

A subtree-based cryptographic protocol for secure group communication

Ismail Bahkali
Department of Information Science
King Abdulaziz University
Jeddah 21589
Saudi Arabia

Abstract

In the current study we introduce an improved identity-based cryptographic (IBC) scheme that aims at addressing the weaknesses of existing frameworks. In further extension of the approach of Meshram, Meshram, and Zhang [21], who formulated an IBC method based on integer-factorization problems and generalized discrete-logarithm without reference to bilinear pairings, this paper determines and removes the stalemate of their construction. Though the scheme proposed by Meshram, Meshram, and Zhang [21] offers protection of data and adversarial resistance, the confidentiality of the encryption mechanism is still on a condition of secret data available in the key authentication center, which is the resource that cannot be accessed by the end users. To overcome this drawback, we present an enhanced subtree-based cryptographic protocol of secure group communication which uses partial discrete logarithms in finite fields. This plan not only removes the problem of the deadlock but also provides security improvement to the solution of Pang, Li, and Wang [31] whose work was undermined by the lack of full security analysis. The scheme proposed incorporates a strong key-distribution design and is more robust to any attack that might occur and thus enhances the security and trustworthiness of identity-based cryptographic schemes.

Subject Classification (2020): 94A60, 11T7, 94A62.

Keywords: *Public key cryptography, Identity-based cryptosystem, Partial discrete logarithm, Security proof, Subtree.*

1. Introduction

In contemporary society, computer technologies and the use of the internet have become integral components of daily routines. The introduction of the Internet of Things (IoT) has played a major role in changing not just individual

ORCID-ID: 0000-0002-3603-4259

E-mail: Ibahkali@kau.edu.sa,
dr.ismailbahkali@gmail.com

life patterns but also the working processes since it has made the establishment of a well-linked interconnection between devices an easy task. Technological advancement, however, has brought about privacy and security concern of data especially with the nature of vulnerability of open and public networks which transfer sensitive information. The confidentiality of such data must be a top priority, and it will require the deployment of secure communication protocols. At the heart of this protocol lies the exchanges of secret keys of the sessions between entities, before encrypted communication. With the growth of users and devices in an exponential manner, the problem of distributing these keys effectively and safely has proven to be more complicated and requires innovative solutions.

The public-key cryptosystem has emerged as an effective solution to the problem of session key distribution in open network systems. Its robustness lies in facilitating verification of interlocutors' public keys, consequently engendering confidence in system-wide communications. A formal model of this authentication operation is the Public-Key Infrastructure (PKI) [36], but its mass use is hampered by the huge overhead of maintenance and administration of infrastructure. Nevertheless, PKI continues to be central to the process of secure communication, which underscores the need to have scalable and manageable key-distribution mechanisms.

Shamir [3] first proposed the Identity-Based Cryptosystem (IBC) in 1984 (see Fig. 1). In this framework, a user's personal identity details, for example, an email address serves as the public key for accessing the corresponding private key. By leveraging the public key as a directly verifiable form of user identity, the innovation effectively reduces authentication overhead [2]. This, in turn, facilitates more straightforward non-interactive session setups among the parties in communication. Although the approach by Shamir [3] proved to be useful in identity-based signatures schemes in their practical implementation, later developments have broadened its usage. It is important to mention that Boneh and Boyen [27] used the Weil pairing property to build a working Identity-Based Encryption (IBE) technique which was a breakthrough towards implementation. Nevertheless, their method of bilinear pairing makes it computationally inefficient with devices that have limited processing ability and therefore demonstrates the continuing difficulty of optimizing cryptographic schemes to run on resource-constrained devices.

Meshram, Meshram, and Zhang [21] suggested the improved version of Identity-based Cryptosystem (IBC) [16], [8], [15], [35], [5] based on the security based on the Integer factorization problem (IFP) and the Generalized Discrete logarithm problem (GDLP). In contrast to previous schemes, their implementation is noteworthy in the sense that they do not have bilinear pairings since they commonly can be very costly in terms of computation. The method is powerful in meeting the fundamental security goals because it ensures the privacy of data and the non-eavesdropping of the encrypted messages and the private keys of the user. The peculiarity of their system is that it is impossible to decrypt only with your own key but also with the help of a confidential part of the private information in the Key Authentication Centre (KAC), that is not known to users.

This means that though a user may have a private key, he/she is unable to decrypt ciphertexts without cooperating with KAC. Even though this two-way control system applies greater security in that it protects the data as well as the private keys, it has a deadlock issue, which poses a significant challenge when it comes to its practical implementation.

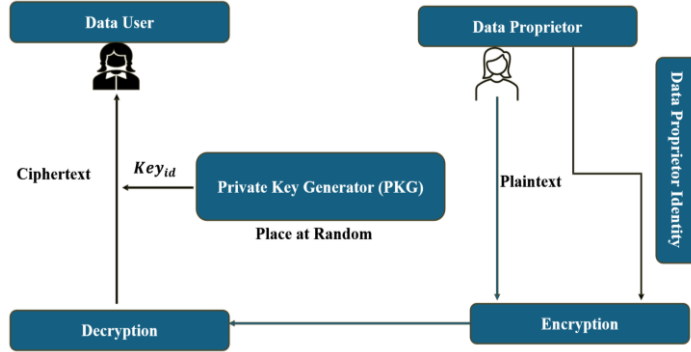


Figure 1
Identity-based Cryptographic Procedure

Pang, Li, and Wang [31] critically reviewed the scheme presented by Meshram et al. and found out that it has major flaws, with the most critical being that it has a deadlock issue. They found that the encryption operation of the approach used by Meshram et al. is based on the private information of the KAC that is not supposed to be exposed to users. This dependency therefore affects the ability of the users to perform encryption as intended thus compromising the usability of the system. Pang, Li, and Wang [31] suggested a better mechanism of eliminating the deadlock problem. However, although their work is heading towards the right direction, it does not have analytical rigor and formal security proof, which is necessary to warrant the soundness of the proposed solution.

The recent development in identity based cryptographic protocols has brought a wide extension of the protocols to the new computing environment. Meshram et al. [19] are significant contributors to this field because they showed groundwork in protocols of online/offline ID-based short signature (IBSS) that uses partial discrete logarithms in wireless sensor networks. Since this, they have gone further to construct transformation models of public-key cryptography and IBSS processes which employ long chaotic maps. Furthermore, Meshram and Meshram [17] and [10] suggested an effective IBE method, which integrates subtree framework and pairing exercises specific to the cloud computing systems to enable fuzzy user information sharing. To supplement them, Ramadan et al. [32] discussed IBE algorithms based on the RSA hypothesis and provided equality test mechanisms. Additional works by Meshram et al. [12] are the cryptosystems and short signature schemes transformation models which are applied to cryptosystems using chaotic maps deployed in cloud structures with the

ability to share fuzzy data. Continuing this field of research, Farjana et al. [33] proposed a new identity-based encryption algorithm aimed at providing safe information transmission to authenticated users, an algorithm that was proven with the help of its implementation in the fog computing environment.

Our contribution: Within the subtree, the cryptographic mechanism offers a novel algorithm built on the partial discrete logarithm (PDL) problem. It does so by making use of the unique properties of discrete exponentials in the multiplicative group of finite fields. A stronger key distribution mechanism is also introduced to augment the cryptographic system. The projected method tends to offer a more protected and effective IBC scheme compared to the models already existing including the one suggested by Pang, Li, and Wang [31], utilizing the hardness assumptions of PDL problem [20], [14], and [9].

Organization: The rest of the paper proceeds as follows: Section 2 reviews Meshram et al.'s IBC approach in detail, while Section 3 discusses the improved IBC proposed by Pang et al. In Section 4, the proposed secure subtree-based cryptosystem is presented and elaborated upon. Section 5 offers formal security proofs and a detailed analysis of the proposed technique. A comparative performance study, including evaluations of the existing IBC schemes, is presented in Section 6. Finally, Section 7 concludes the paper and suggests several directions for future research.

2. Background and Material

The security of our technique depends on the difficulty of solving the PDL problem in the group in which subtree-based cryptography is developed. We quickly go over the definitions [1], [19], [24], [34], and the notations used in the manuscript.

2.1 The Partial Discrete Logarithm (PDL)

We assume that $\mathcal{N} = q_1 p_1$ is a secure prime modulus. This indicates that p_1 and q_1 are primes such that $p_1 = (2p'_1 + 1)$ and $q_1 = (2q'_1 + 1)$, where q'_1 and p'_1 are also primes. Secure prime number arrangements of length ℓ are denoted by $S(\ell)$. The cyclic group of quadratic residues modulo $\mathcal{N}^2$ was $G = QR_{\mathcal{N}^2}$. The formula is $ord(G) = \frac{\lambda(\mathcal{N}^2)}{2} = p_1 p'_1 q_1 q'_1 = \frac{\mathcal{N} \lambda(\mathcal{N})}{2}$, where $\lambda(\mathcal{N}) = 2q'_1 p'_1$. In this group, the component's maximum order is $\frac{\mathcal{N} \lambda(\mathcal{N})}{2}$, and all the components of order $\mathcal{N}$ have the form $\alpha = (1 + k\mathcal{N})$.

Definition 1: (PDL): The Partial Discrete Logarithm (PDL) problem, as defined by Paillier [34], captures the difficulty of recovering a hidden exponent. Specifically, let g denote an element of maximal order in the group G , and suppose it satisfies the condition $g^{\lambda(\mathcal{N})} \equiv (1 + \mathcal{N}) \pmod{\mathcal{N}^2}$, which forces the parameter $k = 1$. Given such a g together with $z = g^a \pmod{\mathcal{N}^2}$ (where a is an unknown integer between 1 and the order of G), the PDL problem is the task of

finding $a \pmod{\mathcal{N}}$. This issue is anticipated to be challenging, particularly in the absence of modulus factorization, as indicated by the accompanying suspicion.

Assumption 1 (PDL over $\mathcal{Z}_{\mathcal{N}^2}^*$): A negligible function $\text{negl}()$ is one that, for any probabilistic polynomial-time (PPT) algorithm A , satisfies the condition of vanishing faster than any inverse polynomial for all sufficiently large security parameters ℓ .

$$\Pr \left[A(\mathcal{N}, g, \mathfrak{z}) = a \pmod{\mathcal{N}} \mid p_1, q_1 \leftarrow SP\left(\frac{\ell}{2}\right); \mathcal{N} = q_1 p_1; g \leftarrow G; a \leftarrow [1, \text{ord}(G)]; \mathfrak{z} \leftarrow g^a \pmod{\mathcal{N}^2} \right] = \text{negl}(\ell)$$

2.2 Notation

This novel IBC scheme leverages the PDL problem to enable fuzzy user data sharing while preserving protection requirements. Notation is as follows: $[y, z]$ denotes the integer interval $\{y, y+1, \dots, z\}$, and $[y]$ means $[1, y]$. For any identity id , let $S_{id} = \{id_1, \dots, id_k\}$ be its participant identity set, and let $I_{id} = \{i : id_i \in S_{\mathbb{T}}\}$ be its location records within the model's tree structure [25], [26], [37]. The expected recipients form a subtree which is characterized by a tree based, identity encryption scheme [11]. The identity vectors as well as the location of these receivers get included in the encryption scheme $\mathbb{T}$ in this hierarchical structure. Any valid $\mathbb{T}$ must include the root node thus representing the structural form of authority of the Private Key Generator (PKG) [13]. The suggested framework is likely to succeed in terms of enabling fuzzy entity data sharing, yet meeting the necessary protection standards, but it faces an issue of efficiency in terms of multi-receiver. The users are assumed to be interconnected in a tree-like structure, as depicted in Figure 2. When a message is sent by a data owner to a subset of receivers, who are members of a subtree, the identity set and positional indices associated will be represented by $S_{\mathbb{T}} = \{\mathcal{G}, \mathcal{F}, \mathcal{B}, \mathcal{A}\}$ and $I_{\mathbb{T}} = \{7, 6, 2, 1\}$, respectively. The higher-node set is stated as the set of superior nodes as: $\text{Sup}(\mathbb{T}) = \{(\mathcal{B}, \mathcal{G}), (\mathcal{B}, \mathcal{F}), (\mathcal{B}), (\mathcal{A})\}$ which represents the agreement of the user that the data owner wishes to express.

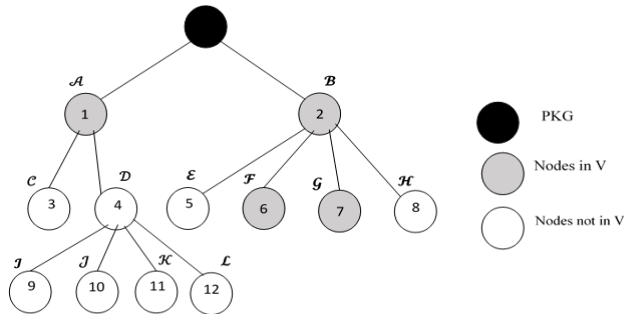


Figure 2
An example of subtree-based cryptographic structure

3. Review on Meshram et al. ID-based Cryptosystem (IBC)

Meshram, Meshram, and Zhang [21] proposed an IBC consisting of four interconnected sub-algorithms: Setup, Extraction, Encryption, and Decryption. Among these, the Setup algorithm is executed by the Key Authentication Center (KAC) and is responsible for generating both the public and private keys for the entire system. Prospective users initiate registration by submitting an application to the KAC, which then performs an extraction algorithm to generate unique private keys for users verified as legitimate. Before sending messages, users must authenticate their identities. If a user wishes to securely transmit a message, they utilize an Encryption algorithm to convert the plaintext into ciphertext. On the recipient's side, the decryption algorithm is employed to recover the original message, which requires possession of the receiver's private key [18], [22], [32]. This general structure aligns with the designs of most IBC schemes documented in literature.

Setup. KAC has taken the actions listed below:

- 1) Choose prime numbers randomly, p_1 and q_1 , such that $N = p_1 q_1$. Calculate the Euler-phi function $\varphi(N) = (p_1 - 1)(q_1 - 1)$ given bit number $n = |\mathcal{N}|$.
- 2) Choose two arbitrary integers, e_1 and d_1 , such that $e_1 d_1 \equiv 1 \pmod{\varphi(N)}$ and $1 \leq e_1, d_1 \leq \varphi(N)$ such that $\gcd(e_1, \varphi(N)) = 1$.
- 3) Create a n dimensional vector $\vec{a} = (a_1, a_2, a_3, \dots, a_n)$ over $Z_{\varphi(N)}^*$, with s. t. $1 \leq a_i \leq \varphi(N)$ and $(1 \leq i \leq n)$, and $a_i \neq a_j \pmod{\varphi(N)}$, $(i \neq j)$.
- 4) Estimate n dimensional vector $\vec{h} = (h_1, h_2, h_3, \dots, h_n)$, where

$$h_i = e_1^{a_i} \pmod{N}, (1 \leq i \leq n).$$
- 5) The private key in the KAC is the pair $(\vec{a}, d)$, and the public one is $(N, e_1, \vec{h})$. A fundamental requirement of the scheme is that every entity receives a copy of the public key, while each entity's private key must be kept strictly confidential.

Extraction. The KAC performs the above procedures in order to come up with the private key which is related to entity i . The identity of each entity is represented by a k -dimensional binary vector, defined as follows:

$$id_i = (x_{i1}, x_{i2}, x_{i3}, x_{i4}, \dots, x_{ik}), x_{ij} \in \{0, 1\}, (1 \leq j \leq k).$$

- 1) Calculate the entity i 's expanded id_i , $\mathcal{E}id_i$, as:

$$\mathcal{E}id_i = (id_i)^e \pmod{N} = (y_{i1}, y_{i2}, y_{i3}, y_{i4}, \dots, y_{it}), y_{ij} \in \{0, 1\}, (1 \leq j \leq t).$$
- 2) The secret key s_i for entity i is determined by computing the inner product of the vector $\vec{a}$ with the identifier $\mathcal{E}id_i$, expressed as follows:

$$s_i = \vec{a} \cdot \mathcal{E}id_i \pmod{\varphi(N)} = \sum_{1 \leq j \leq n} a_j y_{ij} \pmod{\varphi(N)}.$$

The id_i notation represents the public key of entity i .

Encryption: In the present study, we consider a theoretical scenario in which entity 2 wishes to transmit a message M to entity 1. To protect the secrecy of the message, entity 2 uses the encryption protocol that is relevant to the message M by applying the following encryption protocol to the message .

- 1) The expanded identifier of entity i , represented as Eid_i , is computed as follows:

$$\text{Eid}_i = (\text{id}_i)^e \pmod{\mathcal{N}} = (y_{11}, y_{12}, y_{13}, y_{14}, \dots, y_{1t}), y_{1j} \in \{0,1\}, (1 \leq j \leq t).$$

- 2) Calculating

$$\begin{aligned} \gamma_1 &= \prod_{1 \leq i \leq n} h_i^{y_{1i}} \pmod{\mathcal{N}} \\ &= \prod_{1 \leq i \leq n} (e^{a_i})^{y_{1i}} \pmod{\mathcal{N}} \\ &= e^{\sum_{1 \leq i \leq n} a_i y_{1i} \pmod{\varphi(\mathcal{N})}} \pmod{\mathcal{N}} \\ &= e^{s_1} \pmod{\mathcal{N}} \end{aligned}$$

Utilizing γ_1 alongside publicly available information $\vec{h}$ associated with the KAC, we proceed with the following steps:

- 3) Calculate $C_0 = M^{e^{s_1}} \pmod{\mathcal{N}}$.
- 4) Calculate the ciphertext $C = C_0^e \pmod{\mathcal{N}}$.

Decryption: To retrieve the message, the ciphertext, sent by entity 1 has gone through the above steps to retrieve the message, M :

- 1) Calculate $\gamma = C^d \pmod{\mathcal{N}}$.
- 2) Using their own secret key s_1 , the entity can recover the message M as follows:

$$\begin{aligned} \gamma^{d^{s_1}} \pmod{\mathcal{N}} &\equiv C_0^{d^{s_1}} \pmod{\mathcal{N}} \\ &\equiv (M^{e^{s_1}})^{d^{s_1}} \pmod{\mathcal{N}} \\ &\equiv M^{(ed)^{s_1}} \pmod{\mathcal{N}} \\ &\equiv M \pmod{\mathcal{N}}. \end{aligned}$$

4. Review of Pang et al. ID-based Cryptosystem (IBC)

Pang, Li, and Wang [31] suggested an identity based cryptographic (IBC) based on the generalized discrete logarithm problem (GDLP) and the integer-factorization problem (IFP). They have a methodology arranged into four separate sub-algorithms, which include Setup, Extraction, Encryption and Decryption.

Setup: The setup algorithm presented mentioned here is like the one outlined in Section 2, particularly with respect to computing the n -dimensional vector $\vec{h}$. Nevertheless, the salient deviations of the current formulation have been identified, and they are elaborated in the discussion below.

$$\vec{h} = (h_1, h_2, h_3, \dots, h_n), \text{ where } h_i = d^{a_i} \pmod{\mathcal{N}} (1 \leq i \leq n).$$

Extraction: The extraction algorithm used had significant similarities with that described in Section 2.

Encryption: Given that entity 2 wants to send a message M to entity 1. This is how entity 2 encrypts M :

- 1) To find the expanded id of entity i , which is called $\mathcal{E}\text{id}_i$, use the following formula is used:

$$\mathcal{E}\text{id}_i = (\text{id}_i)^e (\text{mod } \mathcal{N}) = (\mathcal{Y}_{11}, \mathcal{Y}_{12}, \mathcal{Y}_{13}, \mathcal{Y}_{14}, \dots, \mathcal{Y}_{1t}), \mathcal{Y}_{1j} \in \{0,1\}, (1 \leq j \leq t).$$

- 2) Estimated

$$\begin{aligned} \gamma &= \prod_{1 \leq i \leq n} h_i^{y_{1i}} (\text{mod } \mathcal{N}) \\ &= \prod_{1 \leq i \leq n} (d^{a_i})^{y_{1i}} (\text{mod } \mathcal{N}) \\ &= d^{\sum_{1 \leq i \leq n} a_i y_{1i} \text{mod } (\varphi(\mathcal{N}))} (\text{mod } \mathcal{N}) \\ &= d^{s_1} (\text{mod } \mathcal{N}) \end{aligned}$$

Using the parameter γ and the publicly available information vector $\vec{h}$ from the KACs), we proceed with the following computational step:

- 3) Estimated ciphertext $C = M^\gamma (\text{mod } \mathcal{N})$.

Decryption: To extract the plaintext message M in the encrypted text, entity 1 needs to do the following operation:

- 1) Utilize the private key s_1 to retrieve M as $M = C^d (\text{mod } \mathcal{N})$.

The accuracy of the scheme is established as follows:

$$\begin{aligned} \text{Due to } \gamma &= \prod_{1 \leq i \leq n} h_i^{y_{1i}} (\text{mod } \mathcal{N}) \\ &= \prod_{1 \leq i \leq n} (d^{a_i})^{y_{1i}} (\text{mod } \mathcal{N}) \\ &= d^{\sum_{1 \leq i \leq n} a_i y_{1i} \text{mod } (\varphi(\mathcal{N}))} (\text{mod } \mathcal{N}) \\ &= d^{s_1} (\text{mod } \mathcal{N}) \end{aligned}$$

We have

$$C^{e^{s_1}} \equiv (M^{d^{s_1}})^{e^{s_1}} (\text{mod } \mathcal{N}) \equiv M^{(ed)^{s_1}} (\text{mod } \mathcal{N}) \equiv M (\text{mod } \mathcal{N}).$$

Pang, Li, and Wang [31] recognized two different deadlock issues, which were reported in Meshram, Meshram, and Zhang [21] and solved them by changing the IBC technique by using GDLP and IFP [20, 14, 9, 17, 19, 22]. Even though they also investigated the security implications of the approach, the authors have not provided formal security proof. Nevertheless, the manuscript based on cryptographic measures require strict security examination and formal demonstration with the corresponding argument.

5. The proposed Subtree-based Cryptosystem (SBC)

The proposed Subtree-Based Cryptosystem (SBC) integrated the PDL problem. This cryptographic framework is broken down logically into four core components: Setup, Extraction, Encryption, and Decryption. Each of these

algorithm's functions as a critical component within the overall framework, and their operational procedures are elaborated as follows:

Setup. KAC took the following actions:

- 1) Let $\mathcal{N} = q_1 p_1$ be a secure prime modulus, meaning that q_1 and p_1 are primes of the form $p_1 = (2p'_1 + 1)$ and $q_1 = (2q'_1 + 1)$, where q'_1 and p'_1 are also primes. Further, let G be a multiplicative group of maximal order generated by g_1 , and suppose that G is contained within the set of invertible elements of the ring $\mathbb{Z}_{\mathcal{N}^2}^*$.
- 2) Create a η dimensional vector $\vec{b} = (b_1, b_2, b_3, \dots, b_\eta)$ over $\mathbb{Z}_{\mathcal{N}^2}^*$, with s. t. $1 \leq b_i \leq \mathcal{N}^2$, $(1 \leq i \leq \eta)$ and $b_i \neq b_j \pmod{\mathcal{N}^2}$, $(i \neq j)$.
- 3) Next, we compute the η dimensional vector $\vec{h} = (h_1, h_2, h_3, \dots, h_\eta)$, where

$$h_i = g_1^{b_i} \pmod{\mathcal{N}^2} (1 \leq i \leq \eta).$$

- 4) The KAC employs $(\vec{b})$ as its private key and $(\mathcal{N}^2, g_1, \vec{h})$ as its public key. Each entity must receive a copy of the public key, whereas the private key must remain confidential.

Extraction. To determine entity i 's private key, the KAC performs the previously mentioned procedures. The identity of an entity is defined by a k -dimensional binary vector, which is provided by

$$\text{id}_i = (z_{i1}, z_{i2}, z_{i3}, z_{i4}, \dots, z_{ik}), \quad z_{ij} \in \{0,1\}, (1 \leq j \leq k).$$

- 1). Calculate the entity i 's expanded id_i , Eid_i , as:
 $\text{Eid}_i = (u_{i1}, u_{i2}, u_{i3}, u_{i4}, \dots, u_{it}), u_{ij} \in \text{Sup}(\mathbb{T}).$
- 2). Determine the secret keys of entity i , w_i , by taking the inner product of $\vec{b}$ and Eid_i given by:

$$w_i = \vec{b} \cdot \text{Eid}_i \pmod{\mathcal{N}^2} = \sum_{1 \leq j \leq n} b_j u_{ij} \pmod{\mathcal{N}^2}.$$

The notation id_i denotes the public key associated with entity i .

Encryption: Consider the scenario in which entity 2 intends to transmit a message $\mathcal{M}$ to entity 1. To ensure confidentiality, entity 2 encrypts message $\mathcal{M}$ by applying the relevant encryption procedure as described below:

- 1) The expanded identifier of entity i , represented by Eid_i , is computed as follows:
 $\text{Eid}_i = (u_{i1}, u_{i2}, u_{i3}, u_{i4}, \dots, u_{it}), u_{ij} \in \text{Sup}(\mathbb{T}).$
- 2) Calculating

$$\begin{aligned} \gamma_1 &= \prod_{1 \leq i \leq \eta} h_i^{u_{1i}} \pmod{\mathcal{N}^2} \\ &= \prod_{1 \leq i \leq \eta} (g_1^{b_i})^{u_{1i}} \pmod{\mathcal{N}^2} \\ &= g_1^{\sum_{1 \leq i \leq \eta} b_i u_{1i} \pmod{\mathcal{N}^2}} \pmod{\mathcal{N}^2} \end{aligned}$$

$$= g_1^{w_1}(\text{mod } \mathcal{N}^2)$$

Utilizing γ_1 alongside publicly available information $\vec{h}$ associated with the KAC, we proceed with the following steps:

Let $\mathcal{M}$ (with $0 \leq \mathcal{M} \leq \mathcal{N}^2 - 1$) denote the message to be transmitted by entity 2. Entity 2 first selects a random integer ν satisfying $0 \leq \nu \leq (\mathcal{N}^2 - 2)$, and then computes the ciphertext (C) as follows:

$$\begin{aligned} C &= (C_1, C_2) \\ C_1 &= g_1^\nu(\text{mod } \mathcal{N}^2) \\ C_2 &= \mathcal{M}(\gamma_1)^\nu(\text{mod } \mathcal{N}^2) \end{aligned}$$

Decryption: Entity 1 has completed the above-mentioned steps to extract $\mathcal{M}$ out of the ciphertext:

$$(C_1)^{w_1}(\text{mod } \mathcal{N}^2), (C_1)^{w_1} = (g_1^\nu)^{w_1}(\text{mod } \mathcal{N}^2)$$

using the secret key w_1 . By computing, the message of entity 2 can be recovered by entity 1 using equations (18) and (22).

$$((C_1)^{w_1})^{-1}C_2 = \{(g_1^\nu)^{w_1}\}^{-1} \mathcal{M}(\gamma_1)^\nu(\text{mod } \mathcal{N}^2) = \mathcal{M}(\text{mod } \mathcal{N}^2)$$

6. Security Investigation and Discussion

The computation strength of the projected SBC procedure is grounded on the intractability of certain index problem, namely, the PDL problem [20], [14], [9], and [19], in the multiplicative cyclic group defining an index, namely, the cyclic multiplicative group of integer elements, that is, in the group of integers, namely, the group of numbers, called the finite field, defined over finite field numbers. It is pertinent to mention that, as per the Coppersmith attack model, a collusion of at least $(\eta + 1)$ number of entities, being equal to or greater than, in this case, to η , may present a threat to the security of the system through a derivation of the secret information of KAC. This vulnerability underscores the necessity of designing robust mechanisms to prevent such collisions and preserve the integrity of the cryptosystem.

5.1 Collusion Between Selected Entities

5.1.1 KAC's secret Information:

The presented subtree-based cryptosystem includes algorithms based on partial discrete logarithms [14], [15], [21], and [22], and is specifically designed to accommodate up to 2^k different entities. Under this framework, we take a group of cooperating entities, denoted by m and m is greater than the frequency of interaction η and each entity is numbered by an integer i which is an integer between 1 and m . These organizations can conspire to re-discover the hidden value of the Key-Authorization Cryptosystem (KAC) which is represented as g_i .

$$g_i \mathcal{Y}_i = w_i(\text{mod } (\mathcal{N}^2)), (1 \leq i \leq m) \quad (1)$$

Consequently, this can be expressed as a system of linear congruences, as follows:

$$\begin{bmatrix} y_1 & 0 & \dots & 0 & 0 \\ 0 & y_2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & y_{\eta-1} & 0 \\ 0 & 0 & \dots & 0 & y_{\eta} \end{bmatrix} \begin{bmatrix} g_1 & 0 & \dots & 0 & 0 \\ 0 & g_2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & g_{\eta-1} & 0 \\ 0 & 0 & \dots & 0 & g_{\eta} \end{bmatrix} = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ \vdots \\ w_{\eta} \end{bmatrix} \pmod{\mathcal{N}^2} \quad (2)$$

$$= \mathfrak{B}g_i \pmod{\mathcal{N}^2} \quad (3)$$

In case matrix $\mathfrak{B}$ as defined in Equation (3) has η linearly independent row vectors over $\mathcal{Z}_{\mathcal{N}^2}^*$, $\eta - 1$, cooperating $\eta - m$ parties can uniquely infer the secret information g_i associated with the KAC. Nevertheless, the pivotal work by Nakamura et al. [30] and Coppersmith [29] has shown that even when matrix $\mathfrak{B}$ lacks η linearly independent row vectors over $\mathcal{Z}_{\mathcal{N}^2}^*$, entities i ($1 \leq i \leq m$) may still reconstruct an alternative version of the secret, denoted g'_i , thus potentially revealing the confidential information of the KAC. These observations have highlighted the existence of some delicate weaknesses to the underlying algebraic construction and require a careful examination of the properties of matrices when determining the safety of such cryptosystems.

5.1.2 Generation of Each User's Secret Key:

As demonstrated in subsection 5.1, entities indexed up to $(\eta - 1)$ are incapable of obtaining the center's secret info through any form of attack. On the other hand, in the event a collusion is formed with η or more, they can compute g_i before it is computed by the centre g'_i . Considering this, we now examine the security of each entity's secret key w_i against collusions involving fewer than η participants.

When fewer than η entities, specifically $t < \eta$, collaborate, the resulting system of linear congruences can be expressed as follows:

$$\begin{bmatrix} y_1 & 0 & \dots & 0 & 0 \\ 0 & y_2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & y_{n-1} & 0 \\ 0 & 0 & \dots & 0 & y_n \end{bmatrix} \begin{bmatrix} g_1 & 0 & \dots & 0 & 0 \\ 0 & g_2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & g_{n-1} & 0 \\ 0 & 0 & \dots & 0 & g_n \end{bmatrix} = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ \vdots \\ w_n \end{bmatrix} \pmod{\mathcal{N}^2} \quad (4)$$

$$= \mathfrak{B}''g_i \pmod{\mathcal{N}^2} \quad (5)$$

In case there is a cover of the entity k , covering a t -dimensional vector, which is the cover of $\mathcal{Z}_{\mathcal{N}^2}^*$.

$$\ell \mathfrak{B}'' = \sum_{1 \leq i \leq \eta} \ell_i y_i \pmod{\mathcal{N}^2} \quad (6)$$

$$= y_k \pmod{\mathcal{N}^2} \quad (7)$$

Then any group of $t < \eta$ entities can recover the private key w_k of entity k by

$$w_k = \sum_{1 \leq i \leq \eta} \ell_i w_i \pmod{\mathcal{N}^2} \quad (8)$$

Noting that $\mathcal{Z}_{\mathcal{N}^2}^*$ does not constitute a field, it can be readily demonstrated that a conspiracy of $t < \eta$ entities can create at most 2^t secret keys corresponding

to other entities, as indicated in equation (8). Consequently, the probability that $t < \eta$ entities can successfully spring the secret key of another entity is bounded by $\frac{2^t}{2^\eta} = 2^{t-\eta}$.

Theorem 5.1 (Coppersmith) [29]: *Let there be $\eta + 1$ entities be indexed by i , where $1 \leq i \leq (\eta + 1)$. Each entity can derive an η -dimensional vector $\mathcal{g}'_i$ over the group $\mathcal{Z}_{\mathcal{N}^2}^*$. This vector $\mathcal{g}'_i$ is equivalent, although not identical to the actual secret info of the KAC.*

Proof: When $(\eta + 1)$ entities denoted as i with $1 \leq i \leq (\eta + 1)$, act in concert or conspire, the resulting framework can be described by a system of linear congruences expressed as follows:

$$\begin{bmatrix} \mathcal{Y}_1 & 0 & \cdots & 0 & 0 \\ 0 & \mathcal{Y}_2 & & 0 & 0 \\ \vdots & & \ddots & \vdots & \\ 0 & 0 & \cdots & \mathcal{Y}_\eta & 0 \\ 0 & 0 & \cdots & 0 & \mathcal{Y}_{\eta+1} \end{bmatrix} \begin{bmatrix} \mathcal{g}_1 & 0 & \cdots & 0 & 0 \\ 0 & \mathcal{g}_2 & & 0 & 0 \\ \vdots & & \ddots & \vdots & \\ 0 & 0 & \cdots & \mathcal{g}_{\eta-1} & 0 \\ 0 & 0 & \cdots & 0 & \mathcal{g}_\eta \end{bmatrix} = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ \vdots \\ w_{\eta+1} \end{bmatrix} \pmod{\mathcal{N}^2} \quad (9)$$

Given that each $\mathcal{Y}_i$ is an η -dimensional binary vector, there exists a corresponding $(\eta + 1)$ -dimensional vector ℓ over the ring $\mathcal{Z}_{\mathcal{N}^2}^*$ satisfying the following relationship:

$$\sum_{1 \leq i \leq \eta+1} \ell_i \mathcal{Y}_i = 0 \quad (10)$$

Here,

$$\sum_{1 \leq i \leq \eta+1} \ell_i w_i = 0 \pmod{\mathcal{N}^2} \quad (11)$$

and thus

$$\sum_{1 \leq i \leq \eta+1} \ell_i w_i = A \mathcal{N}^2 \quad (12)$$

When every entity of the number of them, denoted by $\eta + 1$, has an integer number of multiples of $\mathcal{N}^2$, given that $A \neq 0$, those entities can, together, find out the factors of $\mathcal{N}^2$. The latter fact permits a similar attack as described in Theorem 5.1, and, in turn, the secret data stored in the KAC can be restored via the cooperation of the collusion of $\eta + 1$ participants. In addition, Meshram, Meshram, and Lee [22] suggested a general attack procedure that could be used against the modified system where the concerted efforts of the number of entities of at least, $\eta + 2$, would be enough to extract the secret information of the KAC with high success. This highlights the potential vulnerability of the system under conspiratorial conditions exceed the original threshold.

Theorem 5.2 (Shamir) [3]: *Let $(\eta + 2)$ be a positive integer and consider a collection of distinct entities indexed by i where $1 \leq i \leq (\eta + 2)$. Then, by pooling their computational resources and collaborating in a coordinated manner, these entities can recover the private key $\mathcal{g}$ associated with the key authority center (KAC) with high probability.*

Proof: Suppose $(\eta + 1)$ entities, indexed by $1 \leq i \leq (\eta + 1)$, conspire. Then, from the structure of the underlying secret-sharing scheme, each entity i contributes a linear congruence. Taking these congruences together, the resulting system simplifies precisely to the one shown in Equation (13).

$$\begin{bmatrix} y_1 & 0 & \dots & 0 & 0 \\ 0 & y_2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & y_\eta & 0 \\ 0 & 0 & \dots & 0 & y_{\eta+1} \end{bmatrix} \begin{bmatrix} g_1 & 0 & \dots & 0 & 0 \\ 0 & g_2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & g_{\eta-1} & 0 \\ 0 & 0 & \dots & 0 & g_\eta \end{bmatrix} = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ \vdots \\ w_{\eta+1} \end{bmatrix} \pmod{\mathcal{N}^2} \quad (13)$$

$$= \mathfrak{B} \mathfrak{g} \pmod{\mathcal{N}^2} \quad (14)$$

Let $\mathfrak{B}$ be a matrix whose columns consist of η linearly independent vectors over $\mathcal{Z}_{\mathcal{N}^2}^*$.

Accordingly, there are strictly positive integers ℓ_i for $1 \leq i \leq (\eta + 1)$, such that

$$\begin{bmatrix} y_1 & 0 & \dots & 0 & 0 \\ 0 & y_2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & y_\eta & 0 \\ 0 & 0 & \dots & 0 & y_{\eta+1} \end{bmatrix} \begin{bmatrix} g_1 & 0 & \dots & 0 & 0 \\ 0 & g_2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & g_{\eta-1} & 0 \\ 0 & 0 & \dots & 0 & g_\eta \end{bmatrix} = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ \vdots \\ w_{\eta+1} \end{bmatrix} - \begin{bmatrix} \ell_1 \\ \ell_2 \\ \ell_3 \\ \vdots \\ \ell_{\eta+1} \end{bmatrix} \mathcal{N}^2 \quad (15)$$

Equation (15) may be equivalently expressed as follows:

$$\begin{bmatrix} y_1 & 0 & \dots & 0 & 0 & w_1 \\ 0 & y_2 & \dots & 0 & 0 & w_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & y_\eta & 0 & \vdots \\ 0 & 0 & \dots & 0 & y_{\eta+1} & w_{\eta+1} \end{bmatrix} \begin{bmatrix} g_1 & 0 & \dots & 0 & 0 \\ 0 & g_2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & g_{\eta-1} & 0 \\ 0 & 0 & \dots & 0 & g_\eta \end{bmatrix} = - \begin{bmatrix} \ell_1 \\ \ell_2 \\ \ell_3 \\ \vdots \\ \ell_{\eta+1} \end{bmatrix} \mathcal{N}^2 \quad (16)$$

$$= \mathfrak{B}' \mathfrak{g}'_i \quad (17)$$

By assumption, matrix $\mathfrak{B}$ defined in Equation (14) consists of η column vectors that are linearly independent over ring $\mathcal{Z}_{\mathcal{N}^2}^*$. Consequently, it follows that there exists a nonsingular matrix $\mathfrak{B}'$ over the same ring $\mathcal{Z}_{\mathcal{N}^2}^*$ for which the determinant satisfies $\det(\mathfrak{B}') \neq 0$ with an overwhelming probability. This condition further implies that $\mathfrak{g}'_i \neq 0 \pmod{\mathcal{N}^2}$. Therefore, the system of linear congruence can be reformulated as follows:

$$\mathfrak{B}' \mathfrak{g}'_i = 0 \pmod{\mathcal{N}^2} \quad (18)$$

If $\mathfrak{B}'$ was nonsingular over the multiplicative group $\mathcal{Z}_{\mathcal{N}^2}^*$, it would imply that $\mathfrak{g}'_i = 0 \pmod{\mathcal{N}^2}$, which contradicts the previously established result. Therefore, with an overwhelming probability, $\mathfrak{B}'$ must be singular over $\mathcal{Z}_{\mathcal{N}^2}^*$, and consequently, $\det(\mathfrak{B}') = 0 \pmod{\mathcal{N}^2}$. This observation suggests that, with high probability, $\det(\mathfrak{B}')$ is divisible by $\mathcal{N}^2$.

Furthermore, consider a scenario in which any other subset of $(\eta + 1)$ entities out of $(\eta + 2)$ collaborate. The corresponding matrix is denoted as $\mathfrak{B}''$, which is structured similar to $\mathfrak{B}'$. This leads us to expect that, with high probability, $\det(\mathfrak{B}'')$ is also a multiple of $\mathcal{N}^2$. Consequently, the gcd of $\det(\mathfrak{B}')$ and $\det(\mathfrak{B}'')$ can be written as $d\mathcal{N}^2$, where d is some small positive integer. An efficient assessment of $\mathcal{N}^2$ is made possible with the use of these observations. This additional step in the calculation of the secret information of the center is exactly the articulation of the attack in Theorem 5.2.

7. A Comparative Analysis of Performance Against Existing Techniques

The contemporary part provides the analytical discussion of nine popular identity-based cryptographic (IBC) methods, and the quantitative comparative evaluation of their performance. The methods that we are considering include: the IBC scheme of Cocks [6], the authenticated IBC scheme of Lynn [4], the selective-identity secure IBC scheme of Boneh and Franklin [28], which does not use random oracles, the hierarchical IBC scheme of Gentry et al. [7], the technique of Water [5] and some variations that are the ID-based cryptographic scheme of Boneh and Boyen [20], the approach of Meshram and Meshram [15] and other schemes that were proposed by Meshram. Furthermore, Pang, Li, and Wang [31] researched the IBC technique as the combination of the novel efficient IBC technique presented in this study. The performance metrics which will be used here are based on the considerations of the efficiency of the server side, in this case, the consideration of the encryption and decryption algorithms and the computational overheads involved in these processes. The general objective of this comparative analysis is to clarify the strengths and weaknesses of each methodology in a real-life cryptographic application.

The following notation is adopted to characterize computational performance within a cryptographic framework. The pairing operation is denoted by t_p , while t_M represents the time required for modular multiplication. Modular exponentiation within a group is expressed as t_e , and t_m refers to the time needed for scalar or point multiplication in a group. The execution time for an XOR operation is given by t_x , while t_H denotes a map-to-point hash operation, and t_h corresponds to a one-way hash function. Modular arithmetic operations are accounted for by t_a (modular addition) and t_i (modular inversion). Finally, t_j quantifies the computational time associated with evaluating the Jacobi symbol. These notations offer a systematic and coherent model of doing a comparative analysis of cryptographic algorithms in reference to their computational complexity.

It is well understood that the pairing operation, denoted by t_p , requires significantly more time to execute than other cryptographic operations. The performance simulation results indicate that the execution times for modular addition (t_a) and one-way hash functions (t_h) are negligible when measured against modular exponentiation (t_e), modular multiplication (t_M), XOR operations (t_x), map-to-point hash functions (t_H), modular inverses (t_i), and Jacobi symbol computations (t_j). Notably, both the encryption and decryption

algorithmic phases demand substantially higher computational resources than other phases, such as setup and extraction, which are executed only once. Consequently, the performance comparison focused exclusively on the encryption and decryption phases. The IBC technique proposed herein has been evaluated against existing techniques referenced by their respective citations. A comparative analysis of the computational costs in conjunction with security considerations is presented in Table 1.

Table 1
Comparative analysis of the proposed subtree-based cryptographic technique with existing methods

IBC Techniques	$\mathcal{F}_1$	$\mathcal{F}_2$	$\mathcal{F}_3$
Cocks [6]	$t_J + 2t_a + 2t_M + 2t_i$	$t_J + t_a$	$2t_J + 3t_a + 2t_M + 2t_i$
Gentry and Silverberg [7]	$t_P + t_H + t_h + t_e + t_m + t_x$	$t_P + t_h + t_x$	$2t_P + t_H + 2t_h + t_e + t_m + 2t_x$
Lynn [4]	$t_P + t_H + 3t_h + t_x$	$t_P + t_H + 3t_h + t_x$	$2t_P + 2t_H + 6t_h + 2t_x$
Boneh and Franklin [28]	$t_P + 4t_e + 2t_M$	$t_P + t_e + t_M + t_i$	$2t_P + 5t_e + 3t_M + t_i$
Waters [5]	$2t_P + 3t_m$	$2t_P + t_m + t_i$	$4t_P + 4t_m + t_i$
Pang, Li, and Wang [31]	$3t_e + t_m$	$4t_e + t_m$	$7t_e + 2t_m$
Meshram and Obaidat [23]	$4t_e + t_m$	$2t_e + t_m + \tau_i$	$6t_e + 2t_m + t_i$
Meshram and Meshram [20]	$3t_e + 3t_M$	$3t_e + 2t_M$	$6t_e + 5t_M$
Meshram et al. [14]	$2t_e + 3t_M$	$2t_e + 2t_M$	$4t_e + 5t_M$
Proposed Technique	$2t_e + t_m + t_i$	$2t_e + t_m + t_i$	$4t_e + 2t_m + 2t_i$

$\mathcal{F}_1$: represents the computational cost incurred during the encryption phase; $\mathcal{F}_2$: denotes the corresponding cost for the decryption phase; $\mathcal{F}_3$: captures the overall computational cost, aggregating the expenses of both encryption and decryption stages.

As observed in Table 1, the proposed IBC technique, which is grounded in the PDL and demonstrates a lower computational cost compared to the techniques referenced in [4],[5], [6], [7], [14], [20], [23], [28], [31].

8. Conclusion and Future work

An improved IBC technique that leverages the hardness of the PDL problem is proposed in this work. The security of the proposed technique rests fundamentally on the computational intractability of the PDL problem, specifically when defined over a multiplicative group on a finite field and involving distinct, discrete exponents. Notably, the proposed approach rigorously adheres to Shamir’s foundational principles for IBC. In addition to eliminating the need to have prior interactive communication on the part of the user before every data transmission, as is the case with many of the current schemes, the current approach can be used to enhance the operational efficiency of the scheme.

Besides, the approach is not based on the presence of tamper-proof modules, which makes it more practical in practical environments. When compared to other identity-based cryptographic (IBC) approaches that rely on the generalized discrete logarithm problem (GDLP) or the identity-based fuzzy public key (IFP) model, the present method offers a superior level of security over an extended period. Moreover, it achieves computational efficiency as fewer operations are required during encryption and decryption which highlights its applicability in real practice.

Unlike traditional public-key cryptosystems, which are typically grounded in the classical DLP over generic groups or the IFP, the proposed algorithm offers distinct security advantages by specifically addressing the public-key blind-decryption problem within the multiplicative group over finite fields. Most importantly, the suggested approach removes the problem of deadlock that was detected by Pang et al., thus providing a greater level of security compared to the approach suggested by these researchers. This system facilitates the development of an identity-based encryption scheme grounded in lightweight public-key management models. Lightweight schemes of this type can be defined by relatively small public and private key sizes relative to those listed in many known IBC techniques as reported in the literature. This feature is particularly beneficial in grid-security architectures, where the membership of users varies every now and then due to the entry or exit of personnel into the grid. Since the traditional certificate-based systems are commonly used when submitting each task, key management is getting more complex, and bandwidth use is becoming even more complex in the grid infrastructure. Introduction of a certificate free system of IBC, as suggested, has the prospect of reducing these challenges by simplifying the major management and minimizing overheads to it.

Within the IBC paradigm, a notable advantage lies in the fact that an end client's public key can be generated and used instantaneously, without requiring a public key certificate unlike traditional systems where such certificates must be transmitted to the intended recipient through protocols like the Transport Layer Security (TLS) handshake. Nevertheless, conventional IBC systems are hindered by inherent limitations, namely the key escrow problem and the need to securely distribute private keys, both of which constrain the practical efficiency of identity-based keys. Although the Globus Toolkit (GT) offers single sign-on capabilities along with delegation proxy credentials, the enhanced PDL-based IBC system introduced in this study effectively mitigates both certificate dependency and key escrow issues. This advancement is a meaningful step towards simplifying key management while preserving the robust security properties in identity-based encryption frameworks.

A salient benefit of the IBC paradigm is that the public key of an end-user can be effectively generated and used immediately without the requirement to use a public-key certificate which is usually relayed to the target party through protocols like Transport Layer Security (TLS) handshakes. However, traditional identity-based cryptographic schemes face several fundamental limitations such as key-escrow dilemma and the necessity of secure sharing of private keys; all

these limitations reduce the utility of identity-based key schemes in practice. While the GT relies on single sign-on functionality and delegation proxy credentials, the improved PDL-based IBC system introduced in this study avoids both the issue of certificate dependency and the key escrow problem. The development is an important step towards streamlining important management but maintaining the strong security features of identity-based encryption models.

Acknowledgements

The authors extend their sincere gratitude to the anonymous reviewers of the JDMSC for their thoughtful and constructive comments, which helped improve the quality of this work. This Project was funded by KAU Endowment (WAQF) at King Abdulaziz University, Jeddah. The authors, therefore, acknowledge with thanks WAQF and the Deanship of Scientific Research (DSR) for technical and financial support.

References

- [1] Abhishek Das and Asoke Adhikari, "An efficient IND-CCA2 secure Paillier-based cryptosystem," *Information Processing Letters*, vol. 112, pp. 885–888 (2012).
- [2] Adi Shamir, "Identity-based cryptosystem and signature scheme," in *Advances in Cryptology – Proceedings of CRYPTO'84, Lecture Notes in Computer Science*, vol. 196. Berlin, Germany: Springer, pp. 47–53 (1984).
- [3] Adi Shamir, "Private communication," (Jun. 1988).
- [4] Ben Lynn, "Authenticated ID-based encryption," *Cryptology ePrint Archive*, Report 2002/072 (2002).
- [5] Brent Waters, "Efficient identity-based encryption without random oracles," in *Advances in Cryptology – CRYPTO 2005, Lecture Notes in Computer Science*, vol. 3494. Berlin, Germany: Springer, pp. 114–127 (2005).
- [6] Clifford Cocks, "An identity-based encryption scheme based on quadratic residues," in *International Conference on Cryptography and Coding (Proceedings of IMA), Lecture Notes in Computer Science*, vol. 2260. Berlin, Germany: Springer, pp. 360–363 (2001).
- [7] Craig Gentry and Alice Silverberg, "Hierarchical ID-based cryptography," in *Advances in Cryptology – ASIACRYPT 2002, Lecture Notes in Computer Science*, vol. 2501. Berlin, Germany: Springer, pp. 548–566 (2002).
- [8] Chandrashekhar Meshram, "An efficient ID-based cryptographic encryption based on discrete logarithm problem and integer factor-

- ization problem," *Information Processing Letters*, vol. 115, no. 2, pp. 351–358 (2015).
- [9] Chandrashekhkar Meshram, Chin-Chen Lee, Chien-Ta Li, and Chin-Laung Chen, "A secure key authentication scheme for cryptosystems based on GDLP and IFP," *Soft Computing*, vol. 21, no. 24, pp. 7285–7291 (2017).
 - [10] Chandrashekhkar Meshram, Chin-Chen Lee, Chien-Ta Li, and Sarita G. Meshram, "An efficient online/offline ID-based short signature procedure using extended chaotic maps," *Soft Computing*, vol. 23, no. 3, pp. 747–753 (2019).
 - [11] Chandrashekhkar Meshram, Chin-Chen Lee, Sarita G. Meshram, and Mohammad Khurram Khan, "An identity-based encryption technique using subtree for fuzzy user data sharing under cloud computing environment," *Soft Computing*, vol. 23, no. 24, pp. 13127–13138 (2019).
 - [12] Chandrashekhkar Meshram, Chin-Chen Lee, Sarita G. Meshram, and Ankur Meshram, "OOS-SSS: An efficient online/offline subtree-based short signature scheme using Chebyshev chaotic maps for wireless sensor networks," *IEEE Access*, vol. 8, no. 1, pp. 80063–80073 (2020).
 - [13] Chandrashekhkar Meshram, Chin-Chen Lee, Abhay S. Ranadive, Chien-Ta Li, Sarita G. Meshram, and Jitendra V. Tembhurne, "A subtree-based transformation model for cryptosystem using chaotic maps under cloud computing environment for fuzzy user data sharing," *International Journal of Communication Systems*, vol. 33, no. 7, p. e4307 (2020).
 - [14] Chandrashekhkar Meshram, Chin-Chen Lee, Shyam Gupta Meshram, and Chin-Chen Lee, "An IND-IDCPA secure ID-based cryptographic protocol using GDLP and IFP," *Informatica*, vol. 28, no. 3, pp. 471–484 (2017).
 - [15] Chandrashekhkar Meshram and Sarita G. Meshram, "An identity-based beta cryptosystem," in *Proc. 7th IEEE Int. Conf. Information Assurance and Security (IAS 2011)*, pp. 298–303 (2011).
 - [16] Chandrashekhkar Meshram and Sarita G. Meshram, "An identity-based cryptographic model for discrete logarithm and integer factoring based cryptosystem," *Information Processing Letters*, vol. 113, no. 10–11, pp. 375–380 (2013).
 - [17] Chandrashekhkar Meshram and Sarita G. A. Meshram, "Some modification in ID-based cryptosystem using IFP and DDLP," *International*

- Journal of Advanced Computer Science and Applications*, vol. 2, no. 8, pp. 25–29 (2011).
- [18] Chandrashekhar Meshram, Sarita G. A. Meshram, and Daya Gupta, “An ID-based beta cryptosystem using generalized discrete logarithm problem and integer factorization problem,” *Journal of Information Assurance & Security*, vol. 7, no. 5, pp. 275–283 (2012).
 - [19] Chandrashekhar Meshram, Sarita G. A. Meshram, and Chandra Ram, “Constructing identity-based cryptographic scheme for beta cryptosystem,” *International Journal of Applied Mathematics*, vol. 25, no. 5, pp. 609–624 (2012).
 - [20] Chandrashekhar Meshram and Sarita G. A. Meshram, “Constructing new an ID-based cryptosystem for IFP and GDLP based cryptosystem,” *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 20, no. 5, pp. 1121–1134 (2017).
 - [21] Chandrashekhar Meshram, Sarita G. Meshram, and Min Zhang, “An ID-based cryptographic mechanism based on GDLP and IFP,” *Information Processing Letters*, vol. 112, no. 19, pp. 753–758 (2012).
 - [22] Chandrashekhar Meshram, Sarita G. Meshram, and Chin-Chen Lee, “Constructing provably secure ID-based beta cryptographic scheme in random oracle,” *International Journal of Network Security*, vol. 20, no. 3, pp. 568–574 (2018).
 - [23] Chandrashekhar Meshram and Mohammad S. Obaidat, “An ID-based quadratic-exponentiation randomized cryptographic scheme,” in *Proc. IEEE Int. Conf. Computer, Information, and Telecommunication Systems (CITS 2015)*, pp. 1–5 (2015).
 - [24] Chandrashekhar Meshram, Mohammad S. Obaidat, Cheng-Chi Lee and Sarita Gajbhiye Meshram, “An efficient key authentication procedure for IND-CCA2 secure Paillier-based cryptosystem,” *Soft Computing*, vol. 24, no. 12, pp. 6531–6537 (2020).
 - [25] Chandrashekhar Meshram, Mohammad S. Obaidat, Bilal Sadoun, and Augustine L. Imoize, “A secure and efficient subtree-based authentication scheme for telemedicine information systems,” in *Proc. IEEE Int. Conf. Communications, Computing, Cybersecurity, and Informatics (ICC CI 2025)*, pp. 127–132 (2025).
 - [26] Chandrashekhar Meshram, Mohammad S. Obaidat, Bilal Sadoun, Augustine L. Imoize, and Vishesh P. Gaikwad, “A robust subtree-based authentication scheme for TMIS using chaotic hash function,” in *Proc. IEEE Int. Conf. Computer, Information, and Telecommunication Systems (CITS 2024)*, pp. 1–7 (2024).

- [27] Dan Boneh and Xavier Boyen, "Efficient selective-ID secure identity-based encryption without random oracles," in *Advances in Cryptology – EUROCRYPT 2004, Lecture Notes in Computer Science*, vol. 3027. Berlin, Germany: Springer, pp. 223–238 (2004).
- [28] Dan Boneh and Matthew K. Franklin, "Identity-based encryption from the Weil pairing," *SIAM Journal of Computing*, vol. 32, no. 3, pp. 586–615 (2003).
- [29] Don Coppersmith, "Cryptography," *IBM Journal of Research and Development*, vol. 31, no. 2, pp. 244–248 (1987).
- [30] Kiyoshi Nakamura, Eiji Okamoto, Koji Tanaka, and Satoshi Miura, "Private communication," (Aug. 1987).
- [31] Liang Pang, Hongwei Li, and Yong Wang, "nMIBAS: A novel multi-receiver ID-based anonymous signcryption with decryption fairness," *Computing and Informatics*, vol. 32, no. 3, pp. 441–460 (2013).
- [32] Mohamed Ramadan, Yao Liao, Fenghua Li, Shouhuai Zhou, and Hassan Abdalla, "IBEET-RSA: Identity-based encryption with equality test over RSA for wireless body area networks," *Mobile Networks and Applications*, vol. 25, pp. 223–233 (2020).
- [33] Nusrat Farjana, Sajal Roy, Md. Jahidul N. Mahi, and Mohammad Whaiduzzaman, "An identity-based encryption scheme for data security in fog computing," in *Proc. Int. Joint Conf. Computational Intelligence*, pp. 215–226 (2020).
- [34] Pascal Paillier, "Public key cryptosystem based on discrete logarithm residues," in *EUROCRYPT 99, Lecture Notes in Computer Science*, vol. 1592. Berlin, Germany: Springer, pp. 223–238 (1999).
- [35] Shigeo Tsujii and Toshiya Itoh, "An ID-based cryptosystem based on the discrete logarithm problem," *IEEE Journal on Selected Areas in Communications*, vol. 7, no. 4, pp. 467–473 (1989).
- [36] Taher ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, pp. 469–472 (1995).
- [37] Weiran Liu, Jianwei Liu, Qianhong Wu, Bo Qin, David Naccache and Houda Ferradi, "Efficient subtree-based encryption for fuzzy-entity data sharing," *Soft Computing*, vol. 22, no. 23, pp. 7961–7976 (2018).

Received December, 2025.