Elementary Remarks on Some Quadratic Based Identity Based Encryption Schemes

Paul Cotan[1,2] and George Teşeleanu[1,2]

[1] Advanced Technologies Institute
10 Dinu Vintilă, Bucharest, Romania
{paul.cotan,tgeorge}@dcti.ro
[2] Simion Stoilow Institute of Mathematics of the Romanian Academy
21 Calea Grivitei, Bucharest, Romania

Abstract. In the design of an identity-based encryption (IBE) scheme, the primary security assumptions center around quadratic residues, bilinear mappings, and lattices. Among these approaches, one of the most intriguing is introduced by Clifford Cocks and is based on quadratic residues. However, this scheme has a significant drawback: a large ciphertext to plaintext ratio. A different approach is taken by Zhao *et al.*, who design an IBE still based on quadratic residues, but with an encryption process reminiscent of the Goldwasser-Micali cryptosystem. In the following pages, we will introduce an elementary method to accelerate Cocks' encryption process and adapt a space-efficient encryption technique for both Cocks' and Zhao *et al.*'s cryptosystems.

1 Introduction

The development of identity based encryption (IBE) began in 1984 when Shamir formulated its basic principles in [23]. However, he left the practical construction of such a scheme as an open problem. In 2001, the first IBE schemes were proposed by Boneh and Franklin [6], who used bilinear mappings, and by Cocks [11], who utilized quadratic residues, respectively.

The Cocks' encryption scheme processes messages on a bit-by-bit basis, where each encrypted bit is represented as a pair of two integers. Decryption involves calculating the Jacobi symbol of one of the two integers in each pair. Therefore, Cocks' IBE has a large ciphertext to plaintext ratio, and thus is efficient only for small messages. A space-efficient IBE based on quadratic residues was introduced in [7]. Unfortunately, their solution is based on a quartic deterministic time-complexity algorithm, and thus is infeasible to use in practice. To address this issue, Jhanwar and Barua [4, 18] introduced an efficient probabilistic algorithm. However, their scheme, along with several other variations [13, 14], have been shown to be insecure [22]. A different approach was taken in [24]. Their proposal resembles the Goldwasser-Micali [16] cryptosystem. Their solution also has a large ciphertext to plaintext ratio: to encrypt a bit we need four integers.

Our paper focuses on Cocks' and Zhao *et al.*'s IBE schemes [11, 24]. In the first part of the paper we introduce a different method for generating the special random numbers t required by Cocks' encryption algorithm. The generation

method bears similarity to the Goldwasser-Micali encryption, with the primary distinction being the distribution of one of the public parameters. While this method may seem obvious, it is worth noting that all previous papers dealing with Cocks' IBE have relied on a trial-and-error method based on Jacobi symbols to generate the t values. Therefore, our method lowers the complexity of generating t values from at least $\mathcal{O}(M(2\lambda)\log 2\lambda)$ to $\mathcal{O}(M(2\lambda))$, where λ is a security parameter and $M(\cdot)$ denotes the complexity of a multiplication.

In the second part of our work, we use some elementary remarks to reduce the bandwith requirements for both Cocks' and Zhao *et al.*'s IBE schemes with 2 and 4 bits per ciphertext, respectively. The changes made to achieve this improvement, do not introduce any additional overhead to the encryption process. It is worth noting that both IBEs have been recommended for symmetric key encapsulation. Consequently, the additional bits can serve various purposes, such as authenticating the encapsulation package. Since our changes involve only comparison operators and differences, coupled with our reduced bit usage per encapsulation, we believe that our proposal is preferable when compared to the original schemes.

Structure of the paper. In Section 2, we introduce the fundamental notions used throughout the paper. In Section 3, we present a computationally efficient variant of Cocks' IBE. Section 4 discusses two space-efficient IBEs. Finally, we conclude in Section 5.

2 Preliminaries

Notations. Throughout the paper, λ denotes a security parameter. The action of selecting a random element x from a sample space X is denoted by $x \xleftarrow{\$} X$, while $x \leftarrow y$ represents the assignment of value y to variable x.

The Jacobi symbol of an integer a modulo an integer n will be represented by $J_n(a)$. We consider the sets QR_n and QNR_n of quadratic and, respectively, non-quadratic residues modulo an integer n. J_n denotes the sets of integers modulo n with Jacobi symbol 1.

2.1 Identity-Based Encryption

An IBE scheme [5] comprises four probabilistic polynomial-time (PPT) algorithms, denoted as *Setup*, *KeyGen*, *Enc*, and *Dec*. The first algorithm takes the security parameter as input and produces the master secret key along with the system's public parameters as output. The subsequent algorithm takes an identity id, the master secret key, the public parameters as input, and yields a private key associated with id as output. The third algorithm, labeled *Enc*, accepts a message m, an identity id, and the public parameters as input, encrypting m using a key derived from id to produce the ciphertext c. The final algorithm, *Dec*, decrypts the ciphertext c using the private key associated with id, yielding the original message m.

Cocks' IBE scheme. The first IBE based on the QR assumption[3] was introduced in [11]. The original scheme was defined for primes of type $p \equiv q \equiv 3 \bmod 4$. Later on, this scheme was generalized in [19] to any prime numbers p and q. We further present the IBE scheme provided in [19].

Setup(λ): Given a security parameter λ, generate two primes $p, q > 2^\lambda$ and compute their product $n = pq$. Randomly generate an integer $u \in J_n \setminus QR_n$. The public parameters are $pp = \{n, u, H\}$, where $H : \{0,1\}^* \to J_n$ is a cryptographic hash function. The master secret key is $msk = \{p, q\}$.

KeyGen(pp, msk, id): Let $R = H(id)$. If $R \in QR_n$, then compute $r \equiv R^{1/2} \bmod n$. Otherwise, computes $r = (uR)^{1/2} \bmod n$. The private key is r.

Enc(pp, id, m): On inputting pp, an identity id and a message $m \in \{-1, 1\}$, compute the hash value $R = H(id)$ and randomly choose two values $t_1, t_2 \xleftarrow{\$} \mathbb{Z}_n$ such that $J_n(t_1) = J_n(t_2) = m$. Also, calculate

$$c_1 = t_1 + \frac{R}{t_1} \bmod n \quad \text{and} \quad c_2 = t_2 + \frac{uR}{t_2} \bmod n.$$

Return the ciphertext $C = (c_1, c_2)$.

Dec(pp, r, C): On input pp, a secret key r and a ciphertext C, compute

$$m = \begin{cases} J_n(c_1 + 2r) & \text{if } r^2 \equiv H(id) \bmod n; \\ J_n(c_2 + 2r) & \text{otherwise.} \end{cases}$$

Remark 1. Cocks' IBE scheme does not provide anonymity [7]. As a result, several techniques have been introduced to address this issue [2, 19–21]. Among these, the most efficient method is the one described in [20], which is a simplified version of the approach presented in [19].

Zhao *et al.*'s IBE scheme. An alternative IBE scheme relying on the QR assumption was presented in [24]. Specifically, the scheme operates with polynomials modulo n, where the primes p and q are selected such that $p \equiv -q \bmod 4$. This scheme was subsequently extended and generalized in [12] to accommodate arbitrary values of p and q. We further provide the scheme's description as given in [12].

Setup(λ): Given a security parameter λ, generate two primes $p, q > 2^\lambda$ and compute their product $n = pq$. Randomly generate two integers $u, y \in \mathbb{Z}_n$ such that $J_p(u) = J_q(u) = -1$ and $J_p(y) = -J_q(y)$. The public parameters are $pp = \{n, u, y, H\}$, where $H : \{0,1\}^* \to J_n$ is a cryptographic hash function. The master secret key is $msk = \{p, q\}$.

KeyGen(pp, msk, id): Let $R = H(id)$. If $R \in QR_n$, then compute $r \equiv R^{1/2} \bmod n$. Otherwise, computes $r = (uR)^{1/2} \bmod n$. The private key is r.

[3] This assumption states that an adversary trying to decide if a random element is from $J_n \setminus QR_n$ or QR_n has a negligible success probability.

Enc(pp, id, m): On inputting pp, an identity id and a message $m \in \{0,1\}$, compute the hash value $R = H(id)$ and randomly choose two polynomials $f(x), \overline{f}(x)$ of degree 1 from $\mathbb{Z}_n[x]$. Also, calculate

$$g(x) = f(x)^2 \bmod (x^2 - R) \quad \text{and} \quad \overline{g}(x) = \overline{f}(x)^2 \bmod (x^2 - uR).$$

Return the ciphertext $C = (y^m \cdot g(x), y^m \cdot \overline{g}(x))$.

Dec(pp, r, C): On input pp, a secret key r and a ciphertext $C = (c(x), \overline{c}(x))$, compute

$$m' = \begin{cases} J_n(c(r)) & \text{if } r^2 \equiv H(id) \bmod n; \\ J_n(\overline{c}(r)) & \text{otherwise.} \end{cases}$$

Remark 2. Although Zhao *et al.*'s IBE scheme is not anonymous [24], it can be made so by using the anonymization technique described in [9, 10].

3 Computational Efficient IBE

In this section, we present an efficient method for generating the random t values used in Cocks' IBE. Although the method employed is elementary, it is worth noting that all the papers built upon Cocks' work, generate t values until the Jacobi symbol reaches the desired value.

3.1 Cocks' IBE Efficient Version

We further present the proposed encryption algorithm. To make the proposed scheme work, we incorporate a public element $e \in \mathbb{Z}_n \setminus J_n$ into the setup algorithm. Note that the t values can be interpreted as a Goldwasser-Micali ciphertext [16].

Enc(pp, id, m): On inputting pp, an identity id and a message $m \in \{-1, 1\}$, compute the hash value $R = H(id)$ and randomly choose two values $x_1, x_2 \xleftarrow{\$} \mathbb{Z}_n$. Set $t_i \equiv e^{(1-m)/2} x_i^2 \bmod n$ for $i \in \{1, 2\}$. Also, calculate

$$c_1 = t_1 + \frac{R}{t_1} \bmod n \quad \text{and} \quad c_2 = t_2 + \frac{uR}{t_2} \bmod n.$$

Return the ciphertext $C = (c_1, c_2)$.

3.2 Performance Analysis

To determine the efficiency of our proposal, we consider the following complexities for μ-bit integers

- Multiplication [17]: $M(\mu) = \mathcal{O}(\mu \log \mu)$,
- Jacobi symbol [8]: $\mathcal{O}(M(\mu) \log \mu)$.

Without loss of generality, we further assume that $p \bmod 8 \leq q \bmod 8$. To further accelerate the encryption process, we can select e as follows

$$e = \begin{cases} -1 & p \equiv -q \bmod 4, \\ 2 & p \equiv 1 \bmod 8 \text{ and } q \equiv 5 \bmod 8, \\ 2 & p \equiv 3 \bmod 8 \text{ and } q \equiv 7 \bmod 8, \\ \bar{e} & \text{otherwise}, \end{cases}$$

where $\bar{e}$ is random element from $\mathbb{Z}_n \setminus J_n$. Therefore, generating t values comes down to

$$t = \begin{cases} n - x^2 & e = -1, \\ x^2 + x^2 & e = 2, \\ \bar{e}x^2 & \text{otherwise}. \end{cases}$$

In the original scheme, generating a t value amounts to computing at least an Jacobi symbol. Therefore, we obtain a complexity of at least $\mathcal{O}(M(2\lambda)\log 2\lambda)$. In our proposal, we obtain the following complexity

$$\begin{cases} \mathcal{O}(M(2\lambda)) & e = -1, \\ \mathcal{O}(M(2\lambda)) & e = 2, \\ \mathcal{O}(2M(2\lambda)) & \text{otherwise}. \end{cases}$$

We further provide the reader with benchmarks for Cocks' original scheme and for our proposal. We ran the encryption algorithm for both schemes on a CPU Intel i7-8700 3.20 GHz and used GCC to compile it (with the O3 flag activated for optimization). Note that for all computations we used the GMP library [1]. To calculate the running times we used the native C++ function *clock()*. To obtain the average running time in seconds we chose to encrypt 1000 128/192/256-bit messages. According to NIST [3], the modules of size 3072/7680/15360 offer 128/192/256-bit security. Therefore, we wanted to simulate a key distribution scenario.

The results are provided in Table 1. Please take note that the percentages represent the time improvement relative to the original version. We can clearly see that our proposal significantly reduces encryption time by at least 50%.

4 Space Efficient IBEs

In [19], the author introduces a variant of Cocks' IBE that allows one to derive the encryption of $-m$ from the original ciphertext. Additionally, the author presents a bandwidth-saving approach for this variant. In this section, we show that this technique can be easily adapted to Cocks' and Zhao *et al.*'s IBE schemes.

We further impose the restriction $p \equiv q \bmod 4$. This implies that $J_p(-1) = J_q(-1)$, and therefore $J_n(-1) = 1$. Using this restriction, we are able to restrict the ciphertexts interval from $\{1, \ldots, n-1\}$ to $\{1, \ldots, (n-1)/2\}$.

Key Length	Original			Proposal		
	$e=-1$	$e=2$	$e=\bar{e}$	$e=-1$	$e=2$	$e=\bar{e}$
128 bits	27.2190	23.1005	25.9760	10.1901 (62.56%)	8.55514 (62.96%)	10.1151 (61.06%)
192 bits	118.701	114.695	115.931	50.6101 (57.36%)	48.9982 (57.28%)	52.1820 (54.99%)
256 bits	360.541	355.493	354.617	167.129 (53.64%)	164.818 (53.63%)	173.592 (51.04%)

Table 1. Average Encryption Time (ms)

4.1 Cocks' IBE Compact Version

We remind the reader that Cocks' ciphertext takes the following form

$$c_1 = t_1 + \frac{R}{t_1} \bmod n \quad \text{and} \quad c_2 = t_2 + \frac{uR}{t_2} \bmod n.$$

We can see that

$$\begin{aligned} J_n(-c_1 + 2r) &= J_n(-t_1 - R \cdot t_1^{-1} + 2r) = \\ &= J_n(-(t_1 - r)^2 \cdot t_1^{-1}) = J_n(t_1), \end{aligned}$$

and $J_n(-c_2 + 2r) = J_n(t_2)$. Thus, the decryption algorithm works as intended with any ciphertexts of the form $(\pm c_1, \pm c_2)$. Therefore, we propose the following encryption algorithm aimed at minimizing the bandwith overhead.

Enc(pp, id, m): On inputting pp, an identity id and a message $m \in \{-1, 1\}$, compute the hash value $R = H(id)$ and randomly choose two values $t_1, t_2 \xleftarrow{\$} \mathbb{Z}_n$ such that $J_n(t_1) = J_n(t_2) = m$. Also, calculate

$$c_1' = t_1 + \frac{R}{t_1} \bmod n \quad \text{and} \quad c_2' = t_2 + \frac{uR}{t_2} \bmod n.$$

Define

$$c_1 = \min(c_1', n - c_1') \quad \text{and} \quad c_2 = \min(c_2', n - c_2'),$$

and return the ciphertext $C = (c_1, c_2)$.

Remark 3. Remark that the technique outlined in this section does not interfere with the security proofs of Cocks' IBE provided in [15, 19]. Furthermore, the methods of anonymization outlined in [2, 19–21] can be effectively applied to this variant as well.

4.2 Zhao *et al.*'s IBE Compact Version

Using the trick presented in Section 4.1, we can also make Zhao *et al.*'s IBE scheme more compact. Let $f(x) = a \cdot x + b$ and $\overline{f}(x) = \overline{a} \cdot x + \overline{b}$. When we compute $c(x)$ and $\overline{c}(x)$ we obtain

$$c(x) = c_0 \cdot x + c_1 = [2y^m a] \cdot x + [y^m(a^2R + b^2)]$$
$$\overline{c}(x) = \overline{c}_0 \cdot x + \overline{c}_1 = [2y^m \overline{a}] \cdot x + [y^m(\overline{a}^2 uR + \overline{b}^2)]$$

Therefore, when $r^2 \equiv H(id) \bmod n$ we obtain that

$$\begin{aligned}
J_n(c_0 \cdot r + c_1) &= J_n(y^m \cdot (2ar + a^2R + b^2)) = J_n(y^m \cdot (ar + b)^2) = J_n(y)^m, \\
J_n(c_0 \cdot r - c_1) &= J_n(y^m \cdot (2ar - a^2R - b^2)) = J_n(-y^m \cdot (ar - b)^2) = J_n(y)^m, \\
J_n(-c_0 \cdot r + c_1) &= J_n(y^m \cdot (-2ar + a^2R + b^2)) = J_n(y^m \cdot (ar - b)^2) = J_n(y)^m, \\
J_n(-c_0 \cdot r - c_1) &= J_n(y^m \cdot (-2ar - a^2R - b^2)) = J_n(-y^m \cdot (ar + b)^2) = J_n(y)^m,
\end{aligned}$$

since $J_n(-1) = 1$. Similarly, for the case $r^2 \equiv uH(id) \bmod n$ we obtain

$$J_n(\overline{c}_0 \cdot r + \overline{c}_1) = J_n(\overline{c}_0 \cdot r - \overline{c}_1) = J_n(-\overline{c}_0 \cdot r + \overline{c}_1) = J_n(-\overline{c}_0 \cdot r - \overline{c}_1).$$

Hence, the decryption algorithm works as intended with either of the following ciphertext versions

$$(\pm c_0 \cdot x \pm c_1, \pm \overline{c}_0 \cdot x \pm \overline{c}_1).$$

Therefore, we can use the following encryption algorithm to save bandwith.

Enc(pp, id, m): On inputting pp, an identity id and a message $m \in \{0, 1\}$, compute the hash value $R = H(id)$ and randomly chooses two polynomials $f(x), \overline{f}(x)$ of degree 1 from $\mathbb{Z}_n[x]$. Also, calculate

$$g(x) = f(x)^2 \bmod (x^2 - R) \quad \text{and} \quad \overline{g}(x) = \overline{f}(x)^2 \bmod (x^2 - uR)$$

and let

$$(c'_0 \cdot x + c'_1, \overline{c}'_0 \cdot x + \overline{c}'_1) = (y^m \cdot g(x), y^m \cdot \overline{g}(x)).$$

Define

$$\begin{aligned}
c_0 &= \min(c'_0, n - c'_0) \quad \text{and} \quad c_1 = \min(c'_1, n - c'_1) \\
\overline{c}_0 &= \min(\overline{c}'_0, n - \overline{c}'_0) \quad \text{and} \quad \overline{c}_1 = \min(\overline{c}'_1, n - \overline{c}'_1),
\end{aligned}$$

and return the ciphertext $C = (c_0 \cdot x + c_1, \overline{c}_0 \cdot x + \overline{c}_1)$.

Remark 4. Note that this space-saving technique does not interfere with the security proof of Zhao *et al.*'s IBE provided in [24]. Additionally, the anonymization technique described in [9, 10] can also be applied to this version.

5 Conclusion

In this paper, we have introduced a method for accelerating the Cocks IBE scheme. Additionally, through the application of elementary operations, we managed to reduce the bandwidth requirements of both the Cocks and Zhao *et al.* IBEs.

References

1. The GNU Multiple Precision Arithmetic Library. https://gmplib.org/
2. Ateniese, G., Gasti, P.: Universally Anonymous IBE Based on the Quadratic Residuosity Assumption. In: CT-RSA 2009. Lecture Notes in Computer Science, vol. 5473, pp. 32–47. Springer (2009)
3. Barker, E.: NIST SP800-57 Recommendation for Key Management, Part 1: General. Tech. rep., NIST (2016)
4. Barua, R., Jhanwar, M.P.: On the Number of Solutions of the Equation $Rx^2+Sy^2 = 1 \pmod{N}$. The Indian Journal of Statistics **72-A**, 226–236 (2010)
5. Boneh, D., Crescenzo, G.D., Ostrovsky, R., Persiano, G.: Public Key Encryption with Keyword Search. In: EUROCRYPT 2004. Lecture Notes in Computer Science, vol. 3027, pp. 506–522. Springer (2004)
6. Boneh, D., Franklin, M.K.: Identity-Based Encryption from the Weil Pairing. In: CRYPTO 2001. Lecture Notes in Computer Science, vol. 2139, pp. 213–229. Springer (2001)
7. Boneh, D., Gentry, C., Hamburg, M.: Space-efficient Identity Based Encryption Without Pairings. In: FOCS 2007. pp. 647–657. IEEE Computer Society (2007)
8. Brent, R.P., Zimmermann, P.: An $O(M(n)\log n)$ Algorithm for the Jacobi Symbol. In: ANTS-IX. Lecture Notes in Computer Science, vol. 6197, pp. 83–95. Springer (2010)
9. Clear, M., Hughes, A., Tewari, H.: Homomorphic Encryption with Access Policies: Characterization and New Constructions. In: AFRICACRYPT 2013. Lecture Notes in Computer Science, vol. 7918, pp. 61–87. Springer (2013)
10. Clear, M., Tewari, H., McGoldrick, C.: Anonymous IBE from Quadratic Residuosity with Improved Performance. In: AFRICACRYPT 2014. Lecture Notes in Computer Science, vol. 8469, pp. 377–397. Springer (2014)
11. Cocks, C.: An Identity Based Encryption Scheme Based on Quadratic Residues. In: IMACC 2001. Lecture Notes in Computer Science, vol. 2260, pp. 360–363. Springer (2001)
12. Cotan, P., Teşeleanu, G.: Generalized Galbraith's Test: Characterization and Applications to Anonymous IBE Schemes. Mathematics **9**(11), 1184 (2021)
13. Elashry, I., Mu, Y., Susilo, W.: An Efficient Variant of Boneh-Gentry-Hamburg's Identity-Based Encryption Without Pairing. In: WISA 2014. Lecture Notes in Computer Science, vol. 8909, pp. 257–268. Springer (2014)
14. Elashry, I., Mu, Y., Susilo, W.: Jhanwar-Barua's Identity-Based Encryption Revisited. In: NSS 2014. Lecture Notes in Computer Science, vol. 8792, pp. 271–284. Springer (2014)
15. Goldwasser, S.: Cocks' IBE scheme, bilinear maps. MIT Lecture Notes: "6876: Advanced Cryptography" (2004)
16. Goldwasser, S., Micali, S.: Probabilistic Encryption. Journal of Computer and System Sciences **28**, 270–299 (1984)

17. Harvey, D., Van Der Hoeven, J.: Integer Multiplication in Time $\mathcal{O}(n \log n)$. Annals of Mathematics **193**(2), 563–617 (2021)
18. Jhanwar, M.P., Barua, R.: A Variant of Boneh-Gentry-Hamburg's Pairing-Free Identity Based Encryption Scheme. In: Inscrypt 2008. Lecture Notes in Computer Science, vol. 5487, pp. 314–331. Springer (2008)
19. Joye, M.: Identity-Based Cryptosystems and Quadratic Residuosity. In: PKC 2016. Lecture Notes in Computer Science, vol. 9614, pp. 225–254. Springer (2016)
20. Nica, A.M., Ţiplea, F.L.: On Anonymization of Cocks' Identity-based Encryption Scheme. Computer Science Journal of Moldova **81**(3), 283–298 (2019)
21. Schipor, A.G.: On the Anonymization of Cocks IBE Scheme. In: BalkanCryptSec 2014. Lecture Notes in Computer Science, vol. 9024, pp. 194–202. Springer (2014)
22. Schipor, A.G.: On the Security of Jhanwar-Barua Identity-Based Encryption Scheme. In: SecITC 2018. Lecture Notes in Computer Science, vol. 11359, pp. 368–375. Springer (2018)
23. Shamir, A.: Identity-Based Cryptosystems and Signature Schemes. In: CRYPTO 1984. Lecture Notes in Computer Science, vol. 196, pp. 47–53. Springer (1985)
24. Zhao, X., Cao, Z., Dong, X., Zheng, J.: Anonymous IBE from Quadratic Residuosity with Fast Encryption. In: ISC 2020. Lecture Notes in Computer Science, vol. 12472, pp. 3–19. Springer (2020)