Computer Science Journal of Moldova, vol.**27**, no.3(81), 2019

On Anonymization of Cocks' Identity-based Encryption Scheme

Anca-Maria Nica and Ferucio Laurenţiu Ţiplea

Abstract

Cocks' identity-based encryption (IBE) scheme is the first IBE scheme that avoids the use of bilinear maps. Based on quadratic residues and due to its simplicity, the scheme gained much attention from researchers. Unfortunately, the scheme is not anonymous in the sense that the cryptotexts may reveal the identities for which they have been computed. Several anonymous variants of it have then been proposed.

In this paper we revise Joye's approach to the anonymization of the Cocks' IBE scheme. Due to some recent results on the distribution of quadratic residues, we present a very simple and direct approach that leads to Joye's scheme.

Keywords: identity-based encryption, quadratic residue, indistinguishability

1 Introduction

In 1984 Adi Shamir proposed the idea of identity-based encryption [14], which is a special case of public-key encryption. This model avoids the public-key infrastructure and the trust chain for public keys. It uses instead a string which uniquely identifies the receiver and computes his public key based on it, using a publicly known hash function.

In his paper [14], Shamir showed how one can sign using the identity-based paradigm but, regarding IBE, only seventeen years later the first solutions were proposed. Thus, in 2001, Boneh and Franklin [5] designed an IBE scheme relying on bilinear maps. In the same year, Cocks [8] created a pairing-free IBE scheme using quadratic residues.

Despite its cryptotext expansion, Cocks' scheme was a starting point for several quadratic residues (QR) based IBE schemes by virtue of its simplicity and elegance [17].

It was shown in [4] that Cocks' scheme does not provide anonymity of the receiver's public key in the sense of Bellare et al. [3]. From this point on, several ideas and schemes have been proposed in order to obtain anonymous variants. The first one was due to Di Crescenzo and Saraswat [9] in 2007, but it is quite impractical because it uses four keys per bit of plaintext. This is also the first public key encryption scheme with keyword search (PEKS) which is not based on bilinear maps.

Starting from the idea in [8] but using quadratic residues in a lighter and deeper way, Boneh, Gentry, and Hamburg [6] proposed an IBE scheme which hides a message not in an integer but in a Jacobi symbol. Moreover, the scheme is anonymous (please see also [16], [17] for supplementary discussion on this very important scheme).

Two years later, Ateniese and Gasti proposed an interesting solution to the anonymization of Cocks' scheme, that reaches universal anonymity [1]. This means that the anonymization process is independent from encryption and can be done using only the public key of the receiver. Moreover their variant is also parallelizable, as well as Cocks' IBE scheme. Unfortunately, Ateniese and Gasti's scheme has much larger cryptotexts than Cocks' scheme.

A variant of [1] was considered in 2010 by Aouinatou and Belkasmi. It has better performances and complexity that the original one [1] while keeping the security in [8].

In 2014, Clear, Tewari, and McGoldrick [7] designed a variant of Cocks' IBE scheme which, beside the fact that it is universally anonymous, it keeps the time complexity close to the initial scheme. Thus, it is faster than the scheme in [1] (as it is shown in Table 1 in [7]) and, further more, outputs shorter cryptotexts than Cocks' scheme.

In the same year, another scheme starting from [1] and providing universal anonymity was proposed by Schipor [13]. Compared to the universal anonymous variant of Ateniese and Gasti [1], the ciphertext expansion of Schipor's solution is considerably smaller and the scheme

is faster.

Joye's [11] solution to the anonymization of Cocks' scheme is probably the most elegant and efficient one. Joye showed that Cocks ciphertexts are squares in a torus-like algebraic structure, and form a quasi-group. From this, he obtained an anonymous variant of Cocks' scheme.

In this paper we re-consider Cocks' scheme, we discuss Galbraith's test in a very precise way based on the recent results in [18], and we present Joye's scheme for Cocks anonymization in a very direct and simply way. We appreciate that this makes more understandable the anonymization process behind Joye's solution.

2 Preliminaries

We recall now the basic notation and terminology that is to be used in the paper.

The set of integers is denoted by $\mathbb{Z}$. If $n, a, b \in \mathbb{Z}$, then a and b are called *congruent modulo* n, denoted $a \equiv b \bmod n$ or $a \equiv_n b$, if n divides $a - b$. The remainder of the integer division of a by n, assuming $n \neq 0$, is denoted $(a)_n$, respectively. Positive integers $n = pq$ that are product of two distinct primes p and q will be usually called *RSA integers* or *RSA moduli*.

Given a positive integer n, $\mathbb{Z}_n$ stands for the set of remainders modulo n, and $\mathbb{Z}_n^*$ is the subset of integers in $\mathbb{Z}_n$ that are co-prime to n. An integer a co-prime with n is a *quadratic residue modulo* n if $a \equiv_n x^2$, for some integer x; the integer x is called a *square root* of a modulo n.

Let p be a prime. The *Legendre symbol* of an integer a modulo p, denoted $\left(\frac{a}{p}\right)$, is 1 if a is a quadratic residue modulo p, 0 if p divides a, and -1 otherwise. The *Jacobi symbol* extends the Legendre symbol to composite moduli. If $n = p_1^{e_1} \cdots p_m^{e_m}$ is the prime factorization of the positive integer n, then the Jacobi symbol of a modulo n is

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_m}\right)^{e_m}.$$

For the sake of simplicity we will use the terminology of Jacobi symbol

in both cases (prime or composite moduli). For details regarding basic properties of the Jacobi symbol the reader is referred to [12], [15].

Given a positive integer n and a subset $A \subseteq \mathbb{Z}_n^*$, $QR_n(A)$ ($QNR_n(A)$, $J_n^+(A)$, $J_n^-(A)$) stands for the set of quadratic residues (quadratic non-residues, integers with the Jacobi symbol 1, integers with the Jacobi symbol -1, respectively) modulo n from A. When $A = \mathbb{Z}_n^*$, the notation will be simplified to QR_n (QNR_n, J_n^+, J_n^-, respectively). When n is a prime, $QR_n(A) = J_n^+(A)$ and $QNR_n(A) = J_n^-(A)$.

For a set A, $a \leftarrow A$ means that a is uniformly at random chosen from A. If $\mathcal{A}$ is a probabilistic algorithm, then $a \leftarrow \mathcal{A}$ means that a is an output of $\mathcal{A}$ for some given input.

The asymptotic approach to security makes use of security parameters, denoted by λ in our paper. A positive function $f(\lambda)$ is called *negligible* if for any positive polynomial $poly(\lambda)$ there exists n_0 such that $f(\lambda) < 1/poly(\lambda)$, for any $\lambda \geq n_0$.

Let $RSAgen(\lambda)$ be a probabilistic polynomial time algorithm that, given a security parameter λ, outputs a triple (n, p, q), where $n = pq$ is an RSA modulus. The *quadratic residuosity* (QR) *assumption* holds for $RSAgen(\lambda)$ if the distance

$$|P(\mathcal{D}(a, n) = 1 \ : \ (n, p, q) \leftarrow RSAgen(\lambda),\ a \leftarrow QR_n) -$$

$$P(\mathcal{D}(a, n) = 1 \ : \ (n, p, q) \leftarrow RSAgen(\lambda),\ a \leftarrow J_n \setminus QR_n)|,$$

as a function of λ, is negligible for all probabilistic polynomial-time algorithms $\mathcal{D}$.

An IBE scheme consists of four probabilistic polynomial time (PPT) algorithms, Setup, KeyGen, Enc, and Dec. The Setup(λ) algorithm outputs the public parameters PP together with the master secret msk, having as input the security parameter λ. The KeyGen(PP, msk, ID) algorithm outputs the secret key for the identity ID. The third algorithm, Enc(PP, m), computes the ciphertext of the message m for a given identity, while the last algorithm, Dec(sk_{ID}, c), decrypts the cryptotext c using the secret key sk_{ID} of the identity ID.

Regarding the security, an IBE scheme $\mathcal{S}$ is said to be ANON-IND-ID-CPA secure if the advantage of any efficient PPT adversary

$\mathcal{A}$ against the scheme $\mathcal{S}$ is negligible when the following game is considered:

Setup: the challenger $\mathcal{C}$ gives the public parameters outputted by the SETUP algorithm to the adversary.

Phase 1: the adversary queries the challenger for the secret keys corresponding to the identities that $\mathcal{A}$ chooses. In response, $\mathcal{C}$ runs the KEYGEN algorithm and sends $\mathcal{A}$ the secret keys. The adversary also can issue decryption queries where he sends a pair (ID_i, c_i) and receives the corresponding plaintext decrypted by the DEC algorithm.

Challenge: in this phase $\mathcal{A}$ sends two challenge identities ID_0^* and ID_1^* to $\mathcal{C}$, different from all the identities used in the previous phase, and two equal-length messages m_0 and m_1. The challenger chooses at random a bit $b \in \{0, 1\}$ and encrypts the pair (ID_b^*, m_b). Then he sends the ciphertext to $\mathcal{A}$.

Phase 2: the adversary is allowed to issue the same types of queries as in *Phase 1*, with the restriction that the identities he chooses have to be different from ID_0 and ID_1 which were used in the *Challenge* phase.

Guess: the adversary tries to guess the pair that was encrypted by the challenger in the *Challenge* phase. Thus it sends a bit b' to the challenger.

The advantage of the adversary in the above game is computed as

$$Adv_{\mathcal{A},\mathcal{S}}(\lambda) = \left| P[b = b'] - \frac{1}{2} \right|,$$

where λ is the security parameter.

3 Cocks' IBE scheme and anonymization

The first pairing-free IBE scheme was proposed by Cocks and it is based on quadratic residues [8]. The scheme is IND-ID-CPA secure in the random oracle model (ROM) under the Quadratic Residuosity Assumption

(QRA) modulo a large RSA integer. Cocks' IBE scheme is defined by four probabilistic algorithms, as it is described in Algorithm 1 on page 289.

It was mentioned in [4, Section 4] that the scheme is not anonymous in the sense that the outputted cryptotexts contain information about the receiver so one can check if the ciphertext was encrypted for a specific identity. The tool which helps to decide this is Galbraith's test (GT), which was briefly described in [1], [4].

In order to understand Galbraith's test, we will turn our attention to *Cocks ciphertexts*, and mainly follow the approach in [18].

Working in an RSA group $\mathbb{Z}_n^*$, we will consider an integer a, which has the Jacobi symbol modulo n equal to 1 (a corresponds to some identity ID, but, for simplicity, we will call a the identity). Then, a cryptotext computed for the identity a has the form $c = t + at^{-1} \bmod n$, for some $t \in \mathbb{Z}_n^*$. That is, t is a solution to the degree two congruence $t^2 - ct + a \equiv 0 \bmod n$. It is useful then to denote [18]:

$$\begin{aligned} C_n(a) &= \{(t + at^{-1})_n \mid t \in \mathbb{Z}_n^*\}, \\ C_n^*(a) &= C_n(a) \cap \mathbb{Z}_n^*, \\ C_n^{e_1,e_2}(a) &= \left\{c \in \mathbb{Z}_p^* \mid \left(\tfrac{c^2-4a}{p}\right) = e_1,\ \left(\tfrac{c^2-4a}{q}\right) = e_2\right\}, \end{aligned}$$

where n is the product of two primes p and q, and $e_1, e_2 \in \{-1, 0, 1\}$.

We recall below some results in [18]. First of all, we clearly have:

Corollary 1 ([18]). *Let n be an RSA modulus and $a \in \mathbb{Z}_n^*$. Then the set $C_n^*(a)$ is a union of the sets $C_n^{0,0}, C_n^{1,0}, C_n^{0,1}$ and $C_n^{1,1}$.*

This union is pictorially described by Figure 1. This diagram gives us a clear understanding of the output given by Galbraith's test.

Notation 3.1 ([18]). *Let p be an odd prime, $p \bmod 4 = i$, $i \in \{1, 3\}$ and a an integer co-prime with p, then we define:*

$$\tau_{p,a}^i = \begin{cases} 1, & \text{if } (p)_4 = i \text{ and } (a)_p \in QR_p \\ 0, & \text{otherwise} \end{cases}$$

Algorithm 1 Cocks' IBE scheme

procedure SETUP(λ):
  $(p, q, n) \leftarrow RSA_{gen}(\lambda)$, where $n = pq$;
  $e \leftarrow J_n^+ \setminus QR_n$;
  choose a hash function $h : \{0,1\}^* \to J_n^+$;
  PP: n, e, h; ▷ the public parameters
  msk: p, q; ▷ the master secret key
  return (PP, msk).
end procedure

procedure KEYGEN(msk, ID):
  $a = h(ID)$; ▷ the identity
  if $a \in QR_n$ **then**
    $r \leftarrow a^{1/2}$
  else $r \leftarrow (ea)^{1/2}$
  end if;
  return r. ▷ the secret key of the identity ID
end procedure

procedure ENC(PP, ID, m): ▷ $m \in \{\pm 1\}$
  $a = h(ID)$;
  $t_1, t_2 \leftarrow \mathbb{Z}_n^*$ such that $(\frac{t_1}{n}) = (\frac{t_2}{n}) = (\frac{m}{n})$;
  $c_1 = t_1 + at_1^{-1} \bmod n$ and $c_2 = t_2 + eat_2^{-1} \bmod n$;
  return (c_1, c_2).
end procedure

procedure DEC($PP, r, (c_1, c_2)$):
  if $r^2 \equiv h(ID) \bmod n$ **then** $c = c_1$
  else $c = c_2$
  end if;
  $m = \left(\frac{c+2r}{n}\right)$;
  return m.
end procedure

and

$$\bar{\tau}^i_{p,a} = \begin{cases} 1, & \text{if } (p)_4 = i \text{ and } (a)_p \in QNR_p \\ 0, & \text{otherwise,} \end{cases}$$

where $i = 1, 3$.

Corollary 2 ([18]). *Let* p, q *be two odd primes,* $n = pq$ *an RSA modulus,* $a \in \mathbb{Z}_n^*$, $k_1 = p \text{ div } 4$, *and* $k_2 = q \text{ div } 4$. *Then,*

1. $|C_n^*(a)| = |C_p^*((a)_p)| \cdot |C_q^*((a)_q)|$;
2. $|C_n^{0,0}(a)| = 4(\tau^1_{p,a} + \tau^3_{p,a})(\tau^1_{q,a} + \tau^3_{q,a})$;
3. $|C_n^{0,1}(a)| = 4(\tau^1_{p,a} + \tau^3_{p,a})(k_2 - \tau^1_{q,a})$;
4. $|C_n^{1,0}(a)| = 4(\tau^1_{q,a} + \tau^3_{q,a})(k_1 - \tau^1_{p,a})$;
5. $|C_n^{1,1}(a)| = 4|QR_n(a + QR_n)| = 4(k_1 - \tau^1_{p,a})(k_2 - \tau^1_{q,a})$;
6. $|C_n(a)| = |C_p((a)_p)| \cdot |C_q((a)_q)|$.

Now we get the following useful result which will help us to compute a probability in order to analyze Galbraith's test.

Theorem 1 ([18]). *Let* n *be an RSA modulus, the product of odd primes* p *and* q, *and* $a \in \mathbb{Z}_n^*$. *Then the set* $G_n(a)$ *is partitioned by the sets* $C_n^{1,1}(a)$ *and* $C_n^{-1,-1}(a)$, *and its cardinal is:* $4|QR_n(a + J_n^+)|$.

The Galbraith's test of $c \in \mathbb{Z}_n^*$ w.r.t. a, denoted $GT_{n,a}(c)$, is

$$GT_{n,a}(c) = \left(\frac{c^2 - 4a}{n}\right).$$

Let $G_n(a) = \{c \in \mathbb{Z}_n^* \mid GT_{n,a}(c) = 1\}$. Clearly,

$$G_n(a) = C_n^{1,1}(a) \cup C_n^{-1,-1}(a).$$

An integer $c \in \mathbb{Z}_n^*$ passes Galbraith's test w.r.t. n and a if $GT_{n,a}(c) = 1$ (or, $c \in G_n(a)$). Not all Cocks ciphertexts pass Galbraith's test, but most of them do. The diagram in Figure 1 shows clearly which Cocks ciphertexts pass Galbraith's test.

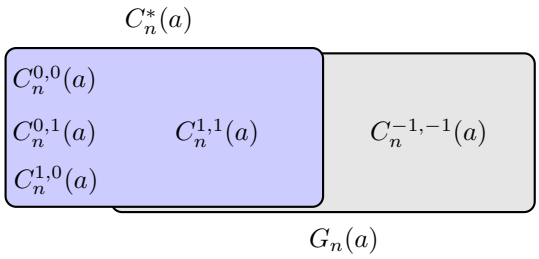

Figure 1. The sets C_n^* and $G_n(a)$

Galbraith's test for anonymity is then described in Algorithm 2.

Algorithm 2 Galbraith's Test

`Input` : RSA modulus n, $a \in J_n^+$, and $c \in \mathbb{Z}_n^*$
`Output` : 1 / 0
if $\left(\frac{c^2-4a}{n}\right) = 1$ **then**
  1 ▷ $c \in C_n^*(a)$ `with prob.` $\frac{1}{2} - \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$
else
  0 ▷ $c \in C_n^*(a)$ `with negl. prob.`
end if

We note that if $\left(\frac{c^2-4a}{n}\right) = -1$, then $c \notin C_n^*(a)$ (with probability 1). However, if $\left(\frac{c^2-4a}{n}\right) = 1$, then c is a Cocks ciphertext with probability overwhelming closed to 1/2. More precise results are offered in [18] by the following probability:
$P(c \in C_n^*(a) : c \leftarrow G_n(a)) = \frac{|C_n^{1,1}(a)|}{|G_n(a)|} = \frac{4|QR_n(a+QR_n)|}{4|QR_n(a+J_n^+)|} = \frac{1}{2} - \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$.

The *key-privacy test* consists of the repeated application of Galbraith's test with values sampled from either $G_n(a)$ (and $G_n(ea)$) or $G_n(b)$ (and $G_n(eb)$), where e is as in Cocks' IBE scheme.

4 Another view on Joye's scheme

Through his work, Joye [11] showed that Cocks' scheme is homomorphic. He analyzed its cryptotexts and defined their precise algebraic structure using a cyclotomic polynomial and an algebraic torus. He defined a special multiplicative group with a certain operation, then he described how it works for a prime modulus in order to use these results for defining it in the case of an RSA modulus. Finally he considered the operation above over Cocks' ciphertexts, using the discriminant $\delta = c^2 - 4a$ of the equation $t^2 - ct + a$ in the unknown t, where $c, a \in \mathbb{Z}_n^*$, and more specifically, he considered c as a Cocks ciphertext and a an identity in the same context.

If we look again to the set of Cocks ciphertexts, whose main part consists of $C_n^{1,1}(a)$, we may imagine the following very simple method to anonymize them: given $c \in C_n^{1,1}(a)$, modify it into c' on a random basis such that $GT_{n,a}(c') = \pm 1$. As we have to decrypt c', the ciphertext c must be altered in such a way so that the receiver be able to reverse it. From this point of view, the simplest method seems to choose and fix d such that $GT_{n,a}(d) = -1$, and then to look for a binary operation $\circ$ on $\mathbb{Z}_n^*$ such that

$$GT_{n,a}(c \circ d) = GT_{n,a}(c) \cdot GT_{n,a}(d).$$

If such a binary operation is found, then we may take $c' = c \circ d$ (but, once again, we flip a coin to decide whether we keep c or compute c').

Under these circumstances we define the operation

$$u \circ v = \frac{uv + 4a}{u + v} \bmod n,$$

for all $u, v \in \mathbb{Z}_n^*$ with $(u + v, n) = 1$.

Although this operation depends on n and a, for the sake of simplicity, we will simply denote it by $\circ$. Its basic properties are listed below.

Proposition 1. *Let $u, v, w \in \mathbb{Z}_n^*$ and $a \in J_n^+$. Then :*

1. *When defined,* $\circ$ *is associative*
$$u \circ (v \circ w) = (u \circ v) \circ w.$$
2. *If* $(u+v, n) = 1$ *and* $(v^2 - 4a, n) = 1$*, then*
$$(u \circ v) \circ (-v) = u$$
(*remark that* $v \circ (-v)$ *is not defined*).
3. $GT_{n,a}(u \circ v) = GT_{n,a}(u) \cdot GT_{n,a}(v)$*, provided that* $u \circ v$ *is defined.*
4. $u \circ u \in G_n(a)$.

Proof. In order to prove (1) we simply apply the operation $\circ$ and do the computation
$$u \circ \frac{vw + 4a}{v + w} = \frac{uv + 4a}{u + v} \circ w.$$
Getting the same result on both sides, we are done
$$\frac{uvw + 4a(u + v + w)}{uv + uw + vw + 4a}.$$
The second property follows from the simple computation below
$$\begin{aligned}
(u \circ v) \circ (-v) &= \frac{\frac{uv+4a}{u+v} \cdot (-v) + 4a}{\frac{uv+4a}{u+v} + (-v)} \\
&= \frac{(u(-v^2) + 4a(u+v-v)) \cdot (u+v)}{(u+v) \cdot (uv + 4a - uv - v^2)} \\
&= \frac{u(4a - v^2)}{4a - v^2} \\
&= u.
\end{aligned}$$
For (3) we have:
$$\begin{aligned}
GT_{n,a}(u \circ v) &= \left(\frac{(u^2 - 4a)(v^2 - 4a)(u+v)^{-2}}{n} \right) \\
&= \left(\frac{u^2 - 4a}{n} \right) \left(\frac{v^2 - 4a}{n} \right) \\
&= GT_{n,a}(u) \cdot GT_{n,a}(v).
\end{aligned}$$
Given that $GT_{n,a}(u \circ u) = GT_{n,a}(u) \cdot GT_{n,a}(u)$ from (3), it immediately follows that $GT_{n,a}(u \circ u)$ is 1, so u is in $G_n(a)$. □

Proposition 1(3) says that $u \circ v$ passes Galbraith's test if and only if both u and v pass Galbraith's test or both do not pass Galbraith's test (provided that $u \circ v$ is defined), and Proposition 1(4) says that $u \circ u$ always passes Galbraith's test.

Fortunately, this is all we need to obtain Joye's approach to the anonymization of Cocks' IBE scheme, as we can see in Algorithm 3 on page 295.

The correctness of the scheme in Algorithm 3 simply follows from Proposition 1. As with respect to security, we have the following result.

Theorem 2. *Cocks' AnonIBE scheme is ANON-IND-ID-CPA secure in the random oracle model under the QRA.*

Proof. Any adversary $\mathcal{A}$ against Cocks' AnonIBE scheme can be transformed into an adversary $\mathcal{A}'$ against Cocks' IBE scheme, with an advantage greater than or equal to the advantage of $\mathcal{A}$. Therefore, as Cocks' IBE scheme is IND-ID-CPA, Cocks' AnonIBE scheme must be.

To prove that Cocks' AnonIBE scheme is anonymous, consider the sets

$$\mathcal{D}_0 = G_n(a_0) \cup (G_n(a_0) \circ d)$$

and

$$\mathcal{D}_1 = G_n(a_1) \cup (G_n(a_1) \circ d),$$

where a_0 and a_1 are two public keys and d is as in Cocks' AnonIBE scheme. We prove that $c \in \mathcal{D}_0$ iff $c \in \mathcal{D}_1$.

Let $c \in \mathcal{D}_0$. Assume first that, if $GT_{n,a_1}(c) = 1$, then $c \in \mathcal{D}_1$. Otherwise, $GT_{n,a_1}(c \circ (-d)) = 1$, which shows that $c \circ (-d) \in G_n(a_1)$. But then, $(c \circ (-d)) \circ d \in G_n(a_1) \circ d$, which leads to $c \in G_n(a_1) \circ d \subseteq \mathcal{D}_1$.

Assume now that $GT_{n,a_0}(c) = -1$. Then, $GT_{n,a_0}(c \circ (-d)) = 1$, which proves that $c \circ (-d) \in G_n(a_0) \subseteq \mathcal{D}_0$. The above argument proves then $c \circ (-d) \in \mathcal{D}_1$, from which it follows that $c \in \mathcal{D}_1$.

As a conclusion, if $c \in \mathcal{D}_0$, then $c \in \mathcal{D}_1$. Due to the symmetry of this relation, we get the theorem. □

Algorithm 3 Cocks' AnonIBE scheme

procedure SETUP(λ):
$PP = (n, e, d, h)$
▷ where n and e are as in Cocks' IBE scheme
$d \leftarrow \mathbb{Z}_n^*$ and $h : \{0,1\}^* \to J_n^+$ are chosen so that $GT_{n,a}(d) = -1 = GT_{n,ea}(d)$, for any output a of h
$msk = (p, q)$
return (PP, msk).
end procedure

procedure EXT(msk, ID):
$a = h(ID)$;
▷ private key: random square root r of a or ea
return r.
end procedure

procedure ENC(PP, ID, m):
$a = h(ID)$;
$t_0, t_1 \leftarrow \mathbb{Z}_n^*$ with $J_n(t_0) = m = J_n(t_1)$;
$c_0 \leftarrow \{u, u \circ d\}$ where $u = t_0 + at_0^{-1} \bmod n$;
$c_1 \leftarrow \{v, v \circ d\}$ where $v = t_1 + eat_1^{-1} \bmod n$;
return (c_0, c_1).
end procedure

procedure DEC($(c_0, c_1), r$):
set $b \in \{0,1\}$ such that $e^b a \equiv_n r^2 \bmod n$;
return $m = \begin{cases} J_n(c_b + 2r), & \text{if } GT_{n,e^b a}(c_b) = 1 \\ J_n(c_b \circ (-d) + 2r), & \text{otherwise} \end{cases}$
end procedure

5 Conclusion

In this paper we achieved the anonymization in Joye's work [11] in a significantly easier way. The main resource used in order to attain this was the new results on quadratic residues in [18]. This extensive study facilitates a better understanding of the cryptotexts outputted by Cocks' IBE scheme and their structure. Furthermore, [18] facilitates a detailed analysis of Galbraith's test, capturing the essence of the anonymization process regarding Cocks' IBE cryptotexts. This allowed us to bring clarity and capture the essence in Joye's variant.

References

[1] Giuseppe Ateniese and Paolo Gasti, "Universally anonymous IBE based on the quadratic residuosity assumption," in *CT-RSA 2009* (Lecture Notes in Computer Science, vol. 5473), Springer, 2009, pp. 32–47.

[2] Rkia Aouinatou and Mostafa Belkasmi, "Efficient anonymity for Cocks' scheme," in *Proceedings of 5th International Symposium on I/V Communications and Mobile Networks, ISIVC 2010*, 2010, pp. 1–4. Preprint on IACR Cryptology ePrint Archive. Report 2011/684, 2016. https://eprint.iacr.org/2011/684.

[3] Mihir Bellare, Dennis Hofheinz, and Scott Yilek, "Possibility and impossibility results for encryption and commitment secure under selective opening," in *Advances in Cryptology - EUROCRYPT 2009, Proceedings of 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, (Cologne, Germany, April 26-30, 2009), 2009, pp. 1–35.

[4] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano, "Public key encryption with keyword search," in *EUROCRYPT 2004* (Lecture Notes in Computer Science, vol. 3027), Springer, 2004, pp. 506–522.

[5] Dan Boneh and Matthew K. Franklin, "Identity-based encryption from the Weil pairing," in *CRYPTO 2001*, (Lecture Notes in Computer Science, vol. 2139), Springer, 2001, pp. 213–229.

[6] Dan Boneh, Craig Gentry, and Michael Hamburg, "Space-efficient identity based encryption without pairings," in *FOCS 2007, IEEE Computer Society*, 2007, pp. 647–657.

[7] Michael Clear, Hitesh Tewari, and Ciarán McGoldrick, "Anonymous IBE from quadratic residuosity with improved performance," in *AFRICACRYPT 2014* (Lecture Notes in Computer Science, vol. 8469), Springer, 2014, pp. 377–397.

[8] Clifford Cocks, "An identity based encryption scheme based on quadratic residues," in *IMACC 2001* (Lecture Notes in Computer Science, vol. 2260), Springer, 2001, pp. 360–363.

[9] Giovanni Di Crescenzo and Vishal Saraswat, "Public key encryption with searchable keywords based on Jacobi symbols," in *Progress in Cryptology – INDOCRYPT 2007, Proceedings of 8th International Conference on Cryptology in India*, (Chennai, India, December 9-13, 2007), 2007, pp. 282–296.

[10] Ryotaro Hayashi and Keisuke Tanaka, "Universally anonymizable public-key encryption," in *Proceedings of the 11th international conference on Theory and Application of Cryptology and Information Security, ASIACRYPT'05*, Berlin, Heidelberg: Springer-Verlag, Dec 2005, pp. 293–312.

[11] Marc Joye, "Identity-based cryptosystems and quadratic residuosity," in *PKC 2016* (Lecture Notes in Computer Science, vol. 9614), Springer, 2016, pp. 225–254.

[12] Melvyn B. Nathanson, *Elementary Methods in Number Theory*, New York: Springer, 2000.

[13] Gheorghe A. Schipor, "On the anonymization of Cocks IBE scheme," in *Cryptography and Information Security in the Balkans*

- *First International Conference, BalkanCryptSec 2014, Revised Selected Papers*, (Istanbul, Turkey, October 16-17, 2014), 2014, pp. 194–202.

[14] Adi Shamir, "Identity-based cryptosystems and signature schemes," in *CRYPTO 1984* (Lecture Notes in Computer Science, vol. 196), Springer, 1985, pp. 47–53.

[15] Victor Shoup, *A Computational Introduction to Number Theory and Algebra*, 2nd edition, New York, NY, USA: Cambridge University Press, 2009.

[16] George Teşeleanu, Ferucio Laurenţiu Ţiplea, Sorin Iftene, and Anca-Maria Nica, "Boneh-Gentry-Hamburg's identity-based encryption schemes revisited," Preprint on IACR Cryptology ePrint Archive. Report 2016/516, 2016. https://eprint.iacr.org/2016/516.

[17] Ferucio Laurenţiu Ţiplea, Sorin Iftene, George Teşeleanu, and Anca-Maria Nica, "Security of identity-based encryption schemes from quadratic residues," in *Innovative Security Solutions for Information Technology and Communications - 9th International Conference, SECITC 2016, Revised Selected Papers*, (Bucharest, Romania, June 9-10, 2016), 2016, pp. 63–77.

[18] Ferucio Laurenţiu Ţiplea, Sorin Iftene, George Teşeleanu, and Anca-Maria Nica, "On the distribution of quadratic residues and non-residues modulo composite integers and applications to cryptography," Preprint on IACR Cryptology ePrint Archive. Report 2019/638, https://eprint.iacr.org/2019/638.pdf, 2019. Submitted to *Applied Mathematics and Computation*, 2019.

Anca-Maria Nica[1], Ferucio Laurenţiu Ţiplea[1] Received September 20, 2019

[1]Department of Computer Science, "Al.I.Cuza" University of Iaşi
E–mail: contact@ancamarianica.ro, ferucio.tiplea@uaic.ro