Advances in Mathematics of Communications doi:10.3934/amc.2021050

A MULTIVARIATE IDENTITY-BASED BROADCAST ENCRYPTION WITH APPLICATIONS TO THE INTERNET OF THINGS

Vikas Srivastava

Department of Mathematics
National Institute of Technology Jamshedpur, Jamshedpur-831014, India

Sumit Kumar Debnath*

Department of Mathematics
National Institute of Technology Jamshedpur, Jamshedpur-831014, India

Pantelimon Stănică

Department of Applied Mathematics
Naval Postgraduate School, Monterey, CA 93943, USA

Saibal Kumar Pal

SAG Lab
Defense Research & Development Organization, Delhi-110054, India

(Communicated by Delaram Kahrobaei)

Abstract. When Kevin Ashton proposed the catchword 'Internet of Things' in 1999, little did he know that technology will become an indispensable part of human lives in just two decades. In short, the Internet of Things (IoT), is a catch-all terminology used to describe devices connected to the internet. These devices can share and receive data as well as provide instructions over a network. By design itself, the IoT system requires multicasting data and information to a set of designated devices, securely. Taking everything into account, Broadcast Encryption (BE) seems to be the natural choice to address the problem. BE allows an originator to broadcast ciphertexts to a big group of receivers in a well-organized and competent way, while ensuring that only designated people can decrypt the data. In this work, we put forward the first Identity-Based Broadcast Encryption scheme based on multivariate polynomials that achieves post-quantum security. Multivariate public key cryptosystems (MPKC), touted as one of the most promising post-quantum cryptography candidates, forms the foundation on which our scheme relies upon, which allows it to be very cost-effective and faster when implemented. In addition, it also provides resistance to collusion attack, and as a consequence our scheme can be utilized to form an efficient and robust IoT system.

2020 *Mathematics Subject Classification:* Primary: 94A60; 68M12; 68P25; 68P30.

Key words and phrases: Multivariate public key cryptography; IoT; post-quantum cryptography; broadcast encryption; identity based cryptography.

The work is supported by DRDO, India (ERIP/ER/202005001/M/01/1775).

* Corresponding author: sdebnath.math@nitjsr.ac.in.

1. Introduction

The Internet of Things (IoT) is an upcoming technology where the devices are connected to the internet and can "talk" to each other over the network. The Internet of Things (IoT) is cutting across our lives in a myriad of ways. From smartwatches to remote door locks, it has already become an indispensable part of our lives. In all likelihood, its impact on our lives will keep on increasing. More often than not, disseminating data to a group of devices connected over a network is a vital part of the IoT systems. In other words, an IoT network requires multicasting sensitive and delicate content prone to privacy theft. Considering the context, Broadcast Encryption (BE) is an efficient and robust cryptographic building block that provides a logical solution to IoT by allowing a broadcaster to broadcast encrypted content to a set of authorized devices. BE empowers broadcaster to make multicast efficiently. Moreover, it also ensures security and confidentiality of user's data.

Naor and Fiat first presented the cryptographic prototype of BE [15]. BE [12, 15, 22] allows the delivery of the encrypted data through a broadcast channel in such a manner that decrypting data is only possible for legitimate users. In more detail, given a subset S of the universe, a sender can encrypt content to S using the public keys such that the user with their private keys can only decrypt encrypted matter if it belongs to the set S. Another property that BE should satisfy is that of collusion resistance, requiring that even assuming all users (not in S) collude together, they cannot gain any knowledge about the broadcasted data (such a scheme is called collusion resistant BE). A fully collusion resistant BE with a short secret key and a ciphertext was developed by Boneh et al. [3]. Furthermore, Delerablée [8], and Sakai and Furukawa [24] conceived the idea of identity based BE (IB-BE).

The hardness of number theoretic problems such as factorization of large integers and discrete logarithms form the base upon which the majority of current cryptographic schemes's security relies. There is no need to mention how important the security of communication and information exchange in the modern world is, and cryptography techniques are at the forefront of ensuring the soundness of the information exchange. There have been several constructions of BE but their security is based on problems like integer factorization or discrete logarithms. Due to Shor's algorithm [25], the security of these classical broadcast encryption schemes is under a big threat in a quantum realm, since Shor's algorithm can solve the above-mentioned number theoretic problems in polynomial time, thus rendering all the current schemes insecure.

As a consequence, there is a growing need for schemes that are based on mathematical problems, which, even quantum computers do not have an advantage on. Multivariate public-key cryptosystem (MPKC) seems to be a promising alternative in this area. The security of MPKC is based on the fact that solving a system of a random quadratic multivariate polynomial is NP-hard [16]. MPKC has so far shown its considerable potential in providing a reliable alternative to classic cryptographic schemes.

1.1. Our contribution.

In this paper, we introduce the design and analysis of the first identity-based broadcast encryption scheme based on the MPKC. The proposed scheme, MulIB-BE consists of four algorithms, namely MulIB-BE.Setup, MulIB-BE.KeyExtract, MulIB-BE.Encrypt, MulIB-BE.Decrypt. Given the total number of users for which the broadcast is intended, broadcaster generates master

public key and master secret key using the algorithm MulIB-BE.Setup. The broadcaster, given S_{Auth}, a subset of $\{U_1, \ldots, U_N\}$ of authorized users, runs the algorithm MulIB-BE.Encrypt to produce the pair (Hdr, K) using the master public key MPK (see Section 2.3 for the meaning of these acronyms). The user U_i with identifier γ_i runs the algorithm MulIB-BE.Decrypt to extract the key from the ciphertext. Our scheme is secure from collusion attack by any number of colluders. The proposed design resists rank attacks and direct attacks. We present the efficiency and complexity analysis of our novel design. In particular, the sizes for the master public key and ciphertext for our scheme are $m\binom{n+2}{2}\binom{N+8}{8}$, respectively, $m\binom{N+9}{9}+1$ field $(\mathbb{F}_q)$ elements, where m is the total number of multivariate quadratic polynomials, n is the total number of variables of the underlying MPKC and N is the total number of broadcasters. Since BE is an efficient and robust cryptographic building block that provides a logical solution by allowing a broadcaster to broadcast encrypted content to a set of authorized devices, our scheme can be used as a key building block in IoT systems. Implementation of the proposed scheme only requires computing field multiplications and additions, making it faster and more efficient than classical schemes. Thereby, our design can be used to form efficient, high-performance IoT systems that provide strong privacy guarantees.

1.2. Organization. The paper is organized in the following manner. The preliminaries are contained in Section 2. Then we present our MulIB-BE in Section 3 followed by its security analysis in Section 4 and efficiency analysis in Section 5. In the following, application of MulIB-BE to IoT has been presented in Section 6 followed by the conclusions in Section 7.

2. Preliminaries

Let $\mathbb{F}_q$ denote the finite field of order q, which is a power of a prime p. A multivariate quadratic polynomial in n variables $z_1, \ldots, z_n$ is of the form

$$f(\mathbf{z}) = \sum_{i,j} a_{ij} z_i z_j + \sum_i b_i z_i + c,$$

where $\mathbf{z} = (z_1, \ldots, z_n)$ and the coefficients $a_{ij}, b_i,$ and $c \in \mathbb{F}_q$. The underlying idea and concept behind the design of MPKC is to select a system $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ of m multivariate polynomials of degree two in n variables. We stipulate that this map $\mathcal{F}$, also known as central map, is easily inverted in the sense that finding the preimage of y under $\mathcal{F}$ is easy. To obfuscate the structure of $\mathcal{F}$, we start by picking up two affine invertible transformations $\mathcal{S} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $\mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^n$. The public key of the cryptosystem is the composition $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, and the secret key of the MPKC is the triple $(\mathcal{S}, \mathcal{F}, \mathcal{T})$.

2.1. Multivariate encryption scheme [11]. A multivariate encryption scheme consists of the following three algorithms:

- $(PK, SK) \leftarrow \mathsf{Gen}(\eta)$: Given a security parameter η, Gen outputs the pair of public key and private key $(\mathcal{P}, \{\mathcal{S}, \mathcal{F}, \mathcal{T}\})$.
- $\mathsf{CText} \leftarrow \mathsf{Encrypt}(m, PK)$: Given a message $m \in \mathbb{F}_q^n$, the encryptor evaluates $y = \mathcal{P}(m) \in \mathbb{F}_q^m$ and outputs y as a ciphertext CText.
- $m \leftarrow \mathsf{Decrypt}(\mathsf{CText}, SK)$: Given a ciphertext $\mathsf{CText} = y \in \mathbb{F}_q^m$, the decryptor executes recursively $\alpha = \mathcal{S}^{-1}(y), \beta = \mathcal{F}^{-1}(\alpha)$ and $m = \mathcal{T}^{-1}(\beta)$ to get back the message m.

2.2. HARDNESS ASSUMPTION [11]. The mathematical problem which lies at the heart of nearly all the multivariate public key cryptosystem is the so called MQ problem. Succinctly speaking, it says that solving a system of quadratic multivariate polynomial is NP-hard. So far there has been no algorithm that can solve it in polynomial time. The MQ problem is formulated mathematically as follows.

Definition 2.1. Given a system $\mathcal{R} = \left(r_{(1)}(\delta, \ldots, \delta_n), \ldots, r_{(k)}(\delta_1, \ldots, \delta_n)\right)$ of k quadratic equations with each $r_{(i)} \in \mathbb{F}_q[\delta_1, \ldots, \delta_n]$, find values $(\bar{\delta}_1, \ldots, \bar{\delta}_n) \in \mathbb{F}_q^n$ such that

$$r_{(1)}\left(\bar{\delta}_1, \ldots, \bar{\delta}_n\right) = \cdots = r_{(k)}\left(\bar{\delta}_1, \ldots, \bar{\delta}_n\right) = 0.$$

In the following section we give the formal definition of IB-BE.

2.3. IDENTITY-BASED BROADCAST ENCRYPTION SCHEME [24]. The identity based BE consists of the following algorithms:

- $(MSK, PK) \leftarrow \mathsf{Setup}(N, \eta)$: Given a security parameter η and the total number of receivers N, Setup algorithm outputs a public key PK and a master secret key MSK.
- $(d_{Id}) \leftarrow \mathsf{KeyExtract}(PK, MSK, Id)$: Given PK, MSK and a unique identifier Id of a receiver as input, KeyExtract outputs secret key d_{Id} of user with identity Id.
- $(Hdr, K) \leftarrow \mathsf{Encrypt}(S, PK)$: Given a subset $S \subseteq \{1, \ldots, N\}$ and a public key PK as input, Encrypt outputs the pair (Hdr, K). Here, K is the encryption key and Hdr, also known as broadcast ciphertext is called header.
- $K \leftarrow \mathsf{Decrypt}(S, Id, d_{Id}, Hdr, PK)$: Given a subset $S \subseteq \{1, \ldots, N\}$, user identity Id, private key d_{Id}, the public key PK, and the header Hdr, Decrypt outputs K, if user belongs to the set S. Otherwise, it outputs 0.

To ensure the correctness of the system, we require that for all users in S, if $(MSK, PK) \leftarrow \mathsf{Setup}(N, \eta), (d_{Id}) \leftarrow \mathsf{KeyExtract}(PK, MSK, Id)$, and $(Hdr, K) \leftarrow \mathsf{Encrypt}(S, PK)$, then $\mathsf{Decrypt}(S, Id, d_{Id}, Hdr, PK) = K$.

3. PROPOSED MULTIVARIATE IDENTITY-BASED BROADCAST ENCRYPTION SCHEME(MulIB-BE)

Our proposed scheme comprises of following algorithms: (i) MulIB-BE.Setup, (ii) MulIB-BE.KeyExtract, (iii) MulIB-BE.Encrypt, (iv) MulIB-BE.Decrypt. Let N denotes the number of users, $\{U_1, \ldots, U_N\}$ for which the transmitter wants to make the BE. Let $\gamma_i = (\gamma_{i1}, \gamma_{i2}, \ldots, \gamma_{iN})$ be the unique identifier corresponding to each user. Using MulIB-BE.Setup, the broadcaster generates master public key MPK and the master secret key MSK. Using the master secret key MSK and $\{\gamma_i\}_{i=1}^N$, the broadcaster generates the secret key for each user. The broadcaster, given S_{Auth}, a subset of $\{U_1, \ldots, U_N\}$ of authorized users, runs the algorithm MulIB-BE.Encrypt to produce the pair (Hdr, K) using the master public key MPK. The user U_i with identifier γ_i runs the algorithm MulIB-BE.Decrypt to extract the key from the ciphertext. We now describe the design of our proposed scheme in detail.

- $(MSK, MPK) \leftarrow \mathsf{MulIB\text{-}BE.Setup}(N, \eta)$: Given N and the security parameter η, the broadcaster generates $MPK = \left(P^{(\widetilde{\mathbf{d}})}, \{\gamma_i\}_{i=1}^N\right)$ and master secret key $MSK = \left(\mathcal{S}^{(\widetilde{\mathbf{d}})}, \mathcal{F}^{(\widetilde{\mathbf{d}})}, \mathcal{T}^{(\widetilde{\mathbf{d}})}\right)$. Here, $\gamma_i \in \mathbb{F}_q^N$ such that Det $(\gamma_1, \ldots, \gamma_N) \neq 0$ and $\widetilde{\mathbf{d}}$ denotes N tuple $(\widetilde{d}_1, \ldots, \widetilde{d}_N)$ such that:

1. $\mathcal{S}^{(\widetilde{\mathbf{d}})} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ is an affine invertible map of the form

$$\mathcal{S}^{(\widetilde{\mathbf{d}})}(y_1, \ldots, y_m) = \left(\mathcal{S}_1^{(\widetilde{\mathbf{d}})}(y_1, \ldots, y_m), \ldots, \mathcal{S}_m^{(\widetilde{\mathbf{d}})}(y_1, \ldots, y_m)\right)$$

with $\mathcal{S}_i^{(\widetilde{\mathbf{d}})}(y_1, \ldots, y_m) = \sum \mathcal{S}_{(i,j)}^{(\widetilde{\mathbf{d}})}(\widetilde{d}_1, \ldots, \widetilde{d}_N) y_j + \mathcal{S}_{(i,0)}^{(\widetilde{\mathbf{d}})}(\widetilde{d}_1, \ldots, \widetilde{d}_N)$, where every $\mathcal{S}_{(i,j)}^{(\widetilde{\mathbf{d}})}(\widetilde{d}_1, \ldots, \widetilde{d}_N)$ is a quadratic polynomial in $\widetilde{d}_1, \ldots, \widetilde{d}_N$.

2. $\mathcal{T}^{(\widetilde{\mathbf{d}})} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is an affine invertible map of the form

$$\mathcal{T}^{(\widetilde{\mathbf{d}})}(y_1, \ldots, y_n) = \left(\mathcal{T}_1^{(\widetilde{\mathbf{d}})}(y_1, \ldots, y_n), \ldots, \mathcal{T}_n^{(\widetilde{\mathbf{d}})}(y_1, \ldots, y_n)\right)$$

with $\mathcal{T}_i^{(\widetilde{\mathbf{d}})}(y_1, \ldots, y_n) = \sum \mathcal{T}_{(i,j)}^{(\widetilde{\mathbf{d}})}(\widetilde{d}_1, \ldots, \widetilde{d}_N) y_j + \mathcal{T}_{(i,0)}^{(\widetilde{\mathbf{d}})}(\widetilde{d}_1, \ldots, \widetilde{d}_N)$, where every $\mathcal{T}_{(i,j)}^{(\widetilde{\mathbf{d}})}(\widetilde{d}_1, \ldots, \widetilde{d}_N)$ is a quadratic polynomial in $\widetilde{d}_1, \ldots, \widetilde{d}_N$.

3. $\mathcal{F}^{(\widetilde{\mathbf{d}})} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is a system of m multivariate polynomials $\left(\mathcal{F}_1^{(\widetilde{\mathbf{d}})}, \ldots, \mathcal{F}_m^{(\widetilde{\mathbf{d}})}\right)$ of the following form

$$\mathcal{F}_k^{(\widetilde{\mathbf{d}})} = \sum_{i,j} a_{k_{ij}} y_i y_j + \sum_i b_{k_i} y_i + c_k,$$

where $a_{k_{ij}}, b_{k_i}, c_k$ are quadratic polynomials in $\widetilde{d}_1, \ldots, \widetilde{d}_N$.

4. $\mathcal{P}^{(\widetilde{\mathbf{d}})} = \mathcal{S}^{(\widetilde{\mathbf{d}})} \circ \mathcal{F}^{(\widetilde{\mathbf{d}})} \circ \mathcal{T}^{(\widetilde{\mathbf{d}})} = \begin{pmatrix} \mathcal{P}_1^{(\widetilde{\mathbf{d}})}(y_1, \ldots, y_n) \\ \mathcal{P}_2^{(\widetilde{\mathbf{d}})}(y_1, \ldots, y_n) \\ \cdots\cdots \\ \mathcal{P}_m^{(\widetilde{\mathbf{d}})}(y_1, \ldots, y_n) \end{pmatrix}$ such that $\mathcal{P}_k^{(\widetilde{\mathbf{d}})}$ can be written as

$$\mathcal{P}_k^{(\widetilde{\mathbf{d}})} = \sum_{i,j} \bar{a}_{k_{ij}} y_i y_j + \sum_i \bar{b}_{k_i} y_i + \bar{c}_k,$$

where $\bar{a}_{k_{ij}}, \bar{b}_{k_i}, \bar{c}_k$ are polynomials in $\widetilde{d}_1, \ldots, \widetilde{d}_N$ of degree four.

- $(d_{Id}) \leftarrow \mathsf{MultIB\text{-}BE.KeyExtract}(MPK, MSK, Id)$: Given $MSK = \left(\mathcal{S}^{(\widetilde{\mathbf{d}})}, \mathcal{F}^{(\widetilde{\mathbf{d}})}, \mathcal{T}^{(\widetilde{\mathbf{d}})}\right)$ and a unique identifier γ_i, the algorithm outputs $d_{\gamma_i} = \left(\mathcal{S}^{(\gamma_i)}, \mathcal{F}^{(\gamma_i)}, \mathcal{T}^{(\gamma_i)}\right)$.
- $(Hdr, K) \leftarrow \mathsf{MultIB\text{-}BE.Encrypt}(S_{Auth}, MPK)$: On input S_{Auth}, MPK, broadcaster executes the following steps:
  1. Solves the following system of equation

$$\langle \mathbf{b}, \gamma_i \rangle = 1 \text{ for } U_i \in S_{Auth}$$
$$\langle \mathbf{b}, \gamma_i \rangle = 0 \text{ for } U_i \in \{U_1, \ldots, U_N\} \setminus S_{Auth}$$

  to compute $\mathbf{b} = (b_1, \ldots, b_N)$.
  2. Chooses randomly n linear functions $e_i(\widetilde{\mathbf{d}})$ in $\widetilde{d}_1, \ldots, \widetilde{d}_N$ such that $\sum_{i=1}^n e_i = (\langle \mathbf{b}, \widetilde{\mathbf{d}} \rangle) K$.
  3. Sets $Hdr = \mathcal{P}^{(\widetilde{\mathbf{d}})}\left(e_1(\widetilde{\mathbf{d}}), \ldots, e_n(\widetilde{\mathbf{d}})\right) = \left(h_1(\widetilde{\mathbf{d}}), \ldots, h_m(\widetilde{\mathbf{d}})\right)$ and outputs the pair $\mathsf{CT}_{BE} = (Hdr, K)$ as broadcast ciphertext.
- $K \leftarrow \mathsf{MultIB\text{-}BE.Decrypt}(S, Id, d_{Id}, Hdr, MPK)$: On receiving CT_{BE} from the broadcaster, an user U_i with identity γ_i does the following.
  1. Evaluates $h_1(\widetilde{\mathbf{d}}), \ldots, h_m(\widetilde{\mathbf{d}})$ at $\widetilde{\mathbf{d}} = \gamma_i$.
  2. Computes $\left(\mathcal{S}^{(\gamma_i)}\right)^{-1} (h_1(\gamma_i), \ldots, h_m(\gamma_i)) = (g_1, \ldots, g_m)$.

3. Finds the preimage of $(g_1, \ldots, g_m)$ under $\mathcal{F}^{(\gamma_i)}$ that is $\left(\mathcal{F}^{(\gamma_i)}\right)^{-1}(g_1, \ldots, g_m) = (j_1, \ldots, j_n)$.
4. Computes $\left(\mathcal{T}^{(\gamma_i)}\right)^{-1}(j_1, \ldots, j_n) = (\widetilde{e}_1, \ldots, \widetilde{e}_n)$.
5. Determines $\sum \widetilde{e}_i$ and outputs it as key.

- **Correctness:** Note that $\sum \widetilde{e}_i = \sum e_i(\gamma_i) = (\langle \mathbf{b}, \gamma_i \rangle)K$. Thus, $\sum \widetilde{e}_i$ turns out to be K if $\langle \mathbf{b}, \gamma_i \rangle = 1$ and 0 if $\langle \mathbf{b}, \gamma_i \rangle = 0$. By the construction of $\mathbf{b}$, $\langle \mathbf{b}, \gamma_i \rangle = 1$ only for the user $U_i \in S_{Auth}$ and $\langle \mathbf{b}, \gamma_i \rangle = 0$ for the user $U_i \in \{U_1, \ldots, U_N\} \setminus S_{Auth}$. Therefore we may conclude that only the user $U_i \in S_{Auth}$ can obtain the key K, while the other users receive 0.

4. Security analysis

4.1. Direct attacks. A direct attack is the most canonical way to attack an encryption system based on multivariate public-key cryptography. As we already know Multivariate Quadratic polynomial (MQ) problem forms the backbone of security for multivariate public key cryptosystems. The following system of quadratic equations is a case in point

$$P^{(\widetilde{\mathbf{d}})}(e_1, e_2, \ldots, e_n) = (h_1, h_2, \ldots, h_m).$$

A subtle point to note here is that in Encryption Schemes, m is greater than n to ensure that a unique plaintext is received after we are done with decryption procedure. To put it another way, we are handling an overdetermined system of equations.

Direct attack algorithms include the XL [7] and Hybrid $F5$ [1], to name just a few. If we go by efficiency and practicality, Hybrid $F5$ is the fastest algorithm for direct attacks at the moment. The heart of the matter is that we pick some of the variables beforehand and try to create an overdetermined system of equations. The public key equations that we encounter are more or less random in nature. Since it is an over-determined system of equations, it would not be wrong to assume that they behave like a semi-regular system of equations, whose degree of regularity (d_{reg}) is easy to predict. Using this d_{reg}, the hybrid $F5$ computation complexity is given by

$$\text{Complexity }_{\text{Hybrid}} = q^k \mathcal{O}\left(t\binom{n-k+d_{\text{reg}}-1)}{d_{\text{reg}}}\right),$$

where t denotes the number of equations and n denote the number of variables. We can summarize this subsection by stating that best direct attack algorithm when working over medium field is $HF5$, while when one is working over large fields Gröbner Basis Algorithms like $F4$ (or $F5$) [14, 13] suits best. When the underground field is small (assuming $m = \epsilon n^2, \epsilon > 0$) the most effective algorithm is the XL algorithm [7], whose complexity is given by $\mathcal{O}((n)^{\omega D}/D!)$ where $D \sim [1/\sqrt{\epsilon}]$.

The difficulty of solving the Multivariate Quadratic (MQ) problem depends upon the size of the base field, number of equations (m), and number of variables (n). For the majority of the multivariate encryption schemes like ABC, $ZHFE$, and $QUAD$ cipher, the number of equations is set to be twice of the number of variables [28], that is, $m = 2n$. The proposed practical parameters, for the different levels of security, and base field sizes are provided in Table 1.

4.2. MinRank attack. The MinRank Attack [18] is based on the below stated MinRank Problem.

Table 1. Proposed practical parameters for MulIB-BE [26]

Level of Security (in bit)	Field ($\mathbb{F}_q$)	Number of equations (m)	Number of variables (n)
80	$\mathbb{F}_{2^{32}}$	112	56
	$\mathbb{F}_{2^{16}}$	200	100
	$\mathbb{F}_{2^8}$	264	128
90	$\mathbb{F}_{2^{32}}$	144	72
	$\mathbb{F}_{2^{16}}$	242	121
	$\mathbb{F}_{2^8}$	312	153
100	$\mathbb{F}_{2^{32}}$	180	90
	$\mathbb{F}_{2^{16}}$	288	144
	$\mathbb{F}_{2^8}$	364	180

MinRank Problem [6]. Let η, n, s be positive integers, and let $M_0, M_1, \ldots, M_\eta$ be $n \times n$ matrices with entries in a finite field $\mathbb{F}_q$. We want to find (if they exist) $\lambda_1, \ldots, \lambda_\eta \in \mathbb{F}_q$ such that $E_\lambda := M_0 - \sum_{i=1}^{\eta} \lambda_i M_i$ has rank not exceeding s.

In this attack we try to find a scalar linear combination of the matrices corresponding to polynomials of underlying MPKC having minimum rank. Let A_i denote the homogeneous quadratic part of the central polynomial $\mathcal{F}$. Let $\widetilde{A_i}$ be the matrix representation of A_i. Note that in our proposed scheme MulIB-BE, $\widetilde{A_i}$ has full rank and therefore our proposed scheme is immune to the MinRank attack.

4.3. Linearization equation attack. The linearization equation attack was used to break the C^* scheme and it first appeared in [23]. In the following, another variant was proposed [10] to break the MFE. The basic idea is to find a bijection between the plaintext and ciphertext. Note that in our proposed scheme MulIB-BE, the central map $\mathcal{F}$ is not a bijection and therefore our proposed scheme is immune to the linearization equation attack.

4.4. Resistance to collusion attack. In this attack, we examine the possibility of collusion by the users to extract the master secret key or the secret key of other users. The way we chose the coefficients of $\mathcal{S}^{(\widetilde{\mathbf{d}})}, \mathcal{T}^{(\widetilde{\mathbf{d}})}, \mathcal{F}^{(\widetilde{\mathbf{d}})}$ makes our scheme immune to the collusion attack. The computation of each private key coefficients involves solving an equation in $d_v = \frac{(N+1)(N+2)}{2}$ variables. Recall that N is the total number of users for which the Broadcaster wants to make the BE. Note that we can not extract the unlimited number of equations as the total number of users for which the message is being broadcasted is fixed. So even in the worst possible case, where all the N users collude together, we have a highly underdetermined system of linear equations. The whole complexity includes extracting equations, which is very costly as it depend on others and solving the aforementioned system of equations (whose complexity is around $(d_v(d_v-1)/2)^3$). Therefore, the total complexity is $\mathcal{O}(N^6)$, and hence it is secure from the collusion attack.

5. Efficiency

The communication and storage overheads of the proposed MulIB-BE are provided in the Table 2.

Table 2. Communication and Storage Overheads of MulIB-BE

MPK Size	$m\binom{n+2}{2}\binom{N+8}{8}$ field ($\mathbb{F}_q$) elements
Ciphertext Size	$m\binom{N+9}{9}+1$ field ($\mathbb{F}_q$) elements
MSK Size	$[m(m+1)+n(n+1)+m\binom{n+2}{2}]\binom{N+2}{2}$ field ($\mathbb{F}_q$) elements
SK Size	$[m(m+1)+n(n+1)+m\binom{n+2}{2}]$ field ($\mathbb{F}_q$) elements

Let κ denotes the field multiplications required for solving N linear equations,

$$\langle \mathbf{b}, \gamma_i \rangle = 1 \text{ for } U_i \in S_{Auth}$$
$$\langle \mathbf{b}, \gamma_i \rangle = 0 \text{ for } U_i \in \{U_1, \ldots, U_N\} \setminus S_{Auth}$$

in N unknowns $\mathbf{b} = (b_1, \ldots, b_N)$. Then we require $\kappa + nmN\binom{N+8}{8} + m\binom{n+2}{2}\binom{N+8}{8}N^2$ field multiplications for encryption and $m\sum_{i=1}^{9} i\binom{N+i-1}{i}$ field multiplications for decryption.

Table 3. Time complexity of MulIB-BE for 80-bit security level over $GF(256)$

	Time (in seconds)
Setup	11.91
Key Extraction	0.56
Encryption	2.17
Decryption	1.25

We assess the running time complexity of MulIB-BE in terms of setup, key extract, encryption, and decryption time for 80-bit security level over the field $GF(256)$. We utilize Simple Matrix ABC scheme with parameters $(q = 256, n = 128, m = 264)$ as the underlying secure multivariate encryption scheme. We made use of SageMath (version 9.2) for the implementation purpose, on a workstation with an Intel Core i5 1.60 GHz processor with 64-bit Linux Lite (v 5.2) operating system. Results are documented in Table 3.

Table 4. Comparison with existing schemes for 100-bit security level

Scheme	Secret key size (in kb)	Ciphertext size (in kb)	Post-quantum secure
ZhanoZhang-IB-BE [30]	0.375	1.25	×
A-IBBE [29]	0.05	0.875	×
Delerablée-IB-BE [9]	0.06	0.5	×
Kim, Jongkil et al. [21]	0.06	0.5	×
He, Kai et al. [20]	0.06	0.28	×
MulIB-BE	21.36	7.09	✓

Since there are no multivariate-based IB-BE in the current state of the art, we compare our proposed design MulIB-BE with other non-multivariate IB-BE. The size of the ciphertext and user's secret key size are crucial benchmarks to check the efficiency of IB-BE schemes. Therefore, we present the comparative analysis in Table 4 of MulIB-BE in terms of the user's secret key size and ciphertext size for 100-bit security level over $GF(256)$ with $N = 3$.

As evidenced in Table 4, it is a known disadvantage with MPKC-based scheme that the size of the keys is huge when compared to classical cryptosystems like RSA or ECC. However, MPKC-based schemes are very fast and can efficiently work on memory-constraint devices. This is because the core operations required in MPKC are only modular field multiplications and additions. In addition, unlike RSA or ECC, our proposed MulIB-BE provides security against the threat of quantum computers. Thus, MulIB-BE has compensatory advantages which gives it an upper hand over existing IB-BE.

6. An application to internet of things (IoT)

An IoT network requires multicasting sensitive and delicate content, prone to privacy theft. More often than not, broadcasting data securely into a set of legitimate devices connected over a network is an essential part of the IoT systems. Let us bolster the argument by supplementing it with an example of a health system using IoT. To facilitate remote monitoring of patients' health, an IoT system is used. In case of any problem, an emergency notification system disseminates information to concerned devices. Thus, such a system entails private health data of patients to be transferred to legitimate devices. To ensure the transmissions' secrecy and confidentiality, cryptographic techniques may provide powerful serviceability with practical efficiencies. Considering the context, BE is an efficient and resilient cryptographic primitive that enables an originator to make multicast efficiently; moreover, it also ensures security and confidentiality of user's data.

Based on key update, we can classify BE into two categories- Stateful BE and Stateless BE. In stateful BE [4], the secret key of clients can be updated after join. In the stateless BE [17, 19, 22], the key is exchanged only once in the initial setup. A natural question arises here, which type of BE is more suitable for IoT systems. Keeping in mind that IoT devices are small, and not every IoT device is ideal for frequent updates and management, so when it comes to implementation in an IoT system, we tend to prefer stateless broadcast encryption as a cryptographic building block. Our proposed scheme MulIB-BE is a stateless IB-BE, and therefore, it may be put to use to build a cost-effective and computationally efficacious IoT system.

This work puts forward a multivariate IB-BE. Our scheme can be employed to build an efficient and resilient IoT system. Our scheme is based on MPKC, which provides security even against attacks by quantum computers under the premise that the MQ problem is NP-hard. Implementation of the proposed scheme only requires doing finite field multiplication and additions. Our MulIB-BE, being a scheme based on a MPKC, is by and large fast and requires only inexpensive computing resources, that makes it ideal for use on economical and budget devices [2, 5, 27], for instance RFID devices and smart cards.

7. Conclusion

In this work, we design and analyse the first IB-BE based on multivariate public-key cryptosystems. The scheme resists collusion attack, and, in addition, our proposed scheme is immune to direct attacks, linearization attacks and rank attacks. Being a scheme whose implementation requires only doing the field multiplications and addition, MulIB-BE is computationally efficient. Our scheme can be efficiently applied to IoT systems as they require data transmission to a group of devices connected over a network safely and soundly. Making use of MulIB-BE in the background as the cryptographic building block, presumably, we can design safe and

sound IoT systems where a centralized device can broadcast data to connected devices in a privacy-preserving manner.

Acknowledgments

The authors express their deep appreciation to the editor for promptly handling our paper, as well as to the anonymous referee, whose thorough reading and constructive comments have greatly improved the paper. This work was supported by DRDO, India (ERIP/ER/202005001/M/01/1775).

References

[1] L. Bettale, J.-C. Faugëre and L. Perret, Hybrid approach for solving multivariate systems over finite fields, *J. Math. Cryptology*, **3** (2009), 177–197.

[2] A. Bogdanov, T. Eisenbarth, A. Rupp and C. Wolf, Time-area optimized public-key engines: MQ-cryptosystems as replacement for elliptic curves?, In *Cryptographic Hardware and Embedded Systems-CHES 2008*, **5154** (2008), 45–61.

[3] D. Boneh, C. Gentry and B. Waters, Collusion resistant broadcast encryption with short ciphertexts and private keys, *Advances in Cryptology–CRYPTO 2005*, **3621** (2005), 258–275.

[4] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor and B. Pinkas, Multicast security: A taxonomy and some efficient constructions, *IEEE INFOCOM '99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now (Cat. No.99CH36320)*, IEEE, 1999.

[5] A. I.-T. Chen, M.-S. Chen, T.-R. Chen, C.-M. Cheng, J. Ding, E. L.-H. Kuo, F. Y.-S. Lee and B.-Y. Yang, SSE implementation of multivariate PKCs on modern s86 CPUs, *Cryptographic Hardware and Embedded Systems - CHES 2009*, (2009), 33–48.

[6] N. T. Courtois, Efficient zero-knowledge authentication based on a linear algebra problem MinRank, In *Advances in Cryptology–ASIACRYPT 2001*, **2248** (2001), 402–421.

[7] N. T. Courtois, A. Klimov, J. Patarin and A. Shamir, Efficient algorithms for solving overdefined systems of multivariate polynomial equations, *Advances in Cryptology–EUROCRYPT 2000*, **1807** (2000), 392–407.

[8] C. Delerablée, Identity-based broadcast encryption with constant size ciphertexts and private keys, In *Advances in Cryptology–ASIACRYPT 2007*, **4833** (2007), 200–215.

[9] C. Delerablée, Identity-based broadcast encryption with constant size ciphertexts and private keys, In *Advances in Cryptology–ASIACRYPT 2007*, **4833** (2007), 200–215.

[10] J. Ding, L. Hu, X. Nie, J. Li and J. Wagner, High order linearization equation hole attack on multivariate public key cryptosystems, In *Public Key Cryptography – PKC 2007*, **4450** (2007), 233–248.

[11] J. Ding, A. Petzoldt and D. S. Schmidt, *Multivariate Public Key Cryptosystems*, 2^{nd} edition, Advances in Information Security, 80. Springer, New York, 2020.

[12] Y. Dodis and N. Fazio, Public key broadcast encryption for stateless receivers, In *Digital Rights Management*, **2696** (2002), 61–80.

[13] J. C. Faugére, A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5), *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, (2002), 75–83.

[14] J.-C. Faugére, A new efficient algorithm for computing Gröbner bases (F_4), *J. Pure Appl. Algebra*, **139** (1999), 61–88.

[15] A. Fiat and M. Naor, Broadcast encryption, *Advances in Cryptology–CRYPTO' 93*, **773** (1993), 480–491.

[16] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, A Series of Books in the Mathematical Sciences, 1979.

[17] M. T. Goodrich, J. Z. Sun and R. Tamassia, Efficient tree-based revocation in groups of low-state devices, *Advances in Cryptology–CRYPTO 2004*, **3152** (2004), 511–527.

[18] L. Goubin and N. T. Courtois, Cryptanalysis of the TTM cryptosystem, *Advances in Cryptology–ASIACRYPT 2000*, **1976** (2000), 44–57.

[19] D. Halevy and A. Shamir, The LSD broadcast encryption scheme, *Advances in Cryptology–CRYPTO 2002*, **2442** (2002), 47–60.

[20] K. He, J. Weng, J.-N. Liu, J. K. Liu, W. Liu and R. H. Deng, Anonymous identity-based broadcast encryption with chosen-ciphertext security, In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, (2016), 247–255.
[21] J. Kim, S. Camtepe, W. Susilo, S. Nepal and J. Baek, Identity-based broadcast encryption with outsourced partial decryption for hybrid security models in edge computing, *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, (2019), 55–66.
[22] D. Naor, M. Naor and J. Lotspiech, Revocation and tracing schemes for stateless receivers, *Advances in Cryptology–CRYPTO 2001*, **2139** (2001), 41–62.
[23] J. Patarin, Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88, *Advances in Cryptology–CRYPT0' 95*, **963** (1995), 248–261.
[24] R. Sakai and J. Furukawa, *Identity-based broadcast encryption*, IACR Cryptol. ePrint Arch., 20072/17, URL http://eprint.iacr.org/2007/217.
[25] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Rev*, **41** (1999), 303–332.
[26] C. Tao, H. Xiang, A. Petzoldt and J. Ding, Simple matrix–a multivariate public key cryptosystem (MPKC) for encryption, *Finite Fields Appl.*, **35** (2015), 352–368.
[27] B.-Y. Yang, C.-M. Cheng, B.-R. Chen and J.-M. Chen, Implementing minimized multivariate PKC on low-resource embedded systems, *Security in Pervasive Computing*, Springer Berlin Heidelberg, **3934** (2006), 73–88.
[28] T. Yasuda, X. Dahan, Y.-J. Huang, T. Takagi and K. Sakurai, *MQ Challenge: Hardness Evaluation of Solving Multivariate Quadratic Problems*, Cryptology ePrint Archive, Report, 2015/275, 2015, https://eprint.iacr.org/2015/275.
[29] Z. Zhao, F. Guo, J. Lai, W. Susilo, B. Wang and Y. Hu, Accountable authority identity-based broadcast encryption with constant-size private keys and ciphertexts, *Theoret. Comput. Sci.*, **809** (2020), 73–87.
[30] X. Zhao and F. Zhang, Fully CCA2 secure identity-based broadcast encryption with black-box accountable authority, *Journal of Systems and Software*, **85** (2012), 708–716.

Appendix A. Toy example

Suppose there are three users A_1, A_2 and A_3 for which the broadcaster wants to make the BE. Let S_{Auth} denote the set of authorized users. Let $S_{Auth} = \{A_1\}$. Let γ_i denote the unique identifier for user A_i such that $\mathrm{Det}(\gamma_1, \ldots, \gamma_3) \neq 0$, say,

$$\gamma_1 = (1,0,0), \gamma_2 = (0,1,0), \text{ and } \gamma_3 = (0,0,1).$$

We set $n = 1, m = 2$.

1. Consider $\mathcal{S}^{(\widetilde{\mathbf{d}})} : \mathbb{F}_q^2 \to \mathbb{F}_q^2$ given by
$$\mathcal{S}^{(\widetilde{\mathbf{d}})}(y_1, y_2) = \left((\widetilde{d_1} + \widetilde{d_3})y_1 + (\widetilde{d_3}\widetilde{d_2})y_2, (\widetilde{d_2}d_1)y_1 + (\widetilde{d_1} + \widetilde{d_3})y_2\right).$$
2. Consider $\mathcal{T}^{(\widetilde{\mathbf{d}})} : \mathbb{F}_q^1 \to \mathbb{F}_q^1$ given by
$$\mathcal{T}^{(\widetilde{\mathbf{d}})}(y_1) = (\widetilde{d_1} + \widetilde{d_3})y_1.$$
3. Consider $\mathcal{F}^{(\widetilde{\mathbf{d}})} : \mathbb{F}_q^1 \to \mathbb{F}_q^2$ given by
$$\mathcal{F}^{(\widetilde{\mathbf{d}})}(y_1) = \left((\widetilde{d_1}\widetilde{d_2} + \widetilde{d_1} + \widetilde{d_3}^2)y_1^2, (\widetilde{d_3} + \widetilde{d_2}\widetilde{d_1})y_1^2\right).$$
4. Determine $\mathcal{P}^{(\widetilde{\mathbf{d}})} = \mathcal{S}^{(\widetilde{\mathbf{d}})} \circ \mathcal{F}^{(\widetilde{\mathbf{d}})} \circ \mathcal{T}^{(\widetilde{\mathbf{d}})}$ which will take the form, $\mathcal{P}^{(\widetilde{\mathbf{d}})}(y_1) = \big((\widetilde{d_1}+\widetilde{d_3})(\widetilde{d_1}\widetilde{d_2}+\widetilde{d_1}+\widetilde{d_3}^2)(\widetilde{d_1}+\widetilde{d_3})y_1^2+(\widetilde{d_3}\widetilde{d_2})(\widetilde{d_3}+\widetilde{d_2}\widetilde{d_1})(\widetilde{d_1}+\widetilde{d_3})y_1^2, \widetilde{d_2}\widetilde{d_1}(\widetilde{d_1}\widetilde{d_2}+\widetilde{d_1}+\widetilde{d_3}^2)(\widetilde{d_1}+\widetilde{d_3})y_1^2 + (\widetilde{d_1}+\widetilde{d_3})(\widetilde{d_3}+\widetilde{d_2}\widetilde{d_1})(\widetilde{d_1}+\widetilde{d_3})y_1^2\big)$.

We can determine the private key of the users. For instance, the private key of A_1 is $\mathcal{S}^{(\gamma_1)}(y_1, y_2) = (y_1, y_2), \mathcal{T}^{(\gamma_1)}(y_1) = y_1, \mathcal{F}^{(\gamma_1)}(y_1) = (y_1^2, 0)$, and the private key of user A_3 is $\mathcal{S}^{(\gamma_3)}(y_1, y_2) = (y_1, y_2), \mathcal{T}^{(\gamma_3)}(y_1) = y_1, \mathcal{F}^{(\gamma_3)}(y_1) = (y_1^2, y_1^2)$.

Below, we compute $\mathbf{b} = (b_1, b_2, b_3)$:

$$\begin{aligned}\langle \mathbf{b}, \gamma_1 \rangle = 1 &\implies b_1 = 1,\\ \langle \mathbf{b}, \gamma_2 \rangle = 0 &\implies b_2 = 0,\\ \langle \mathbf{b}, \gamma_3 \rangle = 0 &\implies b_3 = 0.\end{aligned}$$

Now we have to choose randomly n linear functions $e_i(\widetilde{\mathbf{d}})$ in $\widetilde{d}_1, \ldots, \widetilde{d}_N$ such that $\sum_{i=1}^{n} e_i = (\langle \mathbf{b}, \widetilde{\mathbf{d}} \rangle)K$. In our case $n = 1$. We pick $e_1(\widetilde{\mathbf{d}}) = \widetilde{d}_1 K$. In the next step, we set $Hdr = \mathcal{P}^{(\widetilde{\mathbf{d}})}(e_1(\widetilde{\mathbf{d}}), \ldots, e_n(\widetilde{\mathbf{d}})) = (h_1(\widetilde{\mathbf{d}}), \ldots, h_m(\widetilde{\mathbf{d}}))$ and output the pair $\mathsf{CT}_{BE} = (Hdr, K)$ as the broadcast ciphertext. Thus, we compute $Hdr = \mathcal{P}^{(\widetilde{\mathbf{d}})}(e_1(\widetilde{\mathbf{d}})) = ((\widetilde{d}_1 + \widetilde{d}_3)(\widetilde{d}_1\widetilde{d}_2 + \widetilde{d}_1 + \widetilde{d}_3{}^2)(\widetilde{d}_1 + \widetilde{d}_3)\widetilde{d}_1{}^2K^2 + (\widetilde{d}_3\widetilde{d}_2)(\widetilde{d}_3 + \widetilde{d}_2\widetilde{d}_1)(\widetilde{d}_1 + \widetilde{d}_3)\widetilde{d}_1{}^2K^2, \widetilde{d}_2\widetilde{d}_1(\widetilde{d}_1\widetilde{d}_2 + \widetilde{d}_1 + \widetilde{d}_3{}^2)(\widetilde{d}_1 + \widetilde{d}_3)\widetilde{d}_1{}^2K^2 + (\widetilde{d}_1 + \widetilde{d}_3)(\widetilde{d}_3 + \widetilde{d}_2\widetilde{d}_1)(\widetilde{d}_1 + \widetilde{d}_3)\widetilde{d}_1{}^2K^2) = (h_1(\widetilde{\mathbf{d}}), h_2(\widetilde{\mathbf{d}}))$.

Recall that in our toy example, the legitimate user is A_1. Let us see how A_1 gets back the key from the Hdr. First A_1 evaluates Hdr at $\widetilde{\mathbf{d}} = \gamma_1$. We put $\widetilde{d}_1 = 1, \widetilde{d}_2 = 0$ and $\widetilde{d}_3 = 0$. We find that $(h_1(\widetilde{\mathbf{d}}), h_2(\widetilde{\mathbf{d}}))$ evaluated at $\widetilde{\mathbf{d}} = \gamma_1$ is $(K^2, 0)$. Note that, $(\mathcal{S}^{(\gamma_1)})^{-1}(K^2, 0) = (K^2, 0)$. Next step is to find the preimage of $(K^2, 0)$ under $\mathcal{F}^{(\gamma_1)}$. Observe that $\mathcal{F}^{(\gamma_1)}(K) = (K^2, 0)$ so the preimage of $(K^2, 0)$ is K. In the final step, we calculate the inverse of K under $\mathcal{T}^{(\gamma_1)}$. We have $(\mathcal{T}^{(\gamma_1)})^{-1}(K) = K$. Thus, we see that user A_1 is able to get back the key from the broadcast ciphertext.

We can easily see that users outside S_{Auth}, namely A_2, A_3 can not obtain K. For instance, we consider the user A_3, who evaluates Hdr at $\widetilde{\mathbf{d}} = \gamma_3$. We put $\widetilde{d}_1 = 0, \widetilde{d}_2 = 0$ and $\widetilde{d}_3 = 1$. We find that $(h_1(\widetilde{\mathbf{d}}), h_2(\widetilde{\mathbf{d}}))$ evaluated at $\widetilde{\mathbf{d}} = \gamma_3$ is $(0, 0)$. Note that, $(\mathcal{S}^{(\gamma_3)})^{-1}(0, 0) = (0, 0)$. Next step is to find the preimage of $(0, 0)$ under $\mathcal{F}^{(\gamma_3)}$. Observe that $\mathcal{F}^{(\gamma_3)}(0) = (0, 0)$, so the preimage of $(0, 0)$ is 0. In the final step, we calculate the inverse of 0 under $\mathcal{T}^{(\gamma_3)}$. We have $(\mathcal{T}^{(\gamma_3)})^{-1}(0) = 0$. Thus, we see that user A_3 is unable to get back the key from the broadcast ciphertext.

Received April 2021; 1st revision August 2021; 2nd revision September 2021; early access November 2021.

E-mail address: vikas.math123@gmail.com
E-mail address: sdebnath.math@nitjsr.ac.in
E-mail address: pstanica@nps.edu
E-mail address: skptech@yahoo.com