DOI: 10.19884/j.1672-5220.202405005

Some Remarks on Cocks' Identity-Based Encryption Scheme

ZHAO Xiaopeng *
School of Computer Science and Technology, Donghua University, Shanghai 201620, China

Abstract: The theory of quadratic residues plays an important role in cryptography. In 2001, Cocks developed an identity-based encryption (IBE) scheme based on quadratic residues, resolving Shamir's 17-year-old open problem. However, a notable drawback of Cocks' scheme is the significant expansion of the ciphertext, and some of its limitations have been addressed in subsequent research. Recently, Cotan and Teşeleanu highlighted that previous studies on Cocks' scheme relied on a trial-and-error method based on Jacobi symbols to generate the necessary parameters for the encryption process. They enhanced the encryption speed of Cocks' scheme by eliminating this trial-and-error method. Based on security analysis, this study concludes that the security of Cotan-Teşeleanu's proposal cannot be directly derived from the security of the original Cocks' scheme. Furthermore, by adopting the Cotan-Teşeleanu method and introducing an additional variable as a public element, this study develops a similar enhancement scheme that not only accelerates the encryption speed but also provides security equivalent to the original Cocks' scheme.

Key words: identity-based encryption (IBE); quadratic residue; security; Cocks' IBE scheme
CLC number: TP309.7 **Document code**: A
Article ID: 1672-5220(2024)04-0447-04

Open Science Identity (OSID)

0 Introduction

In 1984, Shamir[1] proposed the concept of an identity-based cryptosystem in his paper. However, this initial work did not directly result in a complete identity-based encryption (IBE) scheme; instead, it laid the foundations for subsequent research. In 2001, Boneh et al.[2] introduced the first practical IBE scheme using bilinear pairings, while Cocks[3] constructed the first practical IBE scheme based on quadratic residues.

The Cocks' IBE scheme processes messages bit-by-bit, encrypting 1 bit of plaintext into a pair of large integers. Therefore, it results in significant ciphertext expansion. On the other hand, Cocks' IBE scheme offers some advantages, including efficient encryption and decryption, security based on standard cryptographic assumptions, and support for additive homomorphism[4]. Therefore, it can be applied in scenarios involving small messages, such as electronic voting, auction systems, and private information retrieval.

This paper focuses on the elementary method to accelerate Cocks' encryption process proposed by Cotan and Teşeleanu[5]. They noted that all previous papers dealing with Cocks' IBE scheme have relied on a trial-and-error method based on Jacobi symbols to generate the values which are required by Cocks' encryption algorithm. This study analyzes the security of this method and presents a similar method for accelerating Cocks' IBE scheme without compromising its security proof. This study also provides the reader with benchmarks for Cocks' original scheme, the proposed algorithm and Zhao et al.'s IBE scheme[6].

The rest of the paper is organized as follows. In Section 1, the background knowledge on Cocks' IBE scheme is introduced. In Section 2, the security of Cotan and Teşeleanu's method for enhancing Cocks' encryption is analyzed, and the proposed algorithm is described, which is proven secure without affecting efficiency. In Section 3, the performance of encryption algorithms that are relevant are evaluated. Conclusions are then drawn in Section 4.

1 Preliminaries

This section begins with introducing some mathematical notations and definitions, then moves on to discussing the Cocks' IBE scheme and its security.

1.1 Notations

For a set X, write $x \xleftarrow{R} X$ for the process of sampling an element x from X uniformly at random. For any algorithm $\mathcal{A}$, write $x \leftarrow \mathcal{A}(y)$ to mean the operation of running $\mathcal{A}$ on input y, and obtaining the output x. Let N be the product of two Rivest-Shamir-Adleman (RSA) primes p and q. The Jacobi symbol of an integer a modulo

Received date: 2024-05-15
Foundation items: Rising-Star Program of Shanghai 2023 Science and Technology Innovation Action Plan (Yangfan Special Project), China (No. 23YF1401000); Fundamental Research Funds for the Central Universities, China (No. 2232022D-25)
* Correspondence should be addressed to ZHAO Xiaopeng, email: zxp@dhu.edu.cn
Citation: ZHAO X P. Some remarks on cocks' identity-based encryption scheme[J]. *Journal of Donghua University (English Edition)*, 2024, 41(4): 447-450.

n is represented by (a/n). Let $Q_N = \{x^2 \mid x \in Z_N^*\}$ be the set of quadratic residues in the multiplicative group $Z_N^* = \{a \in \{0, 1, \cdots, N\} \mid \gcd(a, N) = 1\} \bmod N$. Let $J_N = \{x \in Z_N^* \mid (x/N) = 1\}$ denote the set of elements in Z_N (the set of the integers modulo N) whose Jacobi symbol with respect to N is 1.

1.2 IBE scheme

An IBE scheme consists of the following four probabilistic polynomial time (PPT) algorithms.

1) $Setup(\kappa)$

The setup algorithm *Setup* takes as input a security parameter κ, and returns a master key pair (m_{pk}, m_{sk}), where m_{pk} denotes the master public key and m_{sk} denotes the master secret key. The message space is denoted by M.

2) $KeyGen(m_{pk}, m_{sk}, i_d)$

The key generation algorithm *KeyGen* takes as input the master key pair (m_{pk}, m_{sk}) and an identity i_d. It returns the secret key s_{id} associated with an identity i_d.

3) $Enc(m_{pk}, i_d, m)$

The encryption algorithm *Enc* takes as input m_{pk}, i_d, and a message $m \in M$. It returns a ciphertext C.

4) $Dec(m_{pk}, s_{id}, C)$

The decryption algorithm *Dec* takes as input m_{pk}, s_{id} and C for i_d. It returns a message m when C is a valid ciphertext, or outputs $\perp$ to denote the failure.

Correctness. Given any i_d and all messages $m \in M$, the correctness property requires that $Dec(m_{pk}, s_{id}, C \leftarrow Enc(m_{pk}, i_d, m)) = m$.

1.3 Cocks' IBE scheme

Cocks[3] constructed the first IBE scheme based on the quadratic residuosity assumption (QRA) in 2001, thus solving the open problem proposed by Shamir[1] that has lasted for 17 years. Cocks's IBE scheme does not satisfy anonymity due to the Galbraith's test[7]. As a result, researchers have proposed different methods to solve this problem[4,8-9]. For example, in 2016, Joye[4] proposed an anonymous variant based on cyclotomic polynomials and algebraic torus. This variant is comparable to the Cocks's IBE scheme in terms of both efficiency and ciphertext expansion. Here gives its extended version based on the details provided in Ref.[4] (the original scheme only considers prime numbers $p \equiv q \equiv 3 \pmod 4$).

1) $Setup(\kappa)$

Given a security parameter κ, generate two κ-bit RSA primes p, q and compute their product $N = pq$. Sample an element $u \xleftarrow{R} J_N \backslash Q_N$. The public parameters are $mpk = \{N, u, H\}$, where H is $\{0,1\}^* \rightarrow J_N$, a publicly available cryptographic hash function mapping an arbitrary binary string to the set J_N. The master secret key is $m_{sk} = \{p, q\}$.

2) $KeyGen(m_{pk}, m_{sk}, i_d)$

Set $R_{id} = H(i_d)$. If $R_{id} \in Q_N$, then compute $r_{id} = R_{id}^{\frac{1}{2}} \bmod N$; otherwise compute $r_{id} = (uR_{id})^{\frac{1}{2}} \bmod N$. Return $s_{id} = \{r_{id}\}$ as user i_d's private key.

3) $Enc(m_{pk}, i_d, m)$

On inputting m_{pk}, an identity i_d and a message $m \in \{-1, 1\}$, derive the hash value $R_{id} = H(i_d)$. Choose at random two values t_1, $t_2 \xleftarrow{R} Z_N$ such that $(t_1/N) = (t_2/N) = m$. Calculate $c_1 = t_1 + R_{id}/t_1 \bmod N$ and $c_2 = t_2 + uR_{id}/t_2 \bmod N$. Return the ciphertext $C = (c_1, c_2)$.

4) $Dec(m_{pk}, s_{id}, C)$

On inputting m_{pk}, a secret key $s_{id} = \{r_{id}\}$ and a ciphertext $C = (c_1, c_2)$, compute and return the message

$$m = \begin{cases} \left(\dfrac{c_1 + 2r_{id}}{N}\right), & \text{if } r_{id}^2 \equiv H(i_d) \pmod N; \\ \left(\dfrac{c_2 + 2r_{id}}{N}\right), & \text{otherwise.} \end{cases}$$

1.4 Complexity assumption

It is well-known that Cocks' IBE scheme is semantically secure under the QRA in the random oracle model, whose definition is explicitly presented as follows.

Definition 1 (QRA)

Given a security parameter κ, let $RSAGen(\kappa)$ be a polynomial-time algorithm that generates two κ-bit RSA primes p, q and compute their product $N = pq$. The QRA relative to $RSAGen(\kappa)$ asserts that the advantage

$$Adv^{QRA}_{\mathcal{A},RSAGen}(\kappa) = |Pr[\mathcal{A}(N,x) = 1 \mid x \xleftarrow{R} Q_N] - Pr[\mathcal{A}(N,x) = 1 \mid x \xleftarrow{R} J_N \backslash Q_N]|$$

is negligible for any PPT adversary $\mathcal{A}$, where in each case the probabilities $Pr[\cdot]$ are taken over the experiment of running $(N,p,q) \leftarrow RSAGen(\kappa)$, x is chosen uniformly from Q_N and $J_N \backslash Q_N$, respectively.

2 Cocks' IBE Scheme with Efficient Encryption

2.1 Cotan and Teşeleanu's method for enhancing Cocks' encryption

Recall that the encryption algorithm in Cocks' IBE scheme should choose at random two values $t_1, t_2 \xleftarrow{R} Z_N$ such that $(t_1/N) = (t_2/N) = m$. In a recent paper by Cotan and Teşeleanu[5], the authors noted that all the papers based on Cocks' IBE scheme produced multiple values until the Jacobi symbol was m, and presented the following improved encryption algorithm, where $e \in Z_N \backslash J_N$ should be chosen as a public element in the Setup phase. The authors also remarked that $t_i (i = 0,1)$ could be interpreted as a Goldwasser-Micali ciphertext.

$Enc(m_{pk}, i_d, m)$ algorithm is as follows.

On inputting m_{pk}, an identity id and a message $m \in \{-1, 1\}$, derive the hash value $R_{id} = H(i_d)$.

Choose at random two values x_1, $x_2 \xleftarrow{R} Z_N$.

Set $t_i \equiv e^{\frac{1-m}{2}} x_i^2 \bmod N$ for $i \in \{0,1\}$.

Calculate $c_1 = t_1 + R_{\mathrm{id}}/t_1 \bmod N$ and $c_2 = t_2 + uR_{\mathrm{id}}/t_2 \bmod N$.

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

2.2 Security analysis

Cotan and Teşeleanu did not give the security proof of their proposal in the paper. Note that $t_i \in eQ_N$ if $m = -1$ and $t_i \in Q_N$ if $m = 1$, thus the range of t_i is only half of the set $\{t \in Z_N^* \mid (t/N) = m\}$ for $m \in \{-1, 1\}$. Therefore, one cannot directly apply the security proof of Cocks' IBE scheme. In fact, providing the security proof for Cotan and Teşeleanu's proposal is quite complex; it is associated with the distribution of the Jacobi symbols modulo N in the sets $\{t \in eQ_N \mid t + R/t\}$ and $\{t \in Q_N \mid t + R/t\}$ for some fixed $R \in Q_N$.

2.3 The proposed Cocks' efficient encryption algorithm

In light of the above analysis, this study proposes an improved method that can be easily proven secure. In the Setup phase, the system chooses e_1, e_2 as public elements such that $e_1 \in Z_N \backslash J_N$ and $e_2 \in J_N \backslash Q_N$. The master public key $m_{\mathrm{pk}} = \{N, u, e_1, e_2, H\}$, where $u \xleftarrow{R} J_N \backslash Q_N$. The proposed Cocks' efficient encryption algorithm $Enc(m_{\mathrm{pk}}, i_{\mathrm{d}}, m)$ is as follows.

On inputting m_{pk}, an identity i_{d} and a message $m \in \{-1, 1\}$, derive the hash value $R_{\mathrm{id}} = H(i_{\mathrm{d}})$.

Choose at random two values x_1, $x_2 \xleftarrow{R} Z_N$.

Set $t_i \equiv e_1^{\frac{1-m}{2}} e_2^j x_i^2 \bmod N$ for $i \in \{0,1\}$ and $j \xleftarrow{R} \{0,1\}$.

Calculate $c_1 = t_1 + R_{\mathrm{id}}/t_1 \bmod N$ and $c_2 = t_2 + uR_{\mathrm{id}}/t_2 \bmod N$.

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

Assume that $p \bmod 8 \leqslant q \bmod 8$. To accelerate the encryption process, (e_1, e_2) can be selected as

$$(e_1, e_2) = \begin{cases} (-1, 2), & \text{if } p \equiv 3 \pmod 8 \text{ and } q \equiv 5 \pmod 8; \\ (2, -1), & \text{if } p \equiv 3 \pmod 8 \text{ and } q \equiv 7 \pmod 8; \\ (-1, -2), & \text{if } p \equiv 5 \pmod 8 \text{ and } q \equiv 7 \pmod 8; \\ \text{random}, & \text{otherwise.} \end{cases}$$

Therefore, the complexity of the proposed algorithm's encryption is

$$\begin{cases} O(M(\kappa)), & \text{if } p \equiv 3 \pmod 8 \text{ and } q \equiv 5 \pmod 8; \\ O(M(\kappa)), & \text{if } p \equiv 3 \pmod 8 \text{ and } q \equiv 7 \pmod 8; \\ O(M(\kappa)), & \text{if } p \equiv 5 \pmod 8 \text{ and } q \equiv 7 \pmod 8; \\ O(3M(\kappa)), & \text{otherwise,} \end{cases}$$

where $M(\kappa)$ denotes the time to multiply κ-bit numbers.

In the above algorithm, the range of $t_i (i = 0,1)$ is exactly the set $\{t \in Z_N^* \mid (t/N) = m\}$ for $m \in \{-1, 1\}$. Hence, by the proof of Lemma 1 in Ref. [4], the following theorem can be obtained.

Theorem 1 Let $C = (c_1, c_2)$ be the ciphertext generated as above. If $H(i_{\mathrm{d}}) \notin Q_N$, then the component c_1 corresponds with the same probability to the encryption of message $m = 1$ or $m = -1$. On the other hand, if $u\,H(i_{\mathrm{d}}) \notin Q_N$, then the component c_2 corresponds with the same probability to the encryption of message $m = 1$ or $m = -1$.

By Theorem 1, the technique outlined in this section does not interfere with the security proof of Cocks' IBE scheme provided in Appendix A of Ref. [4].

3 Performance Comparison

This study evaluated the encryption algorithms for Cocks' original scheme[3], the proposed algorithm and Zhao et al.'s IBE scheme[6] on a single personal computer using the GMP library (version 6.2.1) for large number operations. The development environment was Visual Studio 2022. It chose to encrypt 100 000 messages, each with a key length of 128, 192 and 256 bits, respectively. According to the data in the National Institute of Standards and Technology (NIST)[10], the RSA modules with the sizes of 3 072, 7 680 and 15 360 offer 128, 192 and 256 bits security, respectively. The results are provided in Table 1.

From Table 1, it can be seen that the proposed algorithm's encryption is nearly 2 times faster than that of the original Cocks' scheme. Zhao et al.'s IBE scheme improves the encryption speed of the original Cocks' scheme by approximately 5 times by omitting the computation of the Jacobi symbol and the modular multiplicative inverse in Cocks' encryption, albeit at the expense of doubling the length of the ciphertext.

Table 1 Average encryption time of different methods

Key length/bit	Average encryption time/ms		
	Original Cocks' scheme	Proposed algorithm	Zhao et al.'s IBE scheme
128	32.458 2	12.920 3	6.184 9
192	113.345 0	51.075 8	22.210 6
256	392.351 0	190.633 0	82.061 1

4 Conclusions

This study analyzes the security of the scheme proposed by Cotan and Teşeleanu, and presents a similar method for accelerating Cocks' IBE scheme without compromising its security proof. This study also provides the reader with benchmarks for the original Cocks'

scheme, the proposed algorithm and Zhao et al.'s IBE scheme. The results show that the proposed algorithm's encryption is nearly 2 times faster than that of the original Cocks' scheme.

References

[1] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Advances in Cryptology (CRYPTO 1984). Berlin: Springer, 1985: 47-53.

[2] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]//Advances in Cryptology (CRYPTO 2001). Berlin: Springer, 2001: 213-229.

[3] COCKS C. An identity based encryption scheme based on quadratic residues[C]//The 8th IMA international conference on cryptography and coding. Berlin: Springer, 2001: 360-363.

[4] JOYE M. Identity-based cryptosystems and quadratic residuosity [C]//Public-Key Cryptography (PKC 2016). Berlin: Springer, 2016: 225-254.

[5] COTAN P, TEŞELEANU G. Elementary remarks on some quadratic based identity based encryption schemes[C]//The 16th International Conference on Information Technology and Communications Security (SecITC 2023). Cham: Springer, 2024: 26-34.

[6] ZHAO X P, CAO Z F, DONG X L, et al. Anonymous IBE from quadratic residuosity with fast encryption [C]//The 23rd International Conference on Information Security (ISC 2020). Cham: Springer, 2020: 3-19.

[7] BONEH D, DI CRESCENZO G, OSTROVSKY R, et al. Public key encryption with keyword search [C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2004: 506-522.

[8] ATENIESE G, GASTI P. Universally anonymous IBE based on the quadratic residuosity assumption[C]//Cryptographers' Track at the RSA Conference 2009. Berlin: Springer, 2009: 32-47.

[9] CLEAR M, TEWARI H, MCGOLDRICK C. Anonymous IBE from quadratic residuosity with improved performance [C]//International Conference on Cryptology in Africa. Cham: Springer, 2014: 377-397.

[10] BARKER E B, BARKER W C, BURR W E, et al. Recommendation for key management, part 1: general (revised)[EB/OL]. (2007-03-01)[2024-04-01]. https://www.nist.gov/publications/recommendation-key-management-part-1-general-revised-march-2007-edition.

关于 Cocks 基于身份的加密方案的评述

赵晓鹏*

东华大学 计算机科学与技术学院，上海 201620

摘　要：二次剩余在密码学中扮演着重要的角色。2001 年 Cocks 基于二次剩余设计了一种基于身份的加密方案，解决了 Shamir 长达 17 年的未解难题。然而，Cocks 方案存在密文扩张率大的显著问题。在后续工作中，其一些局限性得到了解决。最近，Cotan 和 Teşeleanu 指出，之前所有关于 Cocks 方案的论文都依赖于通过雅可比符号的试错来生成 Cocks 加密过程所需要的参数，他们通过避免这种试错来提高 Cocks 方案的加密速度。基于安全性分析，该文得出 Cotan-Teşeleanu 方案的安全性不能直接从原始 Cocks 方案的安全性导出的结论。同时在 Cotan-Teşeleanu 方案的基础上引入另外一个变量作为公共参数，设计了一种类似的改进方案。该方案不但可以提高 Cocks 加密速度，而且安全性与原始 Cocks 方案的安全性等价。

关键词：基于身份的加密；二次剩余；安全性；Cocks 基于身份的加密方案