}+1)}{(R+S_{j_1}t_{j_1}^2)(R+S_{j_2}t_{j_2}^2)(Rx_{j_1}x_{j_2}+1)}\\
&= \frac{2(R-S_{j_1}t_{j_1}^2)(R-S_{j_2}t_{j_2}^2)}{(R+S_{j_1}t_{j_1}^2)(R+S_{j_2}t_{j_2}^2)(Rx_{j_1}x_{j_2}+1)}+\\
&\quad+\frac{2(R+S_{j_1}t_{j_1}^2)(R+S_{j_2}t_{j_2}^2)\frac{4Rs_{j_1}t_{j_1}s_{j_2}t_{j_2}+(R+S_{j_1}t_{j_1}^2)(R+S_{j_2}t_{j_2}^2)}{(R+S_{j_1}t_{j_1}^2)(R+S_{j_2}t_{j_2}^2)}}{(R+S_{j_1}t_{j_1}^2)(R+S_{j_2}t_{j_2}^2)(Rx_{j_1}x_{j_2}+1)}\\
&= \frac{2(R-S_{j_1}t_{j_1}^2)(R-S_{j_2}t_{j_2}^2)}{(R+S_{j_1}t_{j_1}^2)(R+S_{j_2}t_{j_2}^2)(Rx_{j_1}x_{j_2}+1)}+\\
&\quad+\frac{8Rs_{j_1}t_{j_1}s_{j_2}t_{j_2}+2(R+S_{j_1}t_{j_1}^2)(R+S_{j_2}t_{j_2}^2)}{(R+S_{j_1}t_{j_1}^2)(R+S_{j_2}t_{j_2}^2)(Rx_{j_1}x_{j_2}+1)}\\
&= \frac{2R^2-2R(S_{j_1}t_{j_1}^2+S_{j_2}t_{j_2}^2)+2S_{j_1}S_{j_2}t_{j_1}^2t_{j_2}^2}{(R+S_{j_1}t_{j_1}^2)(R+S_{j_2}t_{j_2}^2)(Rx_{j_1}x_{j_2}+1)}+\\
&\quad+\frac{8Rs_{j_1}t_{j_1}s_{j_2}t_{j_2}+2R^2+2R(S_{j_1}t_{j_1}^2+S_{j_2}t_{j_2}^2)+2S_{j_1}S_{j_2}t_{j_1}^2t_{j_2}^2}{(R+S_{j_1}t_{j_1}^2)(R+S_{j_2}t_{j_2}^2)(Rx_{j_1}x_{j_2}+1)}
\end{aligned}$$

$$= \frac{8Rs_{j_1}t_{j_1}s_{j_2}t_{j_2} + 4R^2 + 4S_{j_1}S_{j_2}t_{j_1}^2t_{j_2}^2}{(R + S_{j_1}t_{j_1}^2)(R + S_{j_2}t_{j_2}^2)(Rx_{j_1}x_{j_2} + 1)}$$
$$= \frac{4(R^2 + 2Rs_{j_1}s_{j_2}t_{j_1}t_{j_2} + S_{j_1}S_{j_2}t_{j_1}^2t_{j_2}^2)}{(R + S_{j_1}t_{j_1}^2)(R + S_{j_2}t_{j_2}^2)(Rx_{j_1}x_{j_2} + 1)}$$
$$= \frac{4(R + s_{j_1}s_{j_2}t_{j_1}t_{j_2})^2}{(R + S_{j_1}t_{j_1}^2)(R + S_{j_2}t_{j_2}^2)(Rx_{j_1}x_{j_2} + 1)},$$

and

$$(2y_{j_1}s_{j_1} + 2)(2y_{j_2}s_{j_2} + 2) = \left(\frac{2(R - S_{j_1}t_{j_1}^2)}{s_{j_1}(R + S_{j_1}t_{j_1}^2)}s_{j_1} + 2\right)\left(\frac{2(R - S_{j_2}t_{j_2}^2)}{s_{j_2}(R + S_{j_2}t_{j_2}^2)}s_{j_2} + 2\right)$$
$$= \frac{16R^2}{(R + S_{j_1}t_{j_1}^2)(R + S_{j_2}t_{j_2}^2)},$$

so the Jacobi symbol $\left(\frac{(2y_{j_1}s_{j_1}+2)(2y_{j_2}s_{j_2}+2)(Rx_{j_1}x_{j_2}+1)^{-1}}{N}\right)$ equals the Jacobi symbol $\left(\frac{2y_{j_1,j_2}s_{j_1}s_{j_2}+2}{N}\right)$ even if R is not a residue *modulo* N. This proves that Jhanwar-Barua scheme is not IND-ID-CPA secure. An adversary chooses two messages m_1, m_2 with $m_{1_{j_1}} = m_{2_{j_1}}$, $m_{1_{j_2}} = m_{2_{j_2}}$ and $m_{1_{j_1,j_2}} \neq m_{2_{j_1,j_2}}$, and sends them to the challenger. The challenger randomly picks one, encrypts it and sends it back to the adversary. The adversary can say with non-negligible probability which message has been encrypted: he obtain the Jacobi symbols $\left(\frac{g(s_{j_1})}{N}\right)$, $\left(\frac{g(s_{j_2})}{N}\right)$ used for encrypting the bits j_1, j_2 and computes $\left(\frac{g(s_{j_1}s_{j_2})}{N}\right) = \left(\frac{g(s_{j_1})}{N}\right)\left(\frac{g(s_{j_2})}{N}\right)(Rx_{j_1}x_{j_2} + 1)^{-1}$, so he can decrypt the i^{th} bit, $i = kj_1 + j_2$. Because $m_{1_i} \neq m_{2_i}$ the adversary can say which message has been encrypted. It doesn't matter which component of the ciphertext he chooses for calculating this because the property (2) holds in both cases. This proves that the Jhanwar-Barua scheme is not IND-ID-CPA secure. Also, the scheme proposed by Susilo et al. has the same security flaw.

5 Conclusion

This paper presents a security flaw that affects the Jhanwar-Barua scheme and it's extension proposed in [2]. Although Susilo et al. pointed that Jhanwar-Barua scheme is not IND-ID-CPA secure, their demonstration is based on the fact that some bits are encrypted using the same solution.

However, even if their scheme solves that problem, the security flaw presented in this paper remains.

Acknowledgment 1: I wish to thank to my supervisor, Prof. Dr. Ferucio Laurențiu Țiplea, for helping me by deducing the property (2) from the section 4 (the case when R is not a quadratic residue), after the practical tests told us that the property should hold.

Acknowledgment 2: This paper was submitted on 13 June 2016 to *Information Processing Letters* journal.

References

[1] Boneh, D., Gentry, C., Hamburg, M.: Space-Efficient Identity Based Encryption Without Pairings. In: Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science. pp. 647–657. FOCS '07, IEEE Computer Society, Washington, DC, USA (2007)

[2] Elashry, I., Mu, Y., Susilo, W.: Jhanwar-Barua's identity-based encryption revisited. In: Au, M., Carminati, B., Kuo, C.C. (eds.) Network and System Security, Lecture Notes in Computer Science, vol. 8792, pp. 271–284. Springer International Publishing (2014)

[3] Jhanwar, M.P., Barua, R.: A variant of Boneh-Gentry-Hamburg's pairing-free identity-based encryption scheme. In: Inscrypt. pp. 314–331 (2008)

[4] Boneh, D., Franklin, M.: Identity-Based Encryption from the Weil Pairing. In: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology. pp. 213–229. CRYPTO '01, Springer-Verlag, London, UK, UK (Aug 2001)

[5] Damgård, I. B.: On the randomness of Legendre and Jacobi sequences. In: Advances in Cryptology: Crypto'88. pp. 163–172. S. Goldwasser, Ed. Berlin, Germany: Springer-Verlag (1990)

[6] Shamir, A.: Identity-Based Cryptosystems and Signature Schemes. In: Proceedings of CRYPTO 84 on Advances in Cryptology. pp. 47–53. Springer-Verlag New York, New York, NY, USA (1985)

[7] Cocks, C: An Identity Based Encryption Scheme based on Quadratic Residues. In: Proceedings of the 8th IMA International Conference on Cryptography and Coding. pp. 360–363. Springer-Verlag, London, UK, UK (Dec 2001)