Post-Quantum Secure Identity-Based Encryption from Multivariate Public Key Cryptography

Nibedita Kundu, Kunal Dey, Pantelimon Stănică, Sumit Kumar Debnath, and Saibal Kumar Pal

1 Introduction

In the modern era, we are very much dependent on the use of public key cryptography. Identity-Based Encryption (IBE) systems are well-known advanced candidates of public key cryptosystem. In IBE, a user's public key is some unique information about the user's publicly known identity, which may be an arbitrary string (like an email address). A general IBE system is a tuple of four algorithms:

1. Setup phase produces master public key and master secret key;
2. Extraction contains the generation of the recipient's private key using the master secret key and identity of the recipient;
3. Encryption procedure can be used for encrypting messages corresponding to the receiver's identity and master public key;

N. Kundu (✉)
Department of Mathematics, The LNM Institute of Information Technology,
Jaipur 302031, India
e-mail: nknkundu@gmail.com

K. Dey · S. K. Debnath
Department of Mathematics, National Institute of Technology Jamshedpur,
Jamshedpur 831014, India
e-mail: kunaldey3@gmail.com

S. K. Debnath
e-mail: sdebnath.math@nitjsr.ac.in

P. Stănică
Department of Applied Mathematics, Naval Postgraduate School, Monterey,
CA 93943, USA
e-mail: pstanica@nps.edu

S. K. Pal
SAG Lab, Defense Research & Development Organization, Delhi 110054, India
e-mail: skptech@yahoo.com

P. Stănică et al. (eds.), *Security and Privacy*, Lecture Notes in Electrical Engineering 744,
https://doi.org/10.1007/978-981-33-6781-4_12

4. Decryption allows to decrypt the ciphertext using the user's identity and secret key.

The concept of IBE was developed by Shamir [20] in 1984 for simplifying the certificate management process in e-mail systems. His aim was to make sure that when a sender desires to send a message to a receiver at "**receiver@gmail.com**" through email, there should not be any requirement for the receiver's public key certificate. Rather, the sender uses a public identity string of the receiver, such as **receiver@gmail.com**, for encrypting the message. In the following, the receiver decrypts the email by using his secret key which he obtains from a trusted third party, namely Key Generation Center (KGC), by authenticating himself to KGC. Then only the receiver can read the message. It is notable that KGC has knowledge of the receiver's private key, which means key escrow is inherent in identity-based email systems. Moreover, in contrast to the existing secure email infrastructure, the sender is able to send an encrypted email to the receiver even if the receiver's public key certificate is not set up yet.

So far, most of the research that has been done in the context of IBE systems are relying on the hardness of number theoretical problems, such as the factorization problems [18] and discrete logarithm problems [12, 13]. These number theoretic assumption-based IBE systems are vulnerable to attacks in polynomial time due to Shor's algorithm [21], provided efficient quantum computers are designed. To overcome this threat, finding an alternative, i.e., designing quantum computers immune IBE systems becomes an urgent issue. The construction of these quantum computer resistant IBE systems falls under post-quantum cryptography (PQC) [1]. In the context of PQC, multivariate public key cryptography (MPKC) is one of the most promising candidates, where a system of multivariate polynomials works as a public key. In the current state of the art, there are several constructions of encryption and signature schemes based on MPKC. However, exploring IBE systems through MPKC is at the beginning stage. Thereby, the development of a secure and efficient multivariate IBE becomes an interesting direction for further research.

There is only one multivariate IBE in the literature, which was developed by Samardjiska and Gligoroski [19] in 2012. Apart from the multivariate IBE, there are several other designs of post-quantum IBE systems [2, 6–8, 11, 14–16, 22, 23] based on other candidates of PQC.

2 Our Contribution

This paper deals with the design and analysis of post-quantum secure identity-based encryption schemes relying on multivariate cryptography. We are motivated by the work of [5], which concentrates on the construction of multivariate identity-based signatures. The technique of [5] has been utilized to develop our proposed identity-based encryption scheme, namely MU-IBE. It is quite efficient, as only modular multiplications and modular additions are responsible for generating the computation overhead of the proposed IBE. Our scheme attains IND-ID-CCA security under the hardness of the MQ problem (assuming the number of polynomials is $m = O(n)$, where n is the number of involved variables) in the random oracle model. Moreover, our proposed IBE is immune against collusion attack (in spite of the fact that it was believed that such an MQ-based IBE scheme that is immune against collusions is very hard to construct), while the only existing multivariate IBE of [19] does not achieve CCA or even CPA security. Further, the collusion attack is possible in the scheme of [19]. Thus, from a security point of view, our scheme performs better over the IBE of [19].

3 Preliminaries

Firstly, we introduce the basic notations. In this paper, the "security parameter" is represented by κ, where $x \in_R S$ stands for "x is chosen uniformly at random from a set S", $\mathbb{F}_q$ represents a finite field of order q (a power of a prime p), a π degree extension field of $\mathbb{F}_q$ is denoted by $\mathbb{F}_{q^\pi}$ and $(\mathbb{F}_q)^\pi$ is a vector space, defined as $\{\mathbf{x} = (x_1, \ldots, x_\pi) | x_i \in \mathbb{F}_q \text{ for } i = 1, \ldots, \pi\}$ with the known element-wise inherited operations.

Negligible function: We say that a function $\varphi(\kappa)$ is negligible in κ if for all $\lambda > 0$, we have $\varphi(\kappa) < \kappa^{-\lambda}$, for sufficiently large κ.

3.1 Hardness Assumption

MQ Problem [17]: Given a system of δ quadratic multivariate polynomials $\{p_1(x_1, \ldots, x_\pi), \ldots, p_\delta(x_1, \ldots, x_\pi)\}$ of π variables $x_1, \ldots, x_\pi$ over $\mathbb{F}_q$, it is proven that finding a solution $\mathbf{x} = (x_1, \ldots, x_\pi)$ of the system of equations $p_1(\mathbf{x}) = \cdots = p_\delta(\mathbf{x}) = 0$ is NP-hard even for polynomials of degree 2 over $\mathbb{F}_2$ [9], if $\delta = O(\pi)$ (recall that the big-Oh complexity class Landau notation $f = O(g)$ means that $|f(x)| \leq cg(x)$ for some constant $c > 0$, whenever $x \geq x_c$).

3.2 General Multivariate Encryption [17]

A general MPKC Encryption Scheme contains the following three algorithms:

- Key Generation : This algorithm generates a secret key $(\mathcal{L}, \mathcal{F}, \mathcal{T})$ and a public key $\mathcal{P} = \mathcal{L} \circ \mathcal{F} \circ \mathcal{T}$, where $\mathcal{L} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $\mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ are two invertible affine maps, and $\mathcal{F} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ is an easily invertible function, known as "Central Map". Thereby, $\mathcal{P}$ is a system of $m \in \mathbb{Z}$ number of multivariate polynomials in $n \in \mathbb{Z}$ number of variables.

- Encryption : Given a message $\mathbf{x} \in \mathbb{F}_q^m$ and a public key $\mathcal{P} = \mathcal{L} \circ \mathcal{F} \circ \mathcal{T}$, the encryptor derives the ciphertext $\mathbf{y} = \mathcal{P}(\mathbf{x}) \in \mathbb{F}_q^m$.
- Decryption : To decrypt a ciphertext $\mathbf{y} \in \mathbb{F}_q^m$ using the secret key $(\mathcal{L}, \mathcal{F}, \mathcal{T})$, the decryptor recursively calculates $\mathbf{z} = \mathcal{L}^{-1}(\mathbf{y}) \in \mathbb{F}_q^m$, $\mathbf{w} = \mathcal{F}^{-1}(\mathbf{z}) \in \mathbb{F}_q^n$ and $\mathbf{x} = \mathcal{T}^{-1}(\mathbf{w}) \in \mathbb{F}_q^n$. Finally, it outputs $\mathbf{x} \in \mathbb{F}_q^n$ as the plaintext corresponding to the ciphertext $\mathbf{y} \in \mathbb{F}_q^m$.

3.3 General Identity-Based Encryption [10]

Setup, Extraction, EncryptionandDecryption are the four specified randomized algorithms for a general IBE scheme.

- Setup : It takes a security parameter κ as input and KGC runs these algorithms to create the master public key $\mathcal{MPK}$ and the master secret key $\mathcal{MSK}$ as output, along with the corresponding message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$.
- Extraction : KGC runs this algorithm at the user's request to generate user's private key. This algorithm accepts $\mathcal{MPK}$, $\mathcal{MSK}$ and $ID_i \in \{0, 1\}^*$ as inputs and returns a secret key Sk_{ID_i} as output, where ID_i is the identity parameter of the ith user.
- Encryption : This algorithm is run by an encryptor. It takes $\mathcal{MPK}$, ID_i and message Mg as inputs, and computes output ciphertext Ct.
- Decryption : A user with (Sk_{ID_i}, ID_i) runs this algorithm to original plaintext Mg by decrypting the ciphertext Ct. The plaintext Mg should satisfy the correctness proof:

$$\mathsf{Decryption}(Sk_{ID_i}, ID_i, \mathsf{Encryption}(\mathcal{MPK}, ID_i, \mathsf{Mg})) = \mathsf{Mg}, \forall \mathsf{Mg} \in \mathcal{M}.$$

3.4 CCA Security Model for Identity-Based Encryption [3, 4]

Let us consider an IBE consisting of Setup, Extraction, Encryption and Decryption. The chosen ciphertext security for IBE systems under a chosen identity attack is defined by Boneh and Franklin [3, 4] via the following game between a challenger Ch and an adversary Ad.

Setup : In this phase, Ch runs Setup to generate $(\mathcal{MPK}, \mathcal{MSK})$ and sends $\mathcal{MPK}$ to Ad.

Phase1 : Ad adaptively makes a polynomial number of queries $Q_1, \ldots, Q_{qe}$ to Ch, where Q_i is one of the following:

Extract query: For $ID_i \in \{0, 1\}^*$, Ad queries for the corresponding secret key.

The challenger Ch generates the corresponding secret key Sk_{ID_i} by running the Extraction algorithm and sends it to Ad.

Decryption query: For $ID_i \in \{0, 1\}^*$, Ad queries for the decryption of Ct_i. The challenger Ch first generates the corresponding secret key Sk_{ID_i} by running the Extraction algorithm. It then uses Sk_{ID_i} to decrypt Ct_i and sends the output message Mg_i to Ad.

Challenge : Ad submits two messages Mg_0, Mg_1 and an identity ID. Note that ID must not have appeared in any extract query of Phase 1. In the following, Ch chooses $b \in_R \{0, 1\}$, sets $\mathsf{Ct}_b = Encryption(\mathcal{MPK}, ID, \mathsf{Mg}_b)$ and sends Ct_b to Ad as challenge ciphertext.

Phase2 : This phase is similar to Phase 1, except that Ad is not allowed to make an extract query for ID or decryption query for (ID, C).

Guess : Ad outputs $\overline{b} \in \{0, 1\}$ and wins if $b = \overline{b}$.

An adversary Ad in the aforementioned game is called IND-ID-CCA adversary (IND stands for *indistinguishability*; ID stands for *full-identity attack*; and CCA stands for *chosen-ciphertext attack*).

Definition 1 An IBE is said to be $(\tau, Q_{ID}, Q_{Ct}, \nu)$ IND-ID-CCA secure if for any τ-time, IND-ID-CCA adversary that makes at most Q_{ID} extract queries and at most Q_{Ct} decryption queries has advantage at most ν in winning the aforementioned game.

4 Proposed Multivariate Identity-Based Encryption (MU-IBE)

We now discuss the construction of our proposed MU-IBE scheme. It is a tuple of four algorithms: (i) Setup, (ii) Extraction, (iii) Encryption and (iv) Decryption. Let us assume that the system contains d number of users $\mathsf{u}_1, \mathsf{u}_2, \ldots \mathsf{u}_\mathsf{d}$ and a trusted Key Generation Center (KGC). In Setup, the KGC generates master public key ($\mathcal{MPK}$) and master secret key ($\mathcal{MSK}$). During Extraction, the KGC generates secret key Sk_{ID_i} with the help of $\mathcal{MSK}$ and ID_i for the user u_i with identity ID_i. In Encryption, the Encryptor encrypts a message $\mathsf{Mg} \in \{0, 1\}^\lambda$ using the master public key $\mathcal{MPK}$ and identity ID_i of an user u_i to obtain a ciphertext Ct, where $\lambda \in \mathbb{N}$ is the length of the message. A user u_i with identity ID_i runs the algorithm Decryption with the help of Sk_{iD_i} and ID_i to extract the message Mg from a ciphertext Ct.

Protocol MU-IBE

Setup(1^κ): The KGC, by taking input 1^κ, generates $\mathcal{MPK} = \mathcal{P}^{(\mathbf{v})} = \mathcal{L}^{(\mathbf{v})} \circ \mathcal{F}^{(\mathbf{v})} \circ \mathcal{T}^{(\mathbf{v})} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ and $\mathcal{MSK} = \{\mathcal{L}^{(\mathbf{v})}, \mathcal{F}^{(\mathbf{v})}, \mathcal{T}^{(\mathbf{v})}\}$, where

1. $\mathcal{L}^{(\mathbf{v})} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ is an invertible affine map with

$$\mathcal{L}^{(\mathbf{v})}(x_1, \ldots, x_m) = (L_1^{(\mathbf{v})}(x_1, \ldots, x_m), \ldots, L_m^{(\mathbf{v})}(x_1, \ldots, x_m))$$

and

$$L_i^{(\mathbf{v})}(x_1, \ldots, x_m) = \sum_{j=1}^{m} L_{i,j}(v_1, \ldots, v_\delta)x_j + L_{i,0}(v_1, \ldots, v_\delta),$$

for $i = 1, \ldots, m$, where each $L_{i,j} : \mathbb{F}_q^\delta \to \mathbb{F}_q$ is a linear function.

2. $\mathcal{T}^{(\mathbf{v})} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is an invertible affine map with

$$\mathcal{T}^{(\mathbf{v})}(x_1, \ldots, x_n) = (T_1^{(\mathbf{v})}(x_1, \ldots, x_n), \ldots, T_n^{(\mathbf{v})}(x_1, \ldots, x_n))$$

and

$$T_i^{(\mathbf{v})}(x_1, \ldots, x_n) = \sum_{j=1}^{n} T_{i,j}(v_1, \ldots, v_\delta)x_j + T_{i,0}(v_1, \ldots, v_\delta),$$

for $i = 1, \ldots, n$, where each $T_{i,j} : \mathbb{F}_q^\delta \to \mathbb{F}_q$ is a linear function.

3. $\mathcal{F}^{(\mathbf{v})}(x_1, \ldots, x_n) = (F_1^{(\mathbf{v})}(x_1, \ldots, x_n), \ldots, F_m^{(\mathbf{v})}(x_1, \ldots, x_n))$ is a system of quadratic multivariate polynomials with

$$F_i^{(\mathbf{v})}(x_1, \ldots, x_n) = \sum_{1 \le j \le k \le n} \phi_{i,j,k}(v_1, \ldots, v_\delta)x_j x_k + \sum_{j=1}^{n} \psi_{i,j}(v_1, \ldots, v_\delta)x_j + \zeta_i(v_1, \ldots, v_\delta),$$

for $i = 1, \ldots, m$, where $\phi_{i,j,k}(v_1, \ldots, v_\delta)$, $\psi_{i,j}(v_1, \ldots, v_\delta)$ and $\zeta_i(y_1, \ldots, y_\delta)$ are linear functions from $\mathbb{F}_q^\delta$ to $\mathbb{F}_q$.

4. The public key $\mathcal{P}^{(\mathbf{v})} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ takes the form

$$\mathcal{P}^{(\mathbf{v})}(x_1, \ldots, x_n) = (P_1^{(\mathbf{v})}(x_1, \ldots, x_n), \ldots, P_m^{(\mathbf{v})}(x_1, \ldots, x_n))$$

with

$$P_i^{(\mathbf{v})}(x_1, \ldots, x_n) = \sum_{1 \le j \le k \le n} C_{i,j,k}(v_1, \ldots, v_\delta)x_j x_k + \sum_{j=1}^{n} D_{i,j}(v_1, \ldots, v_\delta)x_j + E_i(v_1, \ldots, v_\delta),$$

for $i = 1, \ldots, m$, where $C_{i,j,k}(v_1, \ldots, v_\delta)$, $D_{i,j}(v_1, \ldots, v_\delta)$ and $E_i(v_1, \ldots, v_\delta)$ are functions of $(v_1, \ldots, v_\delta)$ of degree 4 from $\mathbb{F}_q^\delta$ to $\mathbb{F}_q$.

$\mathsf{Extraction}(\mathcal{MSK}, ID_i)$: In this phase, the following steps are performed.

1. Each user u_i is registered to KGC. The KGC generates a unique public identity $ID_i \in \{0, 1\}^*$ for each u_i and computes $\mathsf{Hash}(ID_i) = \mathbf{b}_i = (b_{1i}, \ldots, b_{\delta i}) \in$

$\mathbb{F}_q^\delta$, using some cryptographically secure collision-free hash function $\mathsf{Hash} : \{0,1\}^* \to \mathbb{F}_q^\delta$.

2. Putting the value of $\mathbf{b}_i = (b_{1i}, \ldots, b_{\delta i})$ in $\mathcal{L}^{(\mathbf{v})}, \mathcal{F}^{(\mathbf{v})}, \mathcal{T}^{(\mathbf{v})}$, the KGC obtains $\mathcal{L}^{(\mathbf{b}_i)}, \mathcal{F}^{(\mathbf{b}_i)}, \mathcal{T}^{(\mathbf{b}_i)}$, which are functions depending upon $x_1, \ldots, x_m$.
3. Given $\mathcal{MSK}$ and the identity vector $\mathbf{b_i} \in \mathbb{F}_q^\delta$, the KGC needs to randomly choose two invertible affine maps $L_i : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $T_i : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that $\widehat{\mathcal{F}}^{(\mathbf{b}_i)} = L_i \circ \mathcal{F}^{(\mathbf{b}_i)} \circ T_i$ can easily be inverted. The KGC also derives $\widehat{\mathcal{L}}^{(\mathbf{b}_i)} = \mathcal{L}^{(\mathbf{b}_i)} \circ L_i^{-1}$ and $\widehat{\mathcal{T}}^{(\mathbf{b}_i)} = T_i^{-1} \circ \mathcal{T}^{(\mathbf{b}_i)}$.
   It is clear that $\mathcal{P}^{(\mathbf{b}_i)} = \mathcal{L}^{(\mathbf{b}_i)} \circ \mathcal{F}^{(\mathbf{b}_i)} \circ \mathcal{T}^{(\mathbf{b}_i)} = \widehat{\mathcal{L}}^{(\mathbf{b}_i)} \circ \widehat{\mathcal{F}}^{(\mathbf{b}_i)} \circ \widehat{\mathcal{T}}^{(\mathbf{b}_i)}$ since

$$\mathcal{L}^{(\mathbf{b}_i)} \circ \mathcal{F}^{(\mathbf{b}_i)} \circ \mathcal{T}^{(\mathbf{b}_i)} = \mathcal{L}^{(\mathbf{b}_i)} \circ L_i^{-1} \circ L_i \circ \mathcal{F}^{(\mathbf{b}_i)} \circ T_i \circ T_i^{-1} \circ \mathcal{T}^{(\mathbf{b}_i)} = \widehat{\mathcal{L}}^{(\mathbf{b}_i)} \circ \widehat{\mathcal{F}}^{(\mathbf{b}_i)} \circ \widehat{\mathcal{T}}^{(\mathbf{b}_i)}.$$

The KGC sends $Sk_{ID_i} = (\widehat{\mathcal{L}}^{(\mathbf{b}_i)}, \widehat{\mathcal{F}}^{(\mathbf{b}_i)}, \widehat{\mathcal{T}}^{(\mathbf{b}_i)})$ along with identity ID_i to the user u_i.

$\mathsf{Encryption}(ID_i, \mathsf{Mg}, \mathcal{MPK})$: To encrypt a message $\mathsf{Mg} \in \{0,1\}^\lambda$, the encryptor, with access to ID_i and $\mathcal{MPK}$, performs the following steps:

1. Derives $\mathbf{b}_i = \mathsf{Hash}(ID_i) = (v_1, \ldots, v_\delta)$.
2. Chooses $\mathbf{r} = (\alpha_1, \ldots, \alpha_n) \in_R \mathbb{F}_q^n$.
3. Computes $\mathcal{P}^{(\mathbf{b}_i)}(\mathbf{r}) = \mathcal{P}^{(\mathbf{b}_i)}(\alpha_1, \ldots, \alpha_n) = (\beta_1, \ldots, \beta_m) = \chi$, where

$$\beta_j = P_j^{(\mathbf{b}_i)}(\alpha_1, \ldots, \alpha_n) \text{ for } j = 1, \ldots, m.$$

4. Evaluates $H_1(\mathbf{r})$ and $H_2(\mathsf{Mg}, \mathbf{r})$, for some publicly known collision-resistant hash functions $H_1, H_2 : \{0,1\}^* \to \{0,1\}^\lambda$.
5. Outputs the corresponding ciphertext as $\mathsf{Ct} = (\chi, \xi, \theta)$, where $\chi = \mathcal{P}^{(\mathbf{b}_i)}(\mathbf{r})$, $\xi = H_1(\mathbf{r}) \oplus \mathsf{Mg}$ and $\theta = H_2(\mathsf{Mg}, \mathbf{r})$.

$\mathsf{Decryption}(ID_i, \mathsf{Ct}, Sk_{ID_i})$: To decrypt the ciphertext $\mathsf{Ct} = (\chi, \xi, \theta)$, n user u_i with identity ID_i and secret key Sk_{ID_i} executes the following steps:

1. Computes $\mathbf{b}_i = \mathsf{Hash}(ID_i) = (v_1, \ldots, v_\delta)$.
2. Evaluates $(\widehat{\mathcal{L}}^{(\mathbf{b}_i)})^{-1}(\chi) = (\widehat{\mathcal{L}}^{(\mathbf{b}_i)})^{-1}(\beta_1, \ldots, \beta_m) = \mathbf{w} = (w_1, \ldots, w_m)$.
3. Calculates the pre-image of $\widehat{\mathcal{F}}^{(\mathbf{b}_i)}$ on a particular value of $\mathbf{x}$, which means

$$(\widehat{\mathcal{F}}^{(\mathbf{b}_i)})^{-1}(\mathbf{w}) = \mathbf{y} = (y_1, \ldots, y_n).$$

4. Evaluates $(\widehat{\mathcal{T}}^{(\mathbf{b}_i)})^{-1}(\mathbf{y}) = \mathbf{z}$.
5. Computes $H_1(\mathbf{z})$, $\overline{\mathsf{Mg}} = \xi \oplus H_1(\mathbf{z})$ and $\overline{\theta} = H_2(\overline{\mathsf{Mg}}, \mathbf{z})$.
6. Checks whether the equality $\overline{\theta} = \theta$ holds. If it holds then the user outputs $\overline{\mathsf{Mg}}$ as the message. Otherwise, again it starts from step 2. Note that H_1 and H_2 are collision-resistant hash functions. Thus, $\overline{\theta} = \theta$ implies $\overline{\mathsf{Mg}} = \mathsf{Mg}$.

5 Security

Theorem 1 *If the hash functions H_1 and H_2 are designed as random oracles, then the proposed scheme* $\mathsf{MU\text{-}IBE}$ *is IND-ID-CCA secure under the hardness of the MQ problem.*

Proof Let $\mathsf{Ct}_b = (\chi_b, \xi_b, \theta_b)$ be the challenge ciphertext received by Ad for the identity ID, where $\chi_b = \mathcal{P}^{(\mathsf{Hash}(ID))}(\mathbf{r}_b)$, $\xi_b = H_1(\mathbf{r}_b) \oplus \mathsf{Mg}_b$ and $\theta_b = H_2(\mathsf{Mg}_b, \mathbf{r}_b)$. Here, the random oracle H_2 is a collision-resistant hash function. As a consequence, it is not feasible to find two distinct pairs $(\mathsf{Mg}, \mathbf{r})$ and $(\mathsf{Mg}^{'}, \mathbf{r}^{'})$ such that $H_2(\mathsf{Mg}, \mathbf{r}) = H_2(\mathsf{Mg}^{'}, \mathbf{r}^{'})$. At each decryption query step and for every $\theta \in \{0, 1\}^{\lambda}$, we define $H_2^{-1}(\theta) = (\mathsf{Mg}, \mathbf{r})$ if H_2 was queried before $(\mathsf{Mg}, \mathbf{r})$, and θ was returned as output; otherwise, $H_2^{-1}(\theta) =\perp$. Note that a ciphertext $\mathsf{Ct} = (\chi, \xi, \theta)$ is completely determined by a pair $(\mathsf{Mg}, \mathbf{r})$, while (χ, ξ) completely determines $(\mathsf{Mg}, \mathbf{r})$. Let us simulate the extract query as follows: the response to the extract query for an identity ID is set as $\{S_1, S_1^{-1} \circ \mathcal{P}^{(ID)} \circ S_2^{-1}, S_2\}$ for randomly chosen invertible affine maps. Note that $S_1 \circ S_1^{-1} \circ \mathcal{P}^{(ID)} \circ S_2^{-1} \circ S_2 = \mathcal{P}^{(ID)}$. Clearly, $S_1 \circ S_1^{-1} \circ \mathcal{P}^{(ID)} \circ S_2^{-1} \circ S_2 = \mathcal{P}^{(ID)}$. Thereby, the simulated view and the real view are indistinguishable. Furthermore, simulate the decryption query in the following way: the response to the decryption query of a ciphertext $\mathsf{Ct} = (\chi, \xi, \theta)$ is set as Mg if there exists some $(\mathsf{Mg}, \mathbf{r})$, such that $H_2^{-1}(\theta) = (\mathsf{Mg}, \mathbf{r})$; otherwise, the response is set as $\perp$, where $\perp$ signifies "failure" or "invalid input". Then the difference between the simulated game and the real game is that the simulated decryption oracle may answer $\perp$, while the real decryption oracle would provide an actual output. However, one may claim that the difference cannot be detected by the Ad with non-negligible probability. Particularly, there may be a difference if Ad can manage to ask a query for $\mathsf{Ct} = (\chi, \xi, \theta)$, satisfying the following:

- $\theta \neq \theta_b$. This is because if $\theta = \theta_b$ then $H_2^{-1}(\theta) = (\mathsf{Mg}_b, \mathbf{r}_b)$ and thereby Ad either asked a query that both oracles respond with $\perp$ or it asked the disallowed query $(\chi_b, \xi_b, \theta_b)$.
- Output of none of the previous queries $(\mathsf{Mg}, \mathbf{r})$ to $H_2(\cdot)$ made by Ad is θ.
- $(\mathsf{Mg}^*, \mathbf{r}^*)$ is determined by χ, ξ such that $H_2(\mathsf{Mg}^*, \mathbf{r}^*) = \theta$.

However, θ is not the output of any previous query to $H_2(\cdot)$, i.e., no $(\mathsf{Mg}, \mathbf{r})$ was asked before, such that $H_2(\mathsf{Mg}, \mathbf{r}) = \theta$. Thus, the probability of the aforementioned circumstance is $2^{-\lambda}$, which is negligible in λ (sufficiently large). In other words, Ad cannot detect the difference between the simulated game and the real game with non-negligible probability. Thus, the decryption box of Ad can be simulated without having the knowledge of $(\mathcal{P}^{(\mathsf{Hash}(ID))})^{-1}$, Mg_b, $\mathbf{r}_b$. In other words, Ad has no use for the decryption box.

Claim: We now claim that the probability that Ad queries $\mathbf{r}_b$ to the random oracles $H_1(\cdot)$ and $H_2(\cdot)$ is negligible.

We will argue that below, by considering the following simulation: substitute $\xi_b = H_1(\mathbf{r}_b) \oplus \mathsf{Mg}_b$ by $\xi_b = k_1 \oplus \mathsf{Mg}_b$ and $\theta_b = H_2(\mathsf{Mg}_b, \mathbf{r}_b)$ by $\theta_b = k_2$, for some random elements k_1, k_2, which are uniformly chosen from $\{0, 1\}^\lambda$. The simulated game may be distinguished from the real game by Ad only if it queries $\mathbf{r}_b$ to the random oracles $H_1(\cdot)$ or $H_2(\cdot)$ and observes that the outputs are different from k_1 and k_2, but then we already lost. Hence, the probability that Ad queries $\mathbf{r}_b$ in the simulated game is the same as the probability that it queries $\mathbf{r}_b$ in the real game.

However, in the simulated game, the only information Ad obtains about $\mathbf{r}_b$ is $\mathcal{P}^{(\mathsf{Hash}(ID))}(\mathbf{r}_b)$. As a consequence, Ad queries $\mathbf{r}_b$ to the random oracles $H_1(\cdot)$ or $H_2(\cdot)$ in the simulated game implies that it inverts $\mathcal{P}^{(\mathsf{Hash}(ID))}$. In other words, it breaks the MQ problem which is assumed to be NP-hard. This leads to a contradiction. Thus, it is possible to ignore the probability that Ad queries $\mathbf{r}_b$.

Utilizing the aforementioned claim, we can consider that $\xi_b = k_1 \oplus \mathsf{Mg}_b$ and $\theta_b = k_2$ for $k_1, k_2 \in_R \{0, 1\}^\lambda$. However, this implies that Ad does not obtain any information about Mg_b. Thereby, Ad will be unable to guess if Mg_b is equal to Mg_0 or Mg_1 with probability greater than 1/2. □

Theorem 2 *The proposed IBE is resistant to the collusion attack.*

Proof In this attack, one needs to check whether the collusion of a polynomial number of users will allow extracting the knowledge of $\mathcal{MSK}$ or other users' secret keys. The additional randomly chosen linear transformations L_i, T_i, used in the construction of users' secret keys, protect our proposed scheme against collusion attack. On the other hand, if we do not bring L_i, T_i into the construction of users' secret keys, then each coefficient of $\mathcal{MSK}$ is just a linear combination of $(v_1, \ldots, v_\delta)$. As a consequence, if an adversary gets δ secret keys corresponding to δ different IDs, then it can solve these obtained linear equations. In other words, if δ many users collude then they would be able to extract $\mathcal{MSK}$. Due to the involvement of L_i, T_i into Sk_{ID_i}, the form of Sk_{ID_i} becomes random, totally different from earlier. Thereby, a collusion attack is not possible in our scheme. □

6 Complexity

The communication and computation overheads of the proposed $\mathsf{MU\text{-}IBE}$ are discussed below.

$\mathcal{MPK}$ size: The size of $\mathcal{MPK}$ is $m\binom{n+2}{2}\binom{\delta+4}{4}$ field ($\mathbb{F}_q$) elements.

$\mathcal{MSK}$ size: The size of $\mathcal{MSK}$ is $\left[m(m+1) + n(n+1) + m\binom{n+2}{2}\right]\delta$ field ($\mathbb{F}_q$) elements.

Sk_{ID_i} size: The size of Sk_{ID_i} is $\left[m(m+1) + n(n+1) + m\binom{n+2}{2}\right]$ field ($\mathbb{F}_q$) elements.

Ct size: The size of ciphertext Ct is m field elements + 2λ bits.

Encryption cost: $m\binom{n+2}{2}\sum_{i=1}^{4} i\binom{\delta+i-1}{i} + m\left[n + \binom{n+1}{2}\right]$ field multiplications and 3 hash function evaluations are required.

Decryption cost: $m^2 + n^2$ field multiplications, 3 hash function evaluations and computation cost due to evaluations of $(\widehat{\mathcal{F}}^{(\mathbf{b}_i)})^{-1}(\mathbf{w}) = \mathbf{y}$ are required.

7 Conclusion

We presented a multivariate IBE system that achieves IND-ID-CCA security under the hardness of the MQ problem in the random oracle model. Our scheme performs better over the only existing multivariate IBE of [19] from the security point of view, since [19] doses not incur CCA security and cannot resist collusion attack, unlike ours. In particular, the proposed IBE is the *first multivariate* IBE that achieves *IND-ID-CCA* security. It will be an interesting direction of future research to extend our work in the standard model (without random oracles).

Acknowledgements This work is supported by DRDO (ER & IPR) under File No: ERIP/ER/202005001/M/01/1775.

References

1. Bernstein DJ (2009) Introduction to post-quantum cryptography. In: Post-quantum cryptography. Springer, pp 1–14
2. Bert P, Fouque P-A, Roux-Langlois A, Sabt M (2018) Practical implementation of ring-SIS/LWE based signature and IBE. In: International conference on post-quantum cryptography. Springer, pp 271–291
3. Boneh D, Franklin M (2001) Identity-based encryption from the Weil pairing. In: Annual international cryptology conference. Springer, pp 213–229
4. Boneh D, Franklin M (2003) Identity-based encryption from the Weil pairing. SIAM J Comput 32(3):586–615
5. Chen J, Ling J, Ning J, Ding J (2019) Identity-based signature schemes for multivariate public key cryptosystems. Comput J 62(8):1132–1147
6. Duong DH, Le HQ, Roy PS, Susilo W (2019) Lattice-based IBE with equality test in standard model. In: International conference on provable security. Springer, pp 19–40
7. Emura K, Katsumata S, Watanabe Y (2019) Identity-based encryption with security against the KGC: a formal model and its instantiation from lattices. In: European symposium on research in computer security. Springer, pp 113–133
8. Gaborit P, Hauteville A, Phan DH, Tillich J-P (2017) Identity-based encryption from codes with rank metric. In: Annual international cryptology conference. Springer, pp 194–224
9. Garey MR, Johnson DS (1979) Computers and intractability, vol 174. Freeman San Francisco
10. Gentry C (2006) Practical identity-based encryption without random oracles. In: Annual international conference on the theory and applications of cryptographic techniques. Springer, pp 445–464
11. Katsumata S, Matsuda T, Takayasu A (2020) Lattice-based revocable (hierarchical) IBE with decryption key exposure resistance. Theor Comput Sci 809:103–136
12. Koblitz N (1987) Elliptic curve cryptosystems. Math Comput 48(177):203–209
13. Kravitz DW (1993) Digital signature algorithm. US Patent 5,231,668
14. Lee K (2020) Efficient identity-based encryption from LWR. In: Information security and cryptology-ICISC 2019: 22nd international conference, Seoul, South Korea, vol 11975. Springer Nature, p 225

15. McCarthy S, Smyth N, O'Sullivan E (2017) A practical implementation of identity-based encryption over NTRU lattices. In: IMA international conference on cryptography and coding. Springer, pp 227–246
16. Nguyen K, Wang H, J Zhang (2016) Server-aided revocable identity-based encryption from lattices. In: International conference on cryptology and network security. Springer, pp 107–123
17. Patarin J (1996) Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In: International conference on the theory and applications of cryptographic techniques. Springer, pp 33–48
18. Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 21(2):120–126
19. Samardjiska S Gligoroski D (2012) Towards a secure multivariate identity-based encryption. In: International conference on ICT innovations. Springer, pp 59–69
20. Shamir A (1984) Identity-based cryptosystems and signature schemes. In: Workshop on the theory and application of cryptographic techniques. Springer, pp 47–53
21. Shor PW (1999) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev 41(2):303–332
22. Takayasu A, Watanabe Y (2017) Lattice-based revocable identity-based encryption with bounded decryption key exposure resistance. In: Australasian conference on information security and privacy. Springer, pp 184–204
23. Zhang X, Tang Y, Wang H, Chunxiang X, Miao Y, Cheng H (2019) Lattice-based proxy-oriented identity-based encryption with keyword search for cloud storage. Inf Sci 494:193–207