Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 6, pp. 1851–1866
DOI : 10.47974/JDMSC-1871

An efficient ID-based cryptographic encryption based on group ring

Sunil Kumar [§]
Defence Research and Development Organization
Near Metcalfe House
Civil Lines 110054
New Delhi
India

and

Department of Mathematics
University of Delhi
Delhi 110007
India

Gaurav Mittal [†]
Defence Research and Development Organization
Near Metcalfe House
Civil Lines 110054
New Delhi
India

and

Department of Mathematics
Indian Institute of Technology Roorkee
Roorkee 247667
Uttarakhand
India

Arvind Yadav*
Department of Mathematics
Hansraj College
University of Delhi
Delhi 110007
India

[§] *E-mail:* sunilsangwan6174@gmail.com
[†] *E-mail:* gaurav.mittaltwins@gmail.com
* *E-mail:* drarvind@hrc.du.ac.in (Corresponding Author)

Abstract

For most of the traditional IBEs (identity-based encryptions), security totally relies on the safekeeping of private keys. In case the private key is exposed, all the previously generated ciphertext need to be reissued. Due to increased usage of unprotected devices or mobiles, the key exposure is frequent. Therefore, it is important to mitigate the threat originated due to the key exposure in case of IBE. To deal with this issue, in this paper, we construct a novel IBE based on group ring that also provides forward security. We show that the security of our novel IBE is based on the hardness of discrete logarithm problem in group ring. Moreover, against the chosen plaintext attack, we show that it is semantically secure in random oracle model. Finally, we compare our IBE with several other existing IBEs in terms of execution cost.

Subject Classification: *(2010) 94A60, 20C05.*

Keywords: *Cryptography, Encryption, Identity-based encryption, Random oracle.*

1. Introduction

An identity-based encryption (IBE) offers a suitable way to encrypt a message through public key encryption with no trouble of distribution of public keys. Through IBE, any sender can encrypt a message by taking public key of the receiver as his/her identity. This means that sender can send the messages to receiver without checking his/her public key certificate. It is well known that the concept of IBE simplified the key management problem and this concept was proposed by Shamir in 1984 [23]. In IBE, the public key is the identity of the receiver that can be an email or certain personal number. The private key corresponding to above-mentioned identity of the receiver is calculated and issued to receiver by a trusted authority known as private key generator (PKG) through a trusted channel (for example, in person or trusted courier). Therefore, in IBE only public key parameters of the PKG needs to be certificated.

Some of the first practical IBEs are proposed in [2, 3, 4, 5, 6]. The schemes of Boneh et al. [2, 3, 4] are based on bilinear maps whereas the scheme of Cocks [6] is based on quardatic residues [11]. Motivated by these schemes, several other efficient IBEs are proposed in the literature (see [10, 14, 16, 18, 19, 22, 24, 25]). In these schemes, a random number selected by PKG or the entity is part of the public key in addition to entity's identity. Consequently, the area of IBE has drawn the attention of various researchers in the recent years. However, most of the above-mentioned IBEs have a common drawback that their security directly or indirectly depends on hard problems such as discrete logarithm problem (DLP) or integer factorization problem (IFP) or their combination. It is well known that these problems are solvable on a sufficiently large quantum computer

(see [1]). Therefore, it is important to construct IBEs whose security depend on other hard problems (possibly quantum safe).

Our contribution. In this paper, we propose a novel IBE based on group ring [20]. The structure of group ring was introduced in the field of cryptography in the last decade [12]. After its introduction, a number of group ring based cryptographic primitives have been proposed in the literature (see [9, 13, 15, 21, 22] and the references therein). The advantage of group ring is that their corresponding hard problems are computationally infeasible to solve even for small size groups (see [22]). Moreover, there is no known quantum algorithm to solve these hard problems within polynomial time [12, 22]. Consequently, the area of group ring based cryptography is drawing the attention of researchers all over the globe. Recently, an IBE based on group ring is introduced in [22], however the size of ciphertext resulted through this IBE is 3 times than that of the plaintext. In this paper, we introduce a group ring based IBE that is efficient as well as provides randomized ciphertext that has size twice than that of the plaintext. We show that time costs of decryption and encryption algorithms of our IBE are similar to that of ElGamal. By discussing a formal proof, we demonstrate that under chosen plaintext attack (CPA), our IBE is semantically secure, provided the DLPGR assumption holds (see section 2.4).

Plan of the paper: We introduce our novel IBE along with the security notion (i.e., IND-ID-CPA security) in Section 2. Section 3 discusses the formal semantic security of our IBE. In Section 4, we exhibit performance comparison of our IBE with several other IBEs. The last section concludes the paper.

2. Novel Scheme based on group ring and security notion

In this section, we propose our novel IBE based on group ring. We start by discussing some preliminaries.

2.1 *Group ring and its related definitions [20, 12]*

Let $\mathfrak{G}$ be a group and $\mathfrak{R}$ be a ring with unity. We consider the set

$$\mathfrak{RG} = \{\sum_{f} r(g_t)g_t : r(g_t) \in \mathfrak{R}, g_t \in \mathfrak{G}\}.$$

Here $\sum_{f}$ means the sum is finite. This means the set $\mathfrak{RG}$ consists of all the finite $\mathfrak{R}$-linear combinations of elements of $\mathfrak{G}$. To define an algebraic structure on $\mathfrak{RG}$, we define

$$\gamma_1 + \gamma_2 = \sum_f r(g_t)g_t + \sum_f r(g_t)'g_t = \sum_f (r(g_t) + r(g_t)')g_t, \tag{2.1}$$

where $\gamma_1 = \sum_f r(g_t)g_t$ and $\gamma_2 = \sum_f r(g_t)'g_t$, where $r(g_t), r(g_t)' \in \mathfrak{R}$ and $g_t \in \mathfrak{G}$. Moreover, for the same γ_1 as defined above and $\gamma_2 = \sum_f r(g_s)g_s$, we define

$$\gamma_1 * \gamma_2 = (\sum_f r(g_t)g_t) * (\sum_f r(g_s)g_s) = \sum_f r(g_t)r(g_s)(g_t g_s). \tag{2.2}$$

The set $\mathfrak{RG}$ is called as group ring with addition and multiplication operations given by (2.1) and (2.2), respectively.

2.1.1 Example

Let $\mathfrak{G} = \{e, a, a^2, a^3\}$ be a cyclic group of order 4 and $\mathfrak{R} = \mathbb{Z}_2 = \{0,1\}$ be a ring. Then we have $\mathbb{Z}_2\mathfrak{G} = \{0, e, a, a^2, a^3, e+a, e+a^2, e+a^3, a+a^2, a+a^3, a^2+a^3, e+a+a^2, e+a+a^3, a+a^2+a^3, e+a^2+a^3, e+a+a^2+a^3\}$. Clearly, the group ring $\mathbb{Z}_2\mathfrak{G}$ has 16 elements.

2.1.2 Unit of group ring and its order

Let γ be an element of $\mathfrak{RG}$. Let δ be another element of $\mathfrak{RG}$ such that $\gamma * \delta = 1$. Then γ is said to be a unit of $\mathfrak{RG}$ and δ is its inverse, i.e., $\gamma^{-1} = \delta$. The order of a unit γ, i.e., $O(\gamma)$ is the smallest positive integer such that $\gamma^{O(\gamma)} = 1$.

2.1.3 Discrete logarithm problem in group ring (DLPGR)

Let $\gamma_1, \gamma_2 \in \mathfrak{RG}$ and there exist a positive integer z such that $\gamma_2 = \gamma_1^z$. Then DLPGR is the problem of deducing z from the known values of γ_1 and γ_2. DLPGR is a NP problem and there is no known quantum algorithm to solve it in polynomial time. The expected security provided by DLPGR is given in the following Table 1 (see [22] for details):

Table 1

Security provided by DLPGR

Size of parameters	Security (in bits)
$\lvert\mathfrak{G}\rvert \geq 2^7$, $O(\gamma_1) \geq 2^{225}$	128
$\lvert\mathfrak{G}\rvert \geq 2^8$, $O(\gamma_1) \geq 2^{485}$	256

Here $|\mathfrak{G}|$ means the number of elements of G and γ_1 is same as in subsection 2.1.3. In comparison to DLP, DLPGR is difficult to break due to the structural properties of group ring (see [12]).

2.2 *Novel IBE scheme*

Our novel IBE group ring based scheme consists of the four algorithms. These algorithms are defined in the following four subsections:

2.2.1 Setup

Let (m,n) be the security parameter for $m<n$ and PKG denote the private key generator. In this algorithm, PKG does the following:

(a) Constructs a hash function $\mathcal{H}:\{0,1\}^* \to \{0,1\}^n$. Here $\{0,1\}^*$ is the set of all binary sequences of arbitrary length.

(b) Generates a finite group $\mathfrak{G}$ of order $\mathcal{O}$ and takes a unit $\gamma \in \mathbb{Z}_2\mathfrak{G}$ (see Example 2.1.1). The inverse γ^{-1} of γ is also known publically. Let $O(\gamma)$ be the order of γ. In contrary to groups, computing inverse in group ring is a hard problem (see [12, 22]). Thus, γ is chosen such that its inverse is also known.

(c) Creates a secret n-dimensional random vector $\mathfrak{R}=(r_1,r_2,\ldots,r_n)$, where $0<r_j<O(\gamma)\ \forall\ j$.

(d) Generates a public vector $\mathfrak{S}=(s_1,s_2,\ldots,s_n)$, where $s_j=\gamma^{r_j}$ for each $1\le j\le n$.

The public parameters are $pm=(\mathfrak{G},\mathbb{Z}_2\mathfrak{G},\gamma,\gamma^{-1},\mathcal{H},\mathfrak{S})$. The PKG's master key is $mk=\mathfrak{R}$.

2.2.2. Extract

Let $\mathrm{ID}\in\{0,1\}^*$ be the identity for which private and public keys need to be generated. The extract algorithm works as follows:

(a) Computes hash value $\mathcal{H}(\mathrm{ID})=(h_1,h_2,\ldots,h_n)$.

(b) Computes private key corresponding to ID as $r_{\mathrm{ID}}=\sum_{j=1}^{n}h_j r_j$.

(c) Computes public key corresponding to ID as

$$s_{\mathrm{ID}}=\prod_{j=1}^{n}(s_j)^{h_j}=\prod_{j=1}^{n}(\gamma^{r_j})^{h_j}=\gamma^{r_{\mathrm{ID}}}. \tag{2.3}$$

2.2.3 Encryption

Let the message $\mathcal{M} \in \{0,1\}^{\mathcal{O}}$ (binary strings of length $\mathcal{O}$) need to be encrypted. If message size is greater than $\mathcal{O}$, then it can be written in blocks of length $\mathcal{O}$ and padding can be done in the last block (if required). This algorithm takes a random $0 < \eta < O(\gamma)$ and computes ciphertext $\mathcal{C} = (\mathcal{C}_1, \mathcal{C}_2) = ((\gamma^{-1})^{\eta}, \mathcal{M} * s_{\mathrm{ID}}^{\eta})$.

2.2.4 Decryption

This algorithm uses private key r_{ID} and (2.3) to decrypt $\mathcal{C}$ as follows:

$$C_2 * C_1^{r_{\mathrm{ID}}} = (\mathcal{M} * s_{\mathrm{ID}}^{\eta}) * ((\gamma^{-1})^{\eta r_{\mathrm{ID}}}) = (\mathcal{M} * s_{\mathrm{ID}}^{\eta}) * ((s_{\mathrm{ID}})^{-\eta}) = \mathcal{M}.$$

2.3 *Security notion*

Our aim is to show that, under chosen plaintext attack (CPA), our novel IBE is semantically secure in the random oracle model (ROM). For this, we define the notion of semantic security and its model against CPA in the following subsections.

2.3.1 ε-advantage

Let X be an adversary. Suppose that in a certain challenge, $\sigma \in \{0,1\}$ is the answer and X reports $\sigma' \in \{0,1\}$ as the answer (through a certain rule). We say that X has $\varepsilon \geq 0$ advantage in wining the challenge if $\mathrm{Advt}(X) = |\Pr[\sigma' = \sigma] - 0.5| = \varepsilon$.

2.3.2 (ρ, ε)-semantically secure

Under adaptive CPA, an IBE is said to be (ρ, ε)-semantically secure if any probabilistic polynomial time (PPT) adversary has at most an ε advantage in breaking the IBE in at most ρ queries of the private key.

2.3.3 IBE Semantically security attack model against CPA (IND-ID-CPA game)

This attack model requires a game to be played between the adversary X and the challenger Y. The game is played as follows:

Setup: Y generates public parameters *pm* along with the master key. Y gives *pm* to X.

Phase 1: X makes private key extraction queries (adaptively) related to identity. To be more precise, X can send queries $\langle \mathrm{ID}_j \rangle$ to Y for some j. Moreover, any new query of X may depend on the previous queries. In response, Y sends private key corresponding to identity ID_j to X.

Challenge: X sends another identity ID to Y along with two messages $\mathcal{M}_0$ and $\mathcal{M}_1$. Note that this ID is different from all the identities queried by X in Phase 1. Y encrypts $\mathcal{M}_\tau$ by taking a random $\tau \in \{0,1\}$ and gives the ciphertext to X.

Phase 2: As in Phase 1, X again makes queries (adaptively) to Y related to identities with the restriction that he/she is not allowed to query the identity ID used in the Challenge phase.

Guess: X makes a guess $\tau' \in \{0,1\}$.

If $\tau = \tau'$, then X wins the game. Otherwise Y wins. In other words, we say that IBE is semantically secure against CPA (or IND-ID-CPA secure) if $\tau \neq \tau'$.

2.4 *Complexity Assumption*

We show that the security of our novel IBE depends on the following DLPGR assumption that is a complexity-theoretic assumption:

DLPGR assumption: Let γ be a unit of group ring $\mathbb{Z}_2\mathfrak{G}$. The challenger randomly selects $\tau \in \{0,1\}$ and positive integers z_1, z_2, z_3 all greater than 1. If $\tau = 1$, the challenger outputs $(\gamma^{z_1}, \gamma^{z_2}, \gamma^{-z_2}, \gamma^{z_1 z_2})$. Otherwise, he/she outputs $(\gamma^{z_1}, \gamma^{z_2}, \gamma^{-z_2}, \gamma^{z_3})$. The adversary guesses $\tau' \in \{0,1\}$ of τ. The ε advantage of adversary is same as discussed in subsection 2.3.1.

Remark 2.1: It is worth to note that computing inverse of a general unit element of group ring is also a hard problem (see [12, 22]). Keeping this thing in mind, we have assumed that the challenger also outputs inverse of γ^{z_2} in DLPGR assumption. The method to find the units whose inverse is also known is discussed in [12, 22].

Decisional assumption: If any PPT adversary has at most ε advantage in solving the game discussed in subsection 2.3.3, then decisional ε-DLPGR assumption holds in the group ring.

3. Semantic security

In this section, we show that our novel IBE is semantically secure under CPA. We follow the seminal work of [4] to discuss the security proof. Our main result is as follows:

Theorem 3.1: *Let* $\mathcal{H}$ *in subsection 2.2.1 be a random oracle and* (m,n) *be the security parameter for* $m<n$. *Then under the decisional* ε_1*-DLPGR assumption in ROM, our IBE is* (m,ε)*-semantically secure, where* $\varepsilon_1 = 0.5\varepsilon(1-e^{-1}-2^{m-n})$.

Proof: Let $\mathfrak{A}$ be an (m,ε)-adversary against our IBE. This means that $\mathfrak{A}$ has at least ε-advantage in at most m queries he/she makes in the IND-ID-CPA game. We construct a PPT simulator $\mathfrak{B}$ to play the IND-ID-CPA game. As a challenge, $\mathfrak{B}$ takes the input $(\gamma, \mathfrak{P}=\gamma^{z_1}, \mathfrak{Q}=\gamma^{z_2}, \mathfrak{Q}^{-1}=\gamma^{-z_2}, \delta)$ (see DLPGR assumption). Here δ is an element of the group ring $\mathbb{Z}_2\mathfrak{G}$ unknown to $\mathfrak{B}$. $\mathfrak{B}$ outputs a guess τ' of τ. For a decent guess τ', an IND-ID-CPA game is played by $\mathfrak{B}$ with $\mathfrak{A}$. The complete sketch of the functioning of $\mathfrak{B}$ and game is as follows:

Setup: $\mathfrak{B}$ randomly and independently chooses m n-dimensional binary vectors. Let these be denoted by $\mathcal{R}_j = (h_{1j}, h_{2j}, \ldots, h_{nj})^T$, where $1 \le j \le m$ and $(\cdot)^T$ denotes transpose of a vector $(\cdot)$. $\mathfrak{B}$ selects a group $\mathfrak{G}$ and takes unit γ of the group ring $\mathbb{Z}_2\mathfrak{G}$. Additionally, $\mathfrak{B}$ randomly selects positive integers y_j for $1 \le j \le n$, where $y_j < O(\gamma)$. Using $\mathcal{R}_j$'s, $\mathfrak{B}$ picks x_j for $1 \le j \le n$, where $x_j < O(\gamma)$ such that

$$(x_1, x_2, \ldots, x_n) \times \mathcal{R}_j = 0 \text{ for all } 1 \le j \le n. \tag{3.1}$$

The existence of such an n-tuple $(x_1, x_2, \ldots, x_n)$ follows from the linear algebra (in fact there exist many solutions of (3.1) and $\mathfrak{B}$ takes any one of them). Using x_j's and y_j's, $\mathfrak{B}$ sets $\mathfrak{S} = (\mathfrak{P}^{x_1}\gamma^{y_1}, \mathfrak{P}^{x_2} * \gamma^{y_2}, \ldots, \mathfrak{P}^{x_n} * \gamma^{y_n})$.. This $\mathfrak{S}$ is one of the public parameters. The associated master key is $\mathfrak{R} = (r_1, r_2, \ldots, r_n) = (z_1x_1 + y_1, z_1x_2 + y_2, \ldots, z_1x_m + y_m)$ as $(\mathfrak{P}^{x_1} * \gamma^{y_1}, \mathfrak{P}^{x_2} * \gamma^{y_2}, \ldots, \mathfrak{P}^{x_m} * \gamma^{y_m}) = (\gamma^{z_1x_1+y_1}, \gamma^{z_1x_2+y_2}, \ldots, \gamma^{z_1x_m+y_m})$. Note that $\mathfrak{R}$ is unknown to $\mathfrak{B}$ as z_1 is not known to it. $\mathfrak{B}$ gives $pm = (\mathfrak{G}, \mathbb{Z}_2\mathfrak{G}, \gamma, \gamma^{-1}, \mathcal{H}, \mathfrak{S})$ (public parameters) to $\mathfrak{A}$, where $\mathcal{H}$ is a random oracle.

Next, $\mathfrak{B}$ uses the following algorithm to reply to the hash value queries of $\mathfrak{A}$. Let q be the maximum queries that $\mathfrak{A}$ can make.

Random oracle queries: $\mathfrak{B}$ randomly selects a subset $\wp$ of $(1,2,\ldots,q)$ of size m. $\mathfrak{B}$ creates a list $\mathfrak{L}$ of three tuples $\langle \mathrm{ID}_j, \mathcal{H}(\mathrm{ID}_j), \tau_j \rangle$ in order to answer the random oracle queries. Here ID_j represents an identity and $\tau_j \in \{0,1\}$. Initially, $\mathfrak{L}$ is empty. $\mathfrak{B}$ responds to a random oracle query as follows:

(a) if ID_j is already queried earlier, $\mathfrak{B}$ responds with the available hash value $\mathcal{H}(\mathrm{ID}_j)$ in $\mathfrak{L}$.

(b) if ID_j is not queried earlier, then $\mathfrak{B}$ generates a random coin $c \in \{0,1\}$. Let ID_j be the wth new random oracle's query. If $c = 0$, then $\mathfrak{B}$ randomly selects a n-tuple $\mathcal{H}(\mathrm{ID}_j) = (h_{1i}, h_{2i}, \ldots, h_{ni})$ for some i (note that this tuple is not present in $\mathfrak{L}$) and sends it to $\mathfrak{A}$. Also, the tuple $\langle \mathrm{ID}_j, \mathcal{H}(\mathrm{ID}_j), 0 \rangle$ is added to list $\mathfrak{L}$. If $c = 1$, then $\mathfrak{B}$ responds with $\mathcal{H}(\mathrm{ID}_j) = (h_{1w'}, h_{2w'}, h_{nw'})$, where w' denotes the smallest wth element of the set $\wp$. In this case, the tuple $\langle \mathrm{ID}_j, \mathcal{H}(\mathrm{ID}_j), 1 \rangle$ is added to list $\mathfrak{L}$ by $\mathfrak{B}$.

Next, we discuss the working mechanism of $\mathfrak{B}$ in the IND-ID-CPA game.

Phase 1: $\mathfrak{A}$ makes a private key extraction query corresponding to ID_j. $\mathfrak{B}$ responds as follows:

(i) if ID_j is in $\mathfrak{L}$ and $\tau_j = 1$, then $\mathfrak{B}$ calculates $r_{\mathrm{ID}_j} = \sum_{\ell=1}^{n} h_{i\ell}' y_\ell$ and sends it to $\mathfrak{A}$. Here, $h_{i\ell}'$ is ith bit of the available hash value $\mathcal{H}(\mathrm{ID}_j)$.

(ii) if ID_j is not in $\mathfrak{L}$ and there exists an unused vector $\mathcal{R}_j$ (means this vector is not used in the reply of previous queries) that was chosen in Setup phase, then using this $\mathcal{R}_j$, $\mathfrak{B}$ sets $\mathcal{H}(\mathrm{ID}_j) = (h_{1i}, h_{2i}, \ldots, h_{ni})$ and $\tau_j = 1$. $\mathfrak{B}$ sends $r_{\mathrm{ID}_j} = \sum_{\ell=1}^{n} h_{\ell i} y_\ell$ to $\mathfrak{A}$ and adds $\langle \mathrm{ID}_j, \mathcal{H}(\mathrm{ID}_j), 1 \rangle$ to $\mathfrak{L}$.

(iii) if none of the above two possibilities occur, then $\mathfrak{B}$ restarts the game and again chooses the set $\wp$. It is important to note that $\mathfrak{B}$ can restart the game $\lambda = \left(\binom{q}{m} - 1\right)$ times. If $\mathfrak{B}$ needs to restart the game $(\lambda + 1)$ th time (or more), $\mathfrak{B}$ outputs a random bit τ' and aborts.

Validity of assigned values to r_{ID_j} in Phase 1: Using master key and (3.1), we deduce that

$$\begin{aligned} r_{\mathrm{ID}_j} &= \sum_{\ell=1}^{n} h_{\ell j} r_\ell = \sum_{\ell=1}^{n} h_{\ell j} (z_1 x_\ell + y_\ell) = z_1 \sum_{\ell=1}^{n} h_{\ell j} x_\ell + \sum_{\ell=1}^{n} h_{\ell j} y_\ell \\ &= z_1 (x_1, x_2, \ldots, x_n) \times \mathcal{R}_j + \sum_{\ell=1}^{n} h_{\ell j} y_\ell = \sum_{\ell=1}^{n} h_{\ell j} y_\ell. \end{aligned} \tag{3.2}$$

The equation (3.2) justifies the values assigned to r_{ID_j} in Phase 1.

Challenge: $\mathfrak{A}$ gives messages $\mathcal{M}_0$ and $\mathcal{M}_1$ to $\mathfrak{B}$ along with an identity ID that is not queried in Phase 1. $\mathfrak{B}$ randomly selects $\mathcal{R}_0^T = (h_{10}, h_{20}, \ldots, h_{n0})$, where $h_{j0} \in \{0,1\}$ for each j. $\mathfrak{B}$ checks whether R_0 can be

written as linear combination of $\mathcal{R}_j$ for $1 \le j \le m$. If yes, then $\mathfrak{B}$ outputs a random $\tau' \in \{0,1\}$ and aborts; otherwise $\mathfrak{B}$ calculates $x = \sum_{\ell=1}^{n} h_{\ell 0} x_\ell$, $y = \sum_{\ell=1}^{n} h_{\ell 0} y_\ell$, $s_{\text{ID}} = \mathfrak{P}^x * \gamma^y$. Also, $\mathfrak{B}$ archives the tuple $\langle \text{ID}, \mathcal{R}_0^T, 0 \rangle$ in $\mathfrak{L}$. To challenge $\mathfrak{A}$, $\mathfrak{B}$ takes an arbitrary element ζ from the set $\{0,1\}$ and sends him/her the ciphertext $\mathcal{C} = (\mathfrak{Q}^{-1}, \mathcal{M}_\zeta * \delta^x * \mathfrak{Q}^y)$.

Phase 2: As in Phase 1, $\mathfrak{A}$ makes adaptive queries related to extraction of private keys. The only restriction is that $\mathfrak{A}$ can not make query related to private key of challenged identity ID. The response of $\mathfrak{B}$ is similar as in Phase 1.

Guess: $\mathfrak{A}$ outputs $\zeta' \in \{0,1\}$. If $\zeta = \zeta'$, then $\mathfrak{B}$ guesses $\tau' = 1$ and otherwise $\tau' = 0$.

To this end, we calculate the minimum advantage possessed by $\mathfrak{B}$. It is clear from the above description that the IND-ID-CPA game aborts (**GA**) in the following two events:

(i) $\mathfrak{B}$ restarts the game $(\lambda + 1)$ th time or more in Phase 1 or 2.

(ii) R_0 is a linear combination of $\mathcal{R}_j$ for $1 \le j \le m$.

At this point, we make the following two claims: Claim (A): the probability of event (i) is at most e^{-1}; Claim (B): the probability of event (ii) is at most 2^{m-n}.

Proof of Claim (A): For a single choice of $\wp$ (see Random oracle queries), probability that the game restarts is at most $1 - \frac{1}{\lambda+1} = \frac{\lambda}{\lambda+1}$. Since $\wp$ can be selected in $\lambda + 1$ ways (i.e., game restarts $\lambda + 1$ times), the maximum probability of event (A) is $\left(\frac{\lambda}{\lambda+1}\right)^{\lambda+1} \approx e^{-1}$.

Proof of Claim (B): We consider the matrix $\mathfrak{M} = (\mathcal{R}_1, \cdots, \mathcal{R}_m, \mathcal{R}_0)$ of order $n \times (m+1)$. Since $\mathcal{R}_0$ is a linear combination of rest of the columns of $\mathfrak{M}$, its rank is at most m (as $n > m$). Let rank of $\mathfrak{M}$ be $\mathfrak{R} \le m$. Without loss of generality, we assume that rows 1 to $\mathfrak{R}$ of $\mathfrak{M}$ are linearly independent. Let us consider a vector $\mathcal{R}'$ of dimension $\mathfrak{R}$ whose elements are linearly independent elements of $\mathfrak{R}_j$, where $1 \le j \le m$. We note that number of such vectors are at most $2^{\mathfrak{R}} \le 2^m$. Further, we know that the number of n-dimensional vectors are 2^n. Thus, we have shown that the span of m n -dimensional vectors (binary as well as random) have a maximum of 2^m binary vectors. Consequently, the probability of event (B) is 2^{m-n}.

It follows from Claims (A) and (B) that $\Pr(\overline{\text{GA}})$ (probability that game does not abort) is at least $1 - e^{-1} - 2^{m-n}$. Finally, we compute the

probability that $\tau = \tau'$ when game does not abort. We Claim (C) that Pr[$\tau = \tau' \mid \overline{\mathrm{GA}}]$ fulfills $|\Pr[\tau = \tau' \mid \overline{\mathrm{GA}}] - 0.5| \geq 0.5\varepsilon$.

Proof of Claim (C) : Suppose that $\mathfrak{B}$ does not abort the game. We have the following cases:

Case 1: if $\tau = 1$, then $\delta = \gamma^{z_1 z_2}$. This means that $\mathcal{C} = (\gamma^{-z_2}, \mathcal{M}_\zeta * \delta^x * \mathfrak{Q}^y) = (\gamma^{-z_2}, \mathcal{M}_\zeta * \gamma^{z_1 z_2 x + z_2 y})$. Note that with identity ID_0, $\mathcal{C}$ is a valid ciphertext of $\mathcal{M}_\zeta$. Consequently, $|\Pr[\zeta = \zeta' \mid \tau = 1 \text{ and } \overline{\mathrm{GA}}] - 0.5| \geq \varepsilon$.

Case 2: if $\tau = 0$, then $\delta = \gamma^{z_3}$ for some randomly chosen z_3. Since δ reveals no information about ζ, we have $\Pr[\zeta = \zeta' \mid \tau = 0 \text{ and } \overline{\mathrm{GA}}] = 0.5 = \Pr[\zeta \neq \zeta' \mid \tau = 0 \text{ and } \overline{\mathrm{GA}}]$. Let $\mathcal{P} := \Pr[\tau = \tau' \mid \overline{\mathrm{GA}}]$. We note that $\mathcal{P} = \Pr[\tau = \tau' = 0 \mid \overline{\mathrm{GA}}] + \Pr[\tau = \tau' = 1 \mid \overline{\mathrm{GA}}]$. This further implies that $\mathcal{P} = \Pr[\tau = 0 \text{ and } \zeta \neq \zeta' \mid \overline{\mathrm{GA}}] + \Pr[\tau = 1 \text{ and } \zeta = \zeta' \mid \overline{\mathrm{GA}}]$. This may be further written as $\mathcal{P} = (\Pr[\zeta \neq \zeta' \mid \tau = 0 \text{ and } \overline{GA}] \times \Pr[\tau = 0 \mid \overline{\mathrm{GA}}]) + (\Pr[\zeta = \zeta' \mid \tau = 1 \text{ and } \overline{\mathrm{GA}}] \times \Pr[\tau = 1 \mid \overline{\mathrm{GA}}])$. Let $\lambda' = \Pr[\zeta = \zeta' \mid \tau = 1 \text{ and } \overline{\mathrm{GA}}]$. So, we note that $\mathcal{P} = (0.5)(0.5) + 0.5\lambda'$. Finally, we derive that $|\Pr[\tau = \tau' \mid \overline{\mathrm{GA}}] - 0.5| = |\mathcal{P} - 0.5| = 0.5\,|\lambda' - 0.5| \geq 0.5\varepsilon$ as ε is given.

Hence, it follows from Claim (C) and the probability $|\Pr[\tau = \tau' \mid \overline{\mathrm{GA}}] - 0.5|$ that advantage of $\mathfrak{B}$ is at least $0.5\varepsilon(1 - e^{-1} - 2^{m-n})$. Thus, result holds.

Next, we discuss about the IND-ID-CCA security of our IBE in the following remark. Here CCA stands for chosen ciphertext attack.

Remark 3.1: From [8] we know that any IND-ID-CPA secure scheme can be extended to an IND-ID-CCA secure scheme by applying a padding technique. As our IBE is IND-ID-CPA secure (cf. Theorem 3.1), we emphasize that it can be extended to an IND-ID-CCA secure IBE.

4. Execution comparison

In this section, we compare our IBE with several other existing IBEs. We consider the schemes of Boneh et al. [3], Boneh et al. [4], Cocks [6], Lynn [17], Waters [25], Meshram [18], Meshram et al. [19], Mittal et al. [22] and our IBE. It is to be noted that encryption and decryption phases are

dominating as compare to Setup and Extraction phases if we look at the computational cost. Consequently, we compare only the computational cost of encryption and decryption phases. In Table 2, we present the comparison analysis of our scheme with above-mentioned schemes. To this end, let us first discuss certain notations that will be used in Table 2.

Notations: Let P denote pairing operation, M denote modular multiplication, e denote modular exponentiation in a group, H denote map to point hash function, x denote XOR operation, m denote scalar multiplication in a group, i denote modular inverse operation, a denote modular addition operation, h denote one way hash function, j denote Jacobi symbol operation, e_{gr} denote exponentiation in a group ring and M_{gr} denote multiplication in a group ring. Let t_χ denote the execution time for χ operation. Let CC stand for computational cost. Let CC(1) and CC(2), respectively, denote the CC for encryption and decryption phases and CC(3) denote the total CC for both encryption and decryption phases. Let S_1 and S_2 denote the security provided in ROM and CPA models, respectively. Let S_3 denote the security against attacks on quantum computers. In the quantum sense, we say that an IBE is secure if there is no known polynomial time quantum algorithm that can solve the underlying hard problem and any non-quantum algorithm to solve the same takes exponential (or subexponential) time. Let Y denotes yes and N denotes no.

Next, we discuss some of the known facts related to execution time t_χ for certain operations χ. Time t_p is overriding most of the other above-mentioned operations [2]. Moreover, it follows from [4, 7] that t_a and t_h may be neglected in comparison to t_x, t_H, t_e, t_M, t_j, t_i. Also, [12, 22] imply that $t_{e_{gr}} \approx t_e$ and $t_{M_{gr}} \approx t_M$ for the parameters mentioned in Table 1.

It follows from Table 2 that our IBE bears lower CC than the IBEs of [3, 4, 6, 17, 25, 22]. Further, as $t_{e_{gr}} \approx t_e$, $t_{M_{gr}} \approx t_M$ and $t_e > t_m$, CC of our IBE is also less than that of [18, 19].

In addition to this, the biggest advantage of our IBE is that its security is based on DLPGR assumption which is a hard problem even in the quantum sense, whereas IFP and DLP are solvable on a quantum computer [1]. Therefore, our IBE is computationally efficient as well as secure.

Table 2

Execution comparison of our IBE with other IBEs.

IBE	CC(1)	CC(2)	CC(3)	S_1	S_2	S_3
Boneh at al. [3]	$4t_e + t_P + 2t_M$	$t_e + t_P + t_i + t_M$	$5t_e + 2t_P$ $t_i + 3t_M$	N	Y	N
Boneh et al. [4]	$t_P + t_e + t_x + t_m + t_H + t_h$	$t_h + t_P + t_x$	$2t_P + t_e + 2t_x + t_m + t_H + 2t_h$	Y	Y	N
Cocks [6]	$2t_a + 2t_M + t_J + 2t_i$	$t_a + t_J$	$3t_a + 2t_M + 2t_J + 2t_i$	N	N	N
Lynn [17]	$t_H + t_P + t_x + 3t_h$	$t_H + t_P + t_x + 3t_h$	$2t_H + 2t_P$ $2t_x + 6t_h$	Y	Y	N
Waters [25]	$3t_m + 2t_p$	$t_m + 2t_p + t_i$	$4t_m + 4t_p + t_i$	N	N	N
Meshram [18]	$t_m + 2t_e$	$t_m + t_e + t_i$	$2t_m + 3t_e + t_i$	Y	Y	N
Meshram et al. [19]	$2t_e$	$t_m + 2t_e$	$t_m + 4t_e$	Y	Y	N
Mittal et al. [22]	$t_h + t_P + t_e + t_H + 2t_{e_{gr}} + t_M + t_{M_{gr}}$	$t_{e_{gr}} + t_{M_{gr}} + t_P + t_H$	$t_h + 2t_P + t_e + 2t_H + 3t_{e_{gr}} + t_M + 2t_{M_{gr}}$	Y	Y	Y
Our IBE	$t_{m_{gr}} + 2t_{e_{gr}}$	$t_{m_{gr}} + t_{e_{gr}}$	$2t_{m_{gr}} + 3t_{e_{gr}}$	Y	Y	Y

Conclusion

We have exhibited a novel IBE based on group ring. We have shown that security of our IBE depends on a hard problem in group ring. Further, we have discussed the IND-ID-CPA security of the IBE along with the possibility of its extension using the results of [8] so that it becomes IND-ID-CCA secure. Finally, we have compared our IBE with several notable IBEs and shown that our IBE is computationally efficient as well as useful

in post-quantum scenario. An important open problem that arises from this work is whether the condition $m < n$ in Theorem 3.1 can be relaxed or not.

Declaration of interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work in this paper.

References

[1] D. J. Bernstein, J. Buchmann, E. Dahmen, Post quantum cryptography, Springer (2009).

[2] D. Boneh, X. Boyen, Secure identity based encryption without random oracles, CRYPTO 2004, in: LNCS, 3152, Springer-Verlag, Berlin, 443-459 (2004).

[3] D. Boneh, X. Boyen, Efficient selective-id secure identity based encryption without random oracles, EUROCRYPT 2004, in: LNCS, 3027, Springer-Verlag, Berlin, 223-238 (2004).

[4] D. Boneh, M. K. Franklin, Identity-based encryption from the Weil pairing, *SIAM J. Comput.*, 32(3), 586-615 (2003).

[5] D. Boneh, R. Canetti, S. Halevi, J. Katz, Chosen-ciphertext security from identity-based encryption, *SIAM J. Comput.*, 36(5), 1301-1328 (2003).

[6] C. Cocks, An identity based encryption scheme based on quadratic residues, in: International conference on cryptography and coding, in: LNCS, 2260, Springer-Verlag, 360-363 (2001).

[7] S. Cui, P. Duan, C. W. Chan, An identity based encryption scheme with batch verifications, in: Proceedings of the Ist ACM international conference on scalable information systems, 2260, Hong Kong, pp. 22 (2006).

[8] E. Fujisaki, T. Okamoto, Secure integration of asymmetric and symmetric encryption schemes, Crypto-99, in: LNCS, 1666, Springer-Verlag, Berlin, 537-554 (1999).

[9] N. Goel, I. Gupta, M. Dubey, B. K. Dass, Undeniable signature scheme based over group ring, AAECC, 27, 523-535 (2016).

[10] S. Heng, K. Kurosawa, k-Resilient identity-based encryption in the standard model, IEICE Trans. Fundam., E89CA(1), 39-46 (2006).

[11] J. Hoffstein, J. Pipher, J. H. Silverman, An introduction of mathematical cryptography, Springer (2008).

[12] B. Hurley, T. Hurley, Group ring cryptography, *Int. J. Pure Appl. Math.*, 69(1), 67-86 (2011).

[13] S. Inam, R. Ali, A new ElGamal-like cryptosystem based on matrices over groupring, Neural Comput. & Applic., doi: 10.1007/s00521-016-2745-2.

[14] E. Kiltz, Y. Vahlis, CCA2 secure IBE: standard model efficiency through authenticated symmetric encryption, in: CT-RSA, in: LNCS, 4964, Springer-Verlag, 221-239 (2008).

[15] Ö. Küsmü, T. Hanoymak, A novel public-key encryption scheme based on Bass cyclic units in integral group rings, *J. Discret. Math. Sci. Cryptogr.,* 25(2), 579-589 (2022).

[16] W. C. Lee, K. C. Liao, Constructing identity-based cryptosystems for discrete logarithm based cryptosystems, *J. Netw. Comput. Appl.*, 22, 191-199 (2004).

[17] B. Lynn, Authenticated ID-based encryption, cryptology, ePrint Archive, Report2002/072, 2002, http://eprint.iacr.org/2002/072.

[18] C. Meshram, An efficient ID-based cryptographic encryption based on discrete logarithm problem and integer factorization problem, Inf. Process. Lett., 115, 351-358 (2015).

[19] C. Meshram, S. Meshram, An IND-ID-CPA secure ID-based cryptographic protocol using GDLP and IFP, Informatica, 28(3), 471-484 (2017).

[20] C. P. Milies, S. K. Sehgal, An Introduction to group rings, Kluwer (2002).

[21] G. Mittal, S. Kumar, S. Narain, S. Kumar, Group rings based public key cryptosystems, *J. Discret. Math. Sci. Cryptogr.,* 25(6), 1683-1704 (2022).

[22] G. Mittal, S. Kumar, S. Kumar, A quantum secure ID-based cryptographic encryption based on group rings, Sadhana, 47, 1-16 (2022).

[23] A. Shamir, Identity-based cryptosystems and signature schemes, CRYPTO'84, in: LNCS, 196, Springer-Verlag, 47-53 (1984).

[24] J. Sun, C. Zhang, Y. Zhang, Y. Fang, An identity-based security system for user privacy in vehicular adhoc networks, *IEEE Trans. Parallel Distrib. Syst.*, 27(9), 1227-1239 (2010).

[25] B. Waters, Efficient identity-based encryption without random oracles, CRYPTO 2005, in: LNCS, 3494, Springer-Verlag, Berlin, 114-127 (2005).

Received April, 2023