Received: 12 May 2020 | Revised: 22 May 2020 | Accepted: 30 May 2020 | Published on: 6 July 2020

DOI: 10.1002/spy2.119

RESEARCH ARTICLE

WILEY

An efficient ID-based cryptographic technique using IFP and GDLP

Chandrashekhar Meshram[1] | **Rabha W. Ibrahim**[2,3] | **Sarita Gajbhiye Meshram**[4,5] | **Kailash W. Kalare**[6] | **Sunil D. Bagde**[7]

[1] Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post-Graduation College, College of Chhindwara University, Betul, Madhya Pradesh, India

[2] Informetrics Research Group, Ton Duc Thang University, Ho Chi Minh City, Vietnam

[3] Faculty of Mathematics & Statistics, Ton Duc Thang University, Ho Chi Minh City, Vietnam

[4] Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam

[5] Faculty of Environment and Labour Safety, Ton Duc Thang University, Ho Chi Minh City, Vietnam

[6] Department of Computer Science and Engineering, Visvesvaraya National Institute of Technology, Nagpur, India

[7] Department of Mathematics, Gondwana University, Gadchiroli, India

Correspondence
Chandrashekhar Meshram, Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post-Graduation College, College of Chhindwara University, Betul, Madhya Pradesh, India.
Email: cs_meshram@rediffmail.com

Abstract

Implementing an improved ID-based cryptographic mechanism is the main objective of the proposed work. In this article, an ID-based cryptographic (IBC) technique using generalized discrete logarithm problem (GDLP) and the integer factorization problem (IFP) presented by Meshram et al have improved. Meshram et al have given IBC technique without using the bilinear pair and also, reveal that their technique can attain data protection and security objectives. Besides, their technique will deter the adversary from eavesdropping the encrypted information or the secret key of the user. However, it has found that their system carries a deadlock problem. Encryption process, as expected by the user, is not guaranteed to be secure. It is because the user may require private information about key authentication center (KAC), which has kept secret from users. Pang et al have proposed an improved technique that overcomes the deadlock problem. It has found that Pang et al have not discussed the analysis and proofs of security. In this article, generalized discrete logarithms in multiplicative group over finite fields and IFP have used to improve the technique and also a key distribution system has discussed. It has analyzed that the proposed strategy is safer than the technique described by Pang et al. Also, it has found that the proposed technique addresses the deadlock problem.

KEYWORDS

cryptography, GDLP, ID-based cryptosystem, IFP, security proof

1 | INTRODUCTION

Nowadays, computer technologies and use of the internet has evolved in the daily life of every individual. The internet of things (IoT) has changed the way of living daily life as well as business life. Secrecy over the internet has become the prime concern of every individual. Secrecy has become essential for the data, that is, transferred over insecure public channels. Before establishing secure communication, secrete session keys to be shared between the communicating parties in an

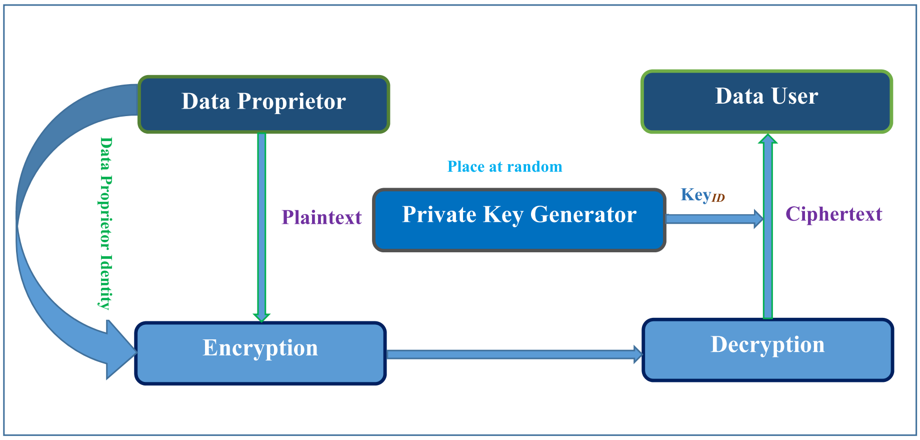

FIGURE 1 Identity-based cryptographic system

open-network environment. It has seen that key-distribution has become a complex issue due to the rapid increase in the number of users.

The session key-distribution issue, handled by the public-key cryptosystem, has found more useful in an open network environment. Before using, each user should validate the public key of the companion. Public-key infrastructure (PKI)[1] handles public-keys authentication; however, it suffers from the large overheads of management.

In 1984, Shamir[2] implemented the ID-based cryptosystem (IBC) (Figure 1). Personal identity information for the user including identification number such as email address can be used to retrieve the personal key for each user. The authentication issue can be escaped, by using the public key as the public identity of the user. It also, helps users to setup a non-interactive session. The technique presented by Shamir[2] has usefulness only in signature scheme based on identity (ID). Boneh et al[3] constructed ID-based encryption by using Weil pairing property. It has seen that the system proposed by Boneh et al[3] became practical. However, the cryptosystem has seen unsuitable for low-performance devices due to bilinear pair operations.

Meshram et al[4] proposed an improved version of IBC.[5-9] Meshram et al[4] considered the solutions to GDLP as well as IPF, as their security assumptions. Also, their technique has not adopted a bilinear pair. The technique proposed by Meshram et al[4] has found better; also, the approach can attain the security objective of data protection and stop adversary from eavesdropping over the encrypted data along with the user's private key. Besides, their technique prevents users from decryption of the cipher-text if the user has not private information of key authentication center (KAC). The private information of KAC is always kept a secret from the users. User is unable to decrypt the cipher-text received by him only by his private key. User must require a portion of private-key of the KAC. The technique proposed by Meshram et al[4] has found secure in protecting data and user's private-key; however, their technique possess a deadlock problem.

Pang et al[10] shown that the technique proposed by Meshram et al[4] found incorrect and possess a deadlock problem. Encryption process has found dependent on the KACs private information; however, it must keep secret from the user. Therefore, users cannot carry encryption as expected. Pang et al[11] presented an improved technique that addresses the deadlock problem. However, proper analysis and proofs presented in their paper, have not discussed.

Recently, Meshram et al[12] demonstrated the basic setting for aggregation of online/offline ID-based short signature (IBSS) protocol using partial discrete logarithm on wireless sensor networks. Meshram et al[13,14] developed transformation model for public key cryptography and online/offline IBSS procedure using extended chaotic maps. Meshram et al[15] proposed efficient ID-based encryption technique using subtree and pairing under cloud computing environment for fuzzy user data sharing. Ramadan et al[16] investigated identity-based encryption scheme under the RSA assumption and providing equality test. Meshram et al[17,18] presented efficient transformation model for cryptosystem and short signature schemes using chaotic maps under cloud computing environment with fuzzy user data sharing Farjana et al[19] demonstrated the new identity-based encryption technique that confirms protected information transmission to certified users and showed its implementation in fog computing.

1.1 Our contribution

In this article, the intensification of security and modification in the ID-based cryptographic mechanism has proposed. The technique used GDLP with unique, discrete exponents in the multiplicative group over finite fields as well as IFP.

Also, the key distribution system presented. The proposed technique will see suitable for developing a more secure IBC approach with GDLP and IFP as compare to Pang et al.[11] Also, formal security proof under the hardness assumption of solving GDLP and IFP[20-22] have provided.

1.2 | Organization

The rest of the paper structured as follows: Meshram et al's ID-based cryptographic approach has reviewed in Section 2. Pang et al's improved IBC has reviewed in Section 3. Proposed more secure IBC has discussed in Section 4. The security proof, along with analysis of the proposed technique have discussed in Section 5. The comparative study based on the performance along with some other existing IBC techniques has discussed in Section 6. Finally, in Section 7, the paper has concluded and future scope has discussed.

2 | REVIEW ON MESHRAM ET AL ID-IBC

Meshram et al's IBC has four related sub-algorithms, such as Setup, Extraction, Encryption, and Decryption.[4] Setup algorithm, run by KAC, has designed to generate public and private keys. User has to send register application to KAC. KAC executes Extraction algorithm and generates the unique private key for the users verified as legal. User has to verify his/her identity before sending the message. User has to execute Encryption algorithm, which encrypts the message if he/she wish to send a message to any other user securely. The receiver, on the other hand, has to execute Decryption algorithm to decrypt the cipher text. Decrypting cipher text requires receiver's private key. Almost all of the IBC methods have described in the same manner.[23-25] Meshram et al's IBC method has shown in the following manner.

2.1 | Setup

KAC has performed the following steps:

1. Select two arbitrary prime numbers p and q, s.t. $N = pq$. Let $n = |N|$ be a bit number and compute the Euler-phi function $\varphi(N) = (p-1)(q-1)$.
2. Select two arbitrary integers e and d, $1 \le e, d \le \varphi(N)$ s. t. $\gcd(e, \varphi(N)) = 1$, and $ed \equiv 1 \ (\bmod\ \varphi(N))$.
3. Create a $n-$dimensional vector $\vec{a} = (a_1, a_2, a_3, \dots, a_n)$ over $Z^*_{\varphi(N)}$, s.t. $1 \le a_i \le \varphi(N)$, $(1 \le i \le n)$ and $a_i \ne a_j (\bmod\ \varphi(N))$, $(i \ne j)$.
4. Compute $n-$dimensional vector $\vec{h} = (h_1, h_2, h_3, \dots, h_n)$, where $h_i = e^{a_i} (\bmod\ N)(1 \le i \le n)$.
5. KAC uses $(N, e, \vec{h})$as its public key, along with $(\vec{a}, d)$ as its private key. The public key has to be distributed to each entity, while the private key as secret.

2.2 | Extraction

KAC carries out the preceding steps to calculate a private key of the entity i. A k-dimensional binary vector defines entities identity, given by

$$\mathrm{ID}_i = (x_{i1},\ x_{i2},\ x_{i3},\ x_{i4},\ \dots,\ x_{ik}),\ x_{ij} \in \{0,\ 1\},\ (1 \le j \le k).$$

1. Compute extended ID of the entity i's, EID$_i$ as:
   $\mathrm{EID}_i = (\mathrm{ID}_i)^e (\bmod\ N) = (y_{i1}, y_{i2}, y_{i3}, y_{i4}, \dots, y_{it}), y_{ij} \in \{0, 1\}, (1 \le j \le t).$
2. Compute entity $i' s$ secrete keys s_i,as the inner product of $\vec{a}$ and EID$_i$given by:
   $s_i = \vec{a}\ \mathrm{EID}_i (\bmod\ \varphi(N)) = \sum_{1 \le j \le n} a_j y_{ij} \bmod\ (\varphi(N)).$

Note that ID$_i$ defines the entity i's public key.

2.3 | Encryption

Suppose entity 2 wishes to send message M to entity 1, and entity 2 performs encryption of M as given below:

1 Calculate extended ID of the entity i'sEID$_1$as: $\mathrm{EID}_1 = (\mathrm{ID}_1)^e(\bmod N) = (y_{11}, y_{12}, y_{13}, y_{14}, \ldots, y_{1t}), y_{1j} \in \{0, 1\}, (1 \leq j \leq t)$.
2 Compute: $\gamma_1 = \prod_{1 \leq i \leq n} {h_i}^{y_{1i}}(\bmod N)$

$$= \prod_{1 \leq i \leq n} (e^{a_i})^{y_{1i}}(\bmod N)$$

$$= e^{\sum_{1 \leq i \leq n} a_i y_{1i} \bmod (\varphi(N))}(\bmod N)$$

$$= e^{s_1}(\bmod N)$$

Using γ_1 and public information $\vec{h}$ of KACs, we follow the next steps:

Compute $\mathrm{C_0} = \mathrm{M}^{\mathrm{e}^{s_1}}(\mathrm{mod\ N})$.
Compute the cipher-text $C = {C_0}^e(\bmod N)$.

2.4 | Decryption

Entity 1 has performed the preceding steps to recover M from cipher text:

1 Compute $\gamma = C^d(\bmod N)$.
2 Recover M, using his/her secrete key s_1:

$$\gamma^{d^{s_1}}(\bmod N) \equiv {C_0}^{d^{s_1}}(\bmod N)$$

$$\equiv (M^{e^{s_1}})^{d^{s_1}}(\bmod N)$$

$$\equiv M^{(ed)^{s_1}}(\bmod N)$$

$$\equiv M(\bmod N).$$

3 | REVIEW OF PANG ET AL IBC

Pang et al[11] proposed an IBC mechanism based on GDLP and IFP. Their technique has outlined into four sub-algorithms, namely, Setup, Extraction, Encryption, and Decryption.

Setup: *Setup* algorithm has found similar to the algorithm described in Section 2, calculation of the n-dimensional vector $\vec{h}$, has found different and given as,

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

Extraction: An *Extraction* algorithm has found similar as that in Section 2.

Encryption: Consider, entity 2 wish to transfer message M to entity 1. An entity 2 encrypts M as follows:

1 Calculate the extended ID of entity i's, denoted by EID$_1$by the following form as:
$\mathrm{EID}_1 = (\mathrm{ID}_1)^e(\bmod N) = (y_{11}, y_{12}, y_{13}, y_{14}, \ldots, y_{1t}), y_{1j} \in \{0, 1\}, (1 \leq j \leq t)$.
2 Compute $\gamma = \prod_{1 \leq i \leq n} {h_i}^{y_{1i}}(\bmod N)$

$$= \prod_{1 \le i \le n} (d^{a_i})^{y_{1i}} (\mathrm{mod}\ N)$$

$$= d^{\sum_{1 \le i \le n} a_i y_{1i} \mathrm{mod}(\varphi(N))} (\mathrm{mod}\ N)$$

$$= d^{s_1} (\mathrm{mod}\ N)$$

Using γ and public information $\vec{h}$ of KACs, we follow the next step:

Compute the cipher-text $C = M^{\gamma} (\mathrm{mod}\ N)$.

Decryption: Plaintext M, to be recovered using cipher text by entity 1, has to perform the following:

1 Use private key s_1 to recover M as $M = C^d (\mathrm{mod}\ N)$.

The correctness is shown as follows:
Due to $\gamma = \prod_{1 \le i \le n} h_i^{y_{1i}} (\mathrm{mod}\ N)$

$$= \prod_{1 \le i \le n} (d^{a_i})^{y_{1i}} (\mathrm{mod}\ N)$$

$$= d^{\sum_{1 \le i \le n} a_i y_{1i} mod\ (\varphi(N))} (\mathrm{mod}\ N)$$

$$= d^{s_1} (\mathrm{mod}\ N)$$

We have $C^{e^{s_1}} \equiv (M^{d^{s_1}})^{e^{s_1}} (\mathrm{mod}\ N) \equiv M^{(ed)^{s_1}} (\mathrm{mod}\ N) \equiv M (\mathrm{mod}\ N)$.

Since Pang et al[10] found out two type of deadlock problems in Meshram et al[26] and removed by some modification in IBC technique using GDLP and IFP[10,20-22,27] and also discussed security of the technique without given formal security proof. But in cryptographic technique-based manuscript, formal security analysis, and security proof are required with proper justification.

4 | THE PROPOSE IMPROVED IBC

GDLP along with IFP[10,20-22,27] are used in this proposed IBC. The technique has divided into four sub-algorithms, including Setup, Extraction, Encryption, and the Decryption. These algorithms have described as follows:

Setup: Setup algorithm has modeled nearly the same as described in Section 2. The n-dimensional vector $\vec{h}$, calculation is as same as in Section 3. The only differences are:

1 Chooses w s.t. $\gcd(w, \varphi(N)) = 1$ and $w < \lfloor \varphi(N)/n \rfloor$ w< ⌊φ(N)/n⌋, where $\lfloor x \rfloor$ ⌊x⌋ has used to represent floor-function, imply the biggest integer as small as compute x. Also select a sequence that is, super increasing corresponding to a as $\vec{a'}_i (1 \le i \le n)$satisfies $\sum_{j=1}^{i-1} \vec{a'}_j + v < \varphi(N)$ where $v < \lfloor \varphi(N)/w \rfloor$ w< ⌊φ(N)/n⌋, and $\sum_{j=1}^{n} \vec{a'}_j < \varphi(N)$.
2 Compute $a_i = a'w (\mathrm{mod}\ \varphi(N))$ and $c_i = a_i (\mathrm{mod}\ w)$, $(1 \le i \le n)$.
3 Compute n-dimensional vectors $g = (g_1, g_2, \ldots., g_n)$,where $g_l = d_l a_l (\mathrm{mod}\ \varphi(N))$, $(1 \le l \le n)$.
4 KAC uses public key as $(N, e, \vec{h})$ and distribute it to every entity. KAC, at same time, uses private key as $(\vec{g}, d)$, and stay it as secret.

Extraction: KAC computes the secret key for the entity i. The identity of KAC is represented as a k-dimensional vector. $\mathrm{ID}_i = (x_{i1}, x_{i2}, x_{i3}, x_{i4}, \ \ldots, x_{ik})$, that is, binary vector, $x_{ij} \in \{0, 1\}$, $(1 \le j \le k)$.

1 Compute extended ID of entity i's as Y_i, denoted by:
$Y_i = (\mathrm{ID}_i)^e (\mathrm{mod}\ N) = (y_{i1}, y_{i2}, y_{i3}, y_{i4}, \ \ldots, y_{it}), y_{ij} \in \{0, 1\}, (1 \le j \le t)$.
2 Entity $i's$ secrete keys $s_i$is given by inner product of $\vec{g}_l$ and Y_i as follows:

$$s_i = \vec{g}_l Y_i (\mathrm{mod}\ \varphi(N))$$

$= \sum_{1 \le j \le n} \vec{g}_l y_{ij} \mathrm{mod}\ (\varphi(N))$.

Encryption: Let, entity 2 sends message M to entity 1. Entity 2 performs encryption on M as follows:

1 Calculate the entity i's expanded ID, Y_i given by:
$Y_1 = (\mathrm{ID}_1)^e (\mathrm{mod}\ N) = (y_{11}, y_{12}, y_{13}, y_{14}, \ \ldots, y_{1t}), y_{1j} \in \{0, 1\}, (1 \le j \le t)$.
2 Compute

$$\gamma = \prod_{1 \le i \le n} (h_i^{y_{1i}})^{d_i} (\mathrm{mod} N)$$

$$= \prod_{1 \le i \le n} ((d^{a_i})^{y_{1i}})^{d_i} (\mathrm{mod} N)$$

$$= d^{\sum\limits_{1 \le i \le n} \vec{g}_l y_{1i} \mathrm{mod}(\varphi(N))} (\mathrm{mod} N)$$

$$= d^{s_1} (\mathrm{mod} N)$$

Using γ and public information $\vec{h}$ of KACs, we follow the next steps:

Compute the cipher-text $C = M^{\gamma} (\mathrm{mod}\ N)$.

Decryption: Recovering the plaintext M from the generated cipher text, entity 1 do the following:

1 Uses s_1 as secret key to recover M as $M = C^d (\mathrm{mod}\ N)$.

The correctness has described as follows:
Due to

$$\gamma = \prod_{1 \le i \le n} (h_i^{y_{1i}})^{d_i} (\mathrm{mod}\ N)$$

$$= \prod_{1 \le i \le n} ((d^{a_i})^{y_{1i}})^{d_i} (\mathrm{mod}\ N)$$

$$= d^{\sum\limits_{1 \le i \le n} \vec{g}_l y_{1i} \mathrm{mod}\ (\varphi(N))} (\mathrm{mod}\ N)$$

$$= d^{s_1} (\mathrm{mod}\ N).$$

We have $C^{e^{s_1}} \equiv (M^{d^{s_1}})^{e^{s_1}} (\mathrm{mod}\ N) \equiv M^{(ed)^{s_1}} (\mathrm{mod}\ N) \equiv M (\mathrm{mod}\ N)$.

5 | SECURITY INVESTIGATION AND DISCUSSION

The security of our proposed IBC technique depends on an index problem including IFP, and GDLP[10,20-22,27] in cyclic group Z_N^*that is multiplicative define over finite field. According to Coppersmith attacking method,[28] (n + 1) entity's conspiracy are able to derive the KACs secret information.

5.1 | Conspiracy of some entities

5.1.1 | KACs secret information

The proposed IBC, which includes GDLP and IFP,[10,20,21,27] can be adjusted up to 2^kentities. Here, $(m > n)$ entities i, $(1 \leq i \leq m)$ has involved to conspire for deriving the KACs secret information g_i. Each entity i, $(1 \leq i \leq m)$ possesses the restricted information of g_i given by:

$$g_i Y_i = s_i(\text{mod}(\varphi(N)), (1 \leq i \leq m) \tag{1}$$

Then, it can be represented as system of linear congruence as:

$$\begin{bmatrix} Y_1 & 0 & \cdots & 0 & 0 \\ 0 & Y_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & Y_{n-1} & 0 \\ 0 & 0 & & 0 & Y_n \end{bmatrix} \begin{bmatrix} g_1 & 0 & \cdots & 0 & 0 \\ 0 & g_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & g_{n-1} & 0 \\ 0 & 0 & & 0 & g_n \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_n \end{bmatrix} (\text{mod } \varphi(N)) \tag{2}$$

$$= Dg_i(\text{mod } \varphi(N)) \tag{3}$$

The m entities conspiracy, can determine the secret information g_i of the KAC uniquely, if the matrix D given in Equation (3) contains n linearly independent row vectors over $Z_{\varphi(N)}$.However, Nakamura et al[29] and Coppersmith[28] have shown that even in the cases where matrix Ddoes not include n linearly independent row vectors over $Z_{\varphi(N)}$,$m$entities i, $(1 \leq i \leq m)$ may derive g_i', that is, the secret information of KAC.

Theorem 5.1. *An n-dimensional vectorg_i'over $Z_{\varphi(N)}$, that is, equal to the original secret information of KAC can be derived by the m(>n) entities i, $(1 \leq i \leq m)$.*

Proof: Since, the proposed IBC technique developed based on intractability, the hardness assumption of solving GDLP and IFP simultaneously, $\varphi(N)$ must contain at least one major prime factor. In this case, we assume that $\varphi(N) = 2^c r$ where $c < < |\varphi(N)|$ and r denotes prime. Without loss of generality, we could have matrix D'as given below, for some n entities i, $(1 \leq i \leq n)$ among m entities i, $(1 \leq i \leq m)$:

$$D' = \begin{bmatrix} Y_1 & 0 & \cdots & 0 & 0 \\ 0 & Y_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & Y_{n-1} & 0 \\ 0 & 0 & & 0 & Y_n \end{bmatrix} \tag{4}$$

which satisfies $det(D') \neq 0(\text{mod } r)$. Hence, such n entities can derive g_i', which satisfy the relation given by:

$$g_i' = g_i(\text{mod } r), (1 \leq i \leq n) \tag{5}$$

By computing $s_k' = Y_k g_i'(\text{mod } r)$, arbitrary entity secret key, for example, entity k's secret key s_k gets decided.

In this case, $g_i'$is not necessarily the same as original entity k's secret key s_k. However, the difference between s_i and s_k is some integer multiple of r. Hence, the original entity k's secret key s_k will be computed in at the most c attempts, where in, $\varphi(N) = 2^c r$ and $c < < | \varphi(N)|$.

Thus, up to$(n-1)$entities do not able to derive the secret information of center by attack (Theorem5.1). However, n or more than n entities are able to compute g_i', that is, equivalent to the secret information of center. By using g_i', an arbitrary entity can get attacked.

5.1.2 | Each users secret key

Thus, Section 5.1 has proven that, up to $(n-1)$ entities do not able to derive the secret information of center by attack (Theorem5.1). Also,n or more entities are able to compute g_i', which is same as the center's private information. Here, we take into account the security of every entities secret key s_i against $t < n$ entities conspiracy.

When $\mathrm{t} < n$ entities conspire, entities may have the system of linear congruence as following:

$$\begin{bmatrix} Y_1 & 0 & \cdots & 0 & 0 \\ 0 & Y_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & Y_{n-1} & 0 \\ 0 & 0 & & 0 & Y_n \end{bmatrix} \begin{bmatrix} g_1 & 0 & \cdots & 0 & 0 \\ 0 & g_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & g_{n-1} & 0 \\ 0 & 0 & & 0 & g_n \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_n \end{bmatrix} (\mathrm{mod}\ \varphi(N)) \tag{6}$$

$$= D^{\varepsilon} g_i (\mathrm{mod}\ \varphi(N)) \tag{7}$$

If a t-dimensional vector cover $Z_{\varphi(N)}$ exist, such that for the entity k

$$cD^{\varepsilon} = \sum_{1 \le i \le n} c_i Y_i (\mathrm{mod}\ \varphi(N)) \tag{8}$$

$$= Y_k (\mathrm{mod}\ \varphi(N)) \tag{9}$$

Then $t < n$ entities can compute the entity k's private key s_k by

$$s_{\mathrm{k}} = \sum_{1 \le i \le n} c_i s_i (\mathrm{mod}\ \varphi(N)) \tag{10}$$

Note that $Z_{\varphi(N)}$is not a representing a field, it can be shown easily that $t < n$ entities conspiracy is able to generate at the most 2^tother entities secret keys as in (10). Hence, probability that $t < n$ entities can derive another entity secret key is at most $2^t/2^n = 2^{t-n}$.

Theorem 5.2. *(Coppersmith[28]): The* $(n+1)$ *entities'* i, $(1 \le i \le n+1)$ *is able to derive an n-dimensional vector* g_i'*over* $Z^*_{\varphi(N)}$, *that is, equivalent (not as same) to the real secret information of KAC.*

Proof: When $(n+1)$entities' i, $(1 \le i \le n+1)$ conspire, then the system of linear congruence is given as follows:

$$\begin{bmatrix} Y_1 & 0 & \cdots & 0 & 0 \\ 0 & Y_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & Y_n & 0 \\ 0 & 0 & & 0 & Y_{n+1} \end{bmatrix} \begin{bmatrix} g_1 & 0 & \cdots & 0 & 0 \\ 0 & g_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & g_{n-1} & 0 \\ 0 & 0 & & 0 & g_n \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_{n+1} \end{bmatrix} (\mathrm{mod}\ \varphi(N)) \tag{11}$$

But each Y_i denoting the n-dimensional vector, that is, binary in nature, there exists an $(n+1)$ dimensional vector c over the $Z_{\varphi(N)}$ such that

$$\sum_{1 \le i \le n+1} c_i Y_i = 0 \tag{12}$$

Here,

$$\sum_{1 \le i \le n+1} c_i s_i = 0 (\text{mod } \varphi(N)) \tag{13}$$

and thus

$$\sum_{1 \le i \le n+1} c_i s_i = A \ \varphi(N) \tag{14}$$

The $(n+1)$ entities may have an integer, multiple of $\varphi(N)$, if $A \neq 0$. Then, entities are able to find the factors of N. A similar method, with (Theorem 5.2) for an attack, can be applied. Hence, the secret information of the KAC, can be computed by $(n+1)$ entities conspiracy.

Also, Shamir has given a general attacking method[24] for the given modified system, in such a way, that,$(n+2)$ entities conspiracy can compute the private information of KAC with huge probability.

Theorem 5.3. *(Shamir[2]): The $(n+2)$ entities' i, $(1 \le i \le n+2)$ are able to compute the private information g of KAC with huge probability.*

Proof: If $(n+1)$entities i, $(1 \le i \le n+1)$ conspire, system of linear congruence's for these entities is defined by (15).

$$\begin{bmatrix} Y_1 & 0 & \cdots & 0 & 0 \\ 0 & Y_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & Y_n & 0 \\ 0 & 0 & & 0 & Y_{n+1} \end{bmatrix} \begin{bmatrix} g_1 & 0 & \cdots & 0 & 0 \\ 0 & g_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & g_{n-1} & 0 \\ 0 & 0 & & 0 & g_n \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_{n+1} \end{bmatrix} (\text{mod } \varphi(N)) \tag{15}$$

$$= Da (\text{mod } \varphi(N)). \tag{16}$$

Let, the matrix D contains n linearly independent column vectors over $Z_{\varphi(N)}$, then, there must exist a positive integers $c_i(1 \le i \le n+1)$ such that

$$\begin{bmatrix} Y_1 & 0 & \cdots & 0 & 0 \\ 0 & Y_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & Y_n & 0 \\ 0 & 0 & & 0 & Y_{n+1} \end{bmatrix} \begin{bmatrix} g_1 & 0 & \cdots & 0 & 0 \\ 0 & g_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & g_{n-1} & 0 \\ 0 & 0 & & 0 & g_n \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_{n+1} \end{bmatrix} - \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_{n+1} \end{bmatrix} \varphi(N) \tag{17}$$

The Equation (17) can be rewritten as:

$$\begin{bmatrix} Y_1 & 0 & \cdots & 0 & 0 & s_1 \\ 0 & Y_2 & & 0 & 0 & s_2 \\ \vdots & & \ddots & & \vdots & . \\ 0 & 0 & \cdots & Y_n & 0 & \vdots \\ 0 & 0 & & 0 & Y_{n+1} & s_{n+1} \end{bmatrix} \begin{bmatrix} g_1 & 0 & \cdots & 0 & 0 \\ 0 & g_2 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & g_{n-1} & 0 \\ 0 & 0 & & 0 & g_n \end{bmatrix} = - \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_{n+1} \end{bmatrix} \varphi(N) \tag{18}$$

$$= D'g_i'. \tag{19}$$

The matrix D given in Equation (16), have n linearly independent column vectors over $Z_{\varphi(N)}$ by supposition, a non-singular matrix D' over $Z_{\varphi(N)}$ (ie, det $(D') \neq 0$)with overwhelming probability. Therefore, $g_i' \neq 0(\text{mod}\varphi(N))$. Thus, system of linear congruence's is given below:

$$D'g_i' = 0(\text{mod}\varphi(N)) \tag{20}$$

If $D'$is non-singular over $Z^*_{\varphi(N)}$, then $g_i' = 0(\text{mod}\varphi(N))$, and thus, it invalidates the result given above. Thus, $D'$is singular over $Z^*_{\varphi(N)}$, and the det$(D') = 0(\text{mod}\varphi(N))$with huge probability. It shows that, det(D') is divisible by $\varphi(N)$ with high probability. Furthermore, consider a case where in, the other $(n+1)$ entities among $(n+2)$ conspire. Consider the matrix D''as same as given above. Then, det(D'') is divisible by $\varphi(N)$ with huge probability. Hence, gcd (det(D'), det(D'')) gives $d\varphi(N)$ where d is a small positive integer. By using above steps, efficient evaluation of $\varphi(N)$ is possible. To compute the center's secret information, this additional step is completely the same as attack (Theorem5.3).

6 | PERFORMANCE COMPARISON WITH OTHER TECHNIQUES

The current section discusses nine IBC techniques that are mostly used along with their performance comparison. These nine IBC techniques are: Cocks's IBC technique,[30] Lynn's authenticated IBC technique,[26] Boneh and Boyen's selective-identity secure IBC technique without random oracles,[31] Gentry et al's hierarchical IBC technique,[32] Water's IBC technique,[9] Meshram et al's ID-based cryptographic scheme,[10] Meshram and Meshram's IBC technique,[7] Meshram et al's IBC technique,[20] Meshram et al's IBC technique,[21] Pang et al's IBC technique,[11] and the proposed efficient IBC technique in this article. These techniques show different server performance for evaluating the performance of encryption algorithms, the performance of decryption algorithms, and the cost of computation.

The notations used for evaluation of computation are given below:

τ_P = Execution time for a paring operation.
τ_M = Execution time for a modular multiplication.
τ_e = Execution time for denoting modular exponentiation in group.
τ_m = Execution time for denoting scalar or point multiplications in group.
τ_x = Execution time for denoting XOR operation.
τ_H = Execution time for denoting a map to point hash function.
τ_h = Execution time for denoting one-way hash function.
τ_a = Execution time for a modular addition operation.
τ_i = Execution time for a modular inverses operation.
τ_j = Execution time for a Jacobi symbol operation.

As we comprehend that, it takes more time to perform a paring operation τ_P than the other operations. Some performance simulation results[3] have shown that τ_a and τ_h are trivial in comparison with τ_e,τ_M,τ_x, τ_H,τ_i, and τ_j.

It has noted that both the algorithmic phase of encryption and the algorithmic phase of decryption require more computation than the other phases. Setup and Extract phases have executed only for one time. Thus, the comparison has been performed only by considering the encryption as well as decryption phase. IBC technique proposed in this article has compared with References 7,9-11,20,21,26, and 30-32. The comparative result based on computational cost along with security issues has shown in Table 1.

It has seen from the Table 1, that the proposed IBC technique based on GDLP and IFP bears lower computational cost than in References 7,9-11,20,21,26, and 30-32.

7 | CONCLUSION AND FUTURE WORK

An Improved IBC technique based on GDLP and IFP has proposed. Its security has dependency on the hardness assumption of GDLP with distinct, discrete exponents in the multiplicative group over finite fields and IFP. The propose

TABLE 1 Comparisons among presented ID-based cryptographic technique and similar technique

IBC techniques	$\mathscr{F}_1$	$\mathscr{F}_2$	$\mathscr{F}_3$
Cocks[30]	$\tau_\mathrm{J} + 2\tau_\mathrm{a} + 2\tau_\mathrm{M} + 2\tau_i$	$\tau_\mathrm{J} + \tau_\mathrm{a}$	$2\tau_j + 3\tau_\mathrm{a} + 2\tau_\mathrm{M} + 2\tau_i$
Gentry and Silverberg[32]	$\tau_\mathrm{P} + \tau_\mathrm{H} + \tau_\mathrm{h} + \tau_\mathrm{e} + \tau_\mathrm{m} + \tau_x$	$\tau_\mathrm{P} + \tau_\mathrm{h} + \tau_x$	$2\tau_\mathrm{P} + \tau_\mathrm{H} + 2\tau_\mathrm{h} + \tau_\mathrm{e} + \tau_\mathrm{m} + 2\tau_x$
Lynn[26]	$\tau_\mathrm{P} + \tau_\mathrm{H} + 3\tau_\mathrm{h} + \tau_x$	$\tau_\mathrm{P} + \tau_\mathrm{H} + 3\tau_\mathrm{h} + \tau_x$	$2\tau_\mathrm{P} + 2\tau_\mathrm{H} + 6\tau_\mathrm{h} + 2\tau_x$
Boneh and Boyen[31]	$\tau_\mathrm{P} + 4\tau_\mathrm{e} + 2\tau_\mathrm{M}$	$\tau_\mathrm{P} + \tau_\mathrm{e} + \tau_\mathrm{M} + \tau_i$	$2\tau_\mathrm{P} + 5\tau_\mathrm{e} + 3\tau_\mathrm{M} + \tau_i$
Waters[9]	$2\tau_\mathrm{P} + 3\tau_\mathrm{m}$	$2\tau_\mathrm{P} + \tau_\mathrm{m} + \tau_i$	$4\tau_\mathrm{P} + 4\tau_\mathrm{m} + \tau_i$
Pang et al[11]	$3\tau_\mathrm{e} + \tau_\mathrm{m}$	$4\tau_\mathrm{e} + \tau_\mathrm{m}$	$7\tau_\mathrm{e} + 2\tau_\mathrm{m}$
Meshram and Obaidat[33]	$4\tau_\mathrm{e} + \tau_\mathrm{m}$	$2\tau_\mathrm{e} + \tau_\mathrm{m} + \tau_i$	$6\tau_\mathrm{e} + 2\tau_\mathrm{m} + \tau_i$
Meshram and Meshram[20]	$3\tau_\mathrm{e} + 3\tau_\mathrm{M}$	$3\tau_\mathrm{e} + 2\tau_\mathrm{M}$	$6\tau_\mathrm{e} + 5\tau_\mathrm{M}$
Meshram et al[21]	$2\tau_\mathrm{e} + 3\tau_\mathrm{M}$	$2\tau_\mathrm{e} + 2\tau_\mathrm{M}$	$4\tau_\mathrm{e} + 5\tau_\mathrm{M}$
Proposed technique	$2\tau_\mathrm{e} + \tau_\mathrm{m} + \tau_i$	$2\tau_\mathrm{e} + \tau_\mathrm{m} + \tau_i$	$4\tau_\mathrm{e} + 2\tau_\mathrm{m} + 2\tau_i$

Note: $\mathscr{F}_1$: Computational cost for encryption phase; $\mathscr{F}_2$: Computational cost for decryption phase; $\mathscr{F}_3$: Overall computational cost for encryption and decryption phases.

technique has found satisfying the Shamir's original concepts in a strict sense. The proposed technique does not require any preliminary interactive communications in each data transmission. Also, it has no assumption that tamper-free modules are available. The proposed technique has found better in providing a longer and higher level of security than the other techniques based on a GDLP and IFP. In addition, the proposed technique is efficient, as it requires minimal operations for encryption and decryption algorithms.

This technique also gives the distinctive outcome from the security point of perspective because at the same moment we face the issue of GDLP and IFP in the multiplicative group over finite fields as opposed to the existing public-key cryptosystems, where the trouble of solving the traditional DLP in casual communities and IFP may occur. The proposed technique is also secure from the issue of the deadlock mentioned by Pang et al and secure than Pang et al. By using our proposed system, it is possible to design an ID-based encryption system which is based on light-weight public key management schemes. Light-weight systems have small sizes of public key and private pairs as compared to the other existing IBC techniques available in the literature. In grid security architecture, it is more beneficial. There may be a big amount of employees joining and leaving the grid environment in any interval, and the certificates are commonly used for each work submission. This scenario may inevitably complicate the issue of key management and boost the grid system's bandwidth demands. It was observed that the use of the certificate-free IBC system could simplify these issues.

In addition, the public key of the end user can be created and used immediately in the IBC setting without having public key certificate that is to be transferred to an intended recipient (usually via a handshake for Transport Layer Security [TLS]). However, some traditional constraints of IBC system such as key escrow and the need to distribute private keys through secure channels hindered the allegedly efficient use of ID-based keys. Globus Toolkit (GT) involve the use of single sign-on with delegation proxy credentials, but our enhanced GDLP and IFP-based IBC system is free of certificate and key escrow issues.

ACKNOWLEDGMENTS

The authors would like to thank anonymous reviewers of Security and Privacy for their careful and helpful comments.

ORCID

Chandrashekhar Meshram https://orcid.org/0000-0003-2434-8928
Kailash W. Kalare https://orcid.org/0000-0002-7689-7243

REFERENCES

1. ElGmal T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans Inform Theory*. 1995;31:469-472.
2. Shamir A. Private communication, June 1988.
3. Boneh D, Franklin MK. Identity based encryption from the Weil pairing. *SIAM J Comput*. 2003;32(3):586-615.
4. Meshram C, Meshram S, Zhang M. An ID-based cryptographic mechanisms based on GDLP and IFP. *Inform Process Lett*. 2012;112(19):753-758.

5. Meshram C, Meshram S. An identity-based cryptographic model for discrete logarithm and integer factoring based cryptosystem. *Inform Process Lett*. 2013;113(10–11):375-380.
6. Meshram C. An efficient ID-based cryptographic encryption based on discrete logarithm problem and integer factorization problem. *Inform Process Lett*. 2015;115(2):351-358.
7. Meshram C, Meshram S. An identity based beta cryptosystem. Paper presented at: IEEE Proceedings of 7th International Conference on Information Assurance and Security (IAS 2011), December 5–8, 2011, pp. 298–303.
8. Tsujii S, Itoh T. An ID-based cryptosystem based on the discrete logarithm problem. *IEEE J Selected Areas Commun*. 1989;7(4):467-473.
9. Waters B. Efficient identity-based encryption without random oracles. Paper presented at: Proceedings of the 25th Annual International Cryptology Conference on Advances in cryptology-CRYPTO 2005, Santa Barbara, California, August 14-18, 2005, Lecture Notes in Computer Science, Vol. 3494, Springer. pp. 114–127.
10. Meshram C, Meshram SA. Some modification in ID-based cryptosystem using IFP & DDLP. *Int J Adv Comput Sci Appl*. 2011;2(8):25-29.
11. Pang L, Li H, Wang Y. nMIBAS: a novel multi-receiver ID-based anonymous signcryption with decryption fairness. *Comput Inform*. 2013;32(3):441-460.
12. Meshram C, Powar PL, Obaidat MS, Lee CC, Meshram SG. Efficient online/offline IBSS protocol using partial discrete logarithm for WSNs. *IET Netw*. 2018;7(6):363-367.
13. Meshram C, Lee CC, Meshram SG, Li CT. An efficient ID-based cryptographic transformation model for extended chaotic map-based cryptosystem. *Soft Comput*. 2019;23(16):6937-6946.
14. Meshram C, Li CT, Meshram SG. An efficient online/offline ID-based short signature procedure using extended chaotic maps. *Soft Comput*. 2019;23(3):747-753.
15. Meshram C, Lee CC, Meshram SG, Khan MK. An identity-based encryption technique using subtree for fuzzy user data sharing under cloud computing environment. *Soft Comput*. 2019;23(24):13127-13138.
16. Shamir A. Identity-based cryptosystem and signature scheme. Paper presented at: Proceedings of the Crypto'84 Advances in cryptology, Lecture Notes in Computer Science, vol. 196, Springer, 1984; pp. 47–53.
17. Meshram C, Lee CC, Meshram SG, Meshram A. OOS-SSS: an efficient online/offline subtree-based short signature scheme using Chebyshev chaotic maps for wireless sensor network. *IEEE Access J*. 2020;8(1):80063-80073.
18. Meshram C, Lee CC, Ranadive AS, Li CT, Meshram SG, Tembhurne GV. A subtree-based transformation model for cryptosystem using chaotic maps under cloud computing environment for fuzzy user data sharing. *Int J Commun Syst*. 2020;33(7):e4307.
19. Farjana N, Roy S, Mahi MJN, Whaiduzzaman M. An identity-based encryption scheme for data security in fog computing. Paper presented at: Proceedings of International Joint Conference on Computational Intelligence, 2020, 215–226.
20. Meshram C, Meshram SA. Constructing new an ID-based cryptosystem for IFP and GDLP based cryptosystem. *J Discrete Math Sci Cryptogr*. 2017;20(5):1121-1134.
21. Meshram C, Tseng YM, Lee CC, Meshram SG. An IND-IDCPA secure ID-based cryptographic protocol using GDLP and IFP. *Informatica*. 2017;28(3):471-484.
22. Meshram C, Lee CC, Li CT, Chen CL. A secure key authentication scheme for cryptosystems based on GDLP and IFP. *Soft Comput*. 2017;21(24):7285-7291.
23. Meshram C, Meshram SA, Gupta D. An ID-based Beta cryptosystem using generalized discrete logarithm problem and integer factorization problem. *J Inform Assur Security*. 2012;7(5):275-283.
24. Meshram C, Meshram SG, Lee CC. Constructing provably secure ID-based Beta cryptographic scheme in random Oracle. *Int J Netw Security*. 2018;20(3):568-574.
25. Ramadan M, Liao Y, Li F, Zhou S, Abdalla H. IBEET-RSA: identity-based encryption with equality test over RSA for wireless body area networks. *Mobile Netw Appl*. 2020;25:223-233.
26. Lynn B. Authenticated ID-based encryption. Paper presented at: Cryptology ePrint Archive, Report 2002/072, 2002. http://eprint.iacr.org/2002/072.
27. Meshram C, Meshram SA, Ram C. Constructing identity-based cryptographic scheme for Beta cryptosystem. *Int J Appl Math*. 2012;25(5):609-624.
28. Coppersmith D. Cryptography. *IBM J Res Dev*. 1987;31(2):244-248.
29. Nakamura K, Okamoto E, Tanaka K, Miura S. Private communication, August 1987.
30. Cocks C. An identity based encryption scheme based on quadratic residues. Paper presented at: International Conference on Cryptography and Coding (Proceedings of IMA), Lecture Notes in Computer Science, vol. 2260, Springer, 2001, pp. 360–363.
31. Boneh D, Boyen X. Efficient selective-ID secure identity based encryption without random oracles. Paper presented at: Advances in cryptology-EUROCRYPT 2004, Lecture Notes in Computer Science, vol. 3027, Springer, 2004; pp. 223–238.
32. Gentry C, Silverberg A. Hierarchical ID-based cryptography. Paper presented at: Advances in cryptology-ASIACRYPT'02, Lecture Notes in Computer Science, vol. 2501, Springer, 2002, pp. 548–566.
33. Meshram C, Obaidat M. An ID-based quadratic-exponentiation randomized cryptographic scheme. In: IEEE Proceedings of International Conference on Computer, Information, and Telecommunication Systems (CITS 2015), July 15–17, 2015, pp. 1–5.

How to cite this article: Meshram C, Ibrahim RW, Meshram SG, Kalare KW, Bagde SD. An efficient ID-based cryptographic technique using IFP and GDLP. *Security and Privacy*. 2020;3:e119. https://doi.org/10.1002/spy2.119