Storage Friendly Provably Secure Multivariate Identity-Based Signature from Isomorphism of Polynomials Problem

Ratna Dutta[1], Sumit Kumar Debnath[2] and Chinmoy Biswas[1]

[1] *Indian Institute of Technology Kharagpur, Kharagpur, 721302, India*

[2] *National Institute of Technology Jamshedpur, Jamshedpur, India*

Keywords: Identity Based Signature, Multivariate Cryptography, Isomorphism of Polynomial Problem, Signature of Knowledge, EUF-CMA Security.

Abstract: *Multivariate public key cryptosystem* (MPKC) is one of the promising candidates for *post-quantum cryptography* (PQC) as it features fast and efficient computation with security under the NP hardness of solving a system of *multivariate quadratic* (MQ) polynomial equations over a finite field. In the last two decades, there have been remarkable development in MPKC specially in signature and encryption scheme. In this work, we have developed a multivariate identity-based signature (MV-IBS) scheme employing a specialized version of non-interactive zero-knowledge proofs of knowledge (NIZK). Our construction is *existentially unforgeable against chosen message and chosen identity attack* (EUF-CMA) in the random oracle model (ROM) under the hardness of the *isomorphism of polynomials* (IP) problem. An IP problem tests the equivalence of two polynomial maps. It says that given access to two quadratic functions which are equal up to linear changes of coordinates, it is difficult to compute these changes of coordinates. We emphasize that unlike most of the MPKC, our scheme achieves provable security in an existing security framework. Additionally, the proposed IBS performs better over the existing works in terms of user's secret key size, master public key size and master secret key size.

1 INTRODUCTION

Multivariate Public Key Cryptograpy (MPKC). In the last few decades, *public key cryptography* (PKC) has become an inevitable part of our global communication infrastructure. Most of our important communication protocols utilize public key cryptosystems like RSA, Diffe-Hellman key exchange, digital signature algorithms and elliptic curve algorithms which rely on number theoretic assumptions like *integer factorization* and *discrete logarithm problem*. (Shor, 1999) came up with an algorithm which can break these number theoretic problems by quantum computer in polynomial time. Consequently, a sufficiently powerful quantum computer will put many forms of modern communication from key exchange to encryption to digital authentication in danger. *Post-quantum cryptography* (PQC) assures the cryptography community that secure communication is possible even in the presence of quantum computer. In literature, the five well studied PQC variants are lattice-based, multivariate-based, code-based, hash based and isogeny-based cryptography. A working group of the National Institute of Standards and Technologies (NIST) is exploring the standardization of PQC since 2013. In addition, a regular Quantum-Safe-Crypto Workshop is organized by the European Telecommunications Standards Institute (ETSI). Among the different PQC variants, *multivariate public key cryptography* (MPKC) catches the special attention to the researchers and have been seen to be alternative to the widely used PKC like RSA, digital signature, elliptic curve, etc. The main advantages of MPKC are significant speed and cost-effective computation, making it worthy for low-cost devices. In Eurocrypt 1988, (Matsumoto and Imai, 1988) introduced MPKC whose security is based on solving a set of multivariate quadratic equations over a finite field which is known to be NP hard problem. To solve a set of multivariate polynomial equations, quantum computers have not yet been efficient so far and are unlikely to provide any advantage against such a problem. In the last few years, there has been an enormous development of designing multivariate schemes (Kipnis et al., 1999; Ding and Schmidt, 2005; Patarin, 1997) in several directions. The MPKC schemes are compu-

Dutta, R., Debnath, S. and Biswas, C.
Storage Friendly Provably Secure Multivariate Identity-Based Signature from Isomorphism of Polynomials Problem.
DOI: 10.5220/0010580505950602
In *Proceedings of the 18th International Conference on Security and Cryptography (SECRYPT 2021)*, pages 595-602
ISBN: 978-989-758-524-1

tationally efficient than other PQC variants. However, they have large key sizes.

Identity Based Cryptography (IBC). IBC is an alternative framework of *public-key infrastructure* (PKI) which is simple and efficient. PKI is developed in order to map users' public keys to real life identities such as names, email addresses, etc. using certifying authority (CA). For example, CA may link public keys of users with real life identities using digital certificates. This linking procedure makes PKI inefficient and complicated. IBC provides a solution by eliminating the requirement of digital certificates. In 1984, the concept of IBC was introduced by (Shamir, 1984) where one can directly derive user's public key from its identity. In IBC, a trusted *private key generator* (PKG) utilizes a msk to derive users' secret keys and issues them to the corresponding users. Note that only the PKG has the knowledge of the msk. In the field of IBC, *identity based signature* (IBS) plays an important role for its widespread use in real life scenarios. For instance, in a company there are several departments and each department is having an authority to sign on behalf of the company in the documents related to that department only. One may use IBS to deal with this instance. In IBS, each user gets a signing key corresponding to his/her identity from a trusted authority via a confidential channel so that signed documents can be verified using the identity of the user. In the literature, there are several works on IBS. However, most of them are cryptosytems based on "number theoretic problem" (Rivest et al., 1978; Kravitz, 1993). Due to (Shor, 1999), these are vulnerable to quantum computer attacks. Consequently, researchers are looking for post-quantum IBS that may resist quantum computer attacks.

Related Works on IBS. The notion of IBS was proposed by (Shamir, 1984) for reducing the complexity of managing the PKI. After its introduction many variants of IBS with different security notions have been proposed (Barreto et al., 2005; Choon and Cheon, 2003; Debiao et al., 2011). These are all vulnerable to quantum attacks. To withstand against quantum attacks, various IBS (Xinyin, 2015; Ducas et al., 2014; Hung et al., 2017; Xie et al., 2020) schemes have been presented depending on the hard problems on lattices such as Gap-SVP and SIS problems.

In resisting quantum attacks, MPKC is another widely known post quantum variant where we rely on the hardness of MQ problem (Huang et al., 2012). The first IBS scheme in the area of multivariate cryptography, named IBUOV, relied on the UOV scheme of (Kipnis et al., 1999) was constructed in (Shen et al., 2013). They showed the forward security of the IBUOV depending on the security of the underlying UOV. However, the IBUOV does not attain $\mathsf{EUF\text{-}CMA}$ security as the underlying UOV protocol does not provide such security guarantee. Subsequently, (Luyen et al., 2019) built an IBS, which is $\mathsf{EUF\text{-}CMA}$ secure and is called IBS-Rainbow. Recently, a general construction of multivariate IBS was proposed by (Chen et al., 2019). Their scheme is compatible with any MPKC.

Our Contribution. MPKC attracts considerable attention to the NIST PQC standardization (Alagic et al., 2020) because of its high speed computation and decent computational resource requisite making it suitable for resource constrained devices like Radio Frequency Identifications (RFIDs) or smart cards. Moreover, most of the MPKC schemes in the literature claim their security either theoretically or experimentally and parameters are selected accordingly. This work concentrates on designing a secure and efficient multivariate IBS scheme with a concrete security analysis in the existing security models instead of using heuristic arguments. Integrating a specialized version of non-interactive zero-knowledge proofs of knowledge, called the *signature of knowledge*, we develop an identity-based multivariate signature scheme, namely $\mathsf{MV\text{-}IBS}$. The proposed scheme is existentially unforgeable against chosen message and chosen identity attack ($\mathsf{EUF\text{-}CMA}$) secure in the ROM under the difficulty of solving *isomorphism of polynomials* (IP) problem. At a high level, the proposed IBS involves four algorithms $\mathsf{Setup}, \mathsf{Extract}, \mathsf{Sign}, \mathsf{Verify}$. A PKG runs Setup on input 1^κ to generate the public parameters params and the master secret key msk. The algorithm $\mathsf{Extract}$ is extracted by the PKG for generating user's secret key $\mathsf{usk}_{\mathsf{id}}$ for the user with identity $\mathsf{id} \in \{0,1\}^*$. The user holding the secret key $\mathsf{usk}_{\mathsf{id}}$, invokes the algorithm Sign to generate a signature μ on a message u. Finally, the algorithm Verify is run by a verifier on input (params,u, id, μ) to check the validity of the message-signature pair (u,μ). Our scheme is storage efficient compared to the existing schemes (Chen et al., 2019; Shen et al., 2013).

We have proved the security of our IBS following an existing security framework. More preciously, we have the following theorem.

Theorem 1.1. *(Informal) Our multivariate IBS scheme* $\mathsf{MV\text{-}IBS} = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Sign}, \mathsf{Verify})$ *is*

$\mathsf{EUF\text{-}CMA}$ *secure under the hardness of IP problem in random oracle model.*

We summarize bellow our contributions in this paper

- The main technical difference of our approach from the existing approaches (Chen et al., 2019; Luyen et al., 2019; Shen et al., 2013) of designing multivariate IBS is that the signature of knowledge is the underlying primary primitive for our construction. The multivariate IBS of (Shen et al., 2013) uses UOV whereas that of (Luyen et al., 2019) uses Rainbow together with UOV. The general construction of (Chen et al., 2019) is compatible for any MPKC.
- Our scheme is provable secure unlike most of the existing MPKC schemes whose security are argued theoretically or experimentally and parameters are selected accordingly. More preciously, we achieve $\mathsf{EUF\text{-}CMA}$ security under the hardness of the IP problem which is known to be a problem harder than the Graph Isomorphism problem (which is NP hard). The multivariate IBS of (Shen et al., 2013) does not exhibit $\mathsf{EUF\text{-}CMA}$ security and has large key sizes. Although the multivariate IBS of (Luyen et al., 2019) achieves $\mathsf{EUF\text{-}CMA}$ security similar to our $\mathsf{MV\text{-}IBS}$, it has formidable huge key sizes. The work of (Chen et al., 2019) also features significantly large key sizes. In contrast, our approach helps to reduce the key sizes considerably although the signature size in our $\mathsf{MV\text{-}IBS}$ remains large.
- The multivariate IBS schemes (Chen et al., 2019; Luyen et al., 2019; Shen et al., 2013) derive their security from the hardness of MQ problem whereas our scheme relies on the hardness of IP problem.

Organization. The rest of the work is structured in the following way. Section 2 gives the necessary preliminaries. The proposed IBS is described in Section 3 followed by its security in Section 4 and efficiency analysis in Section 5. Finally, the work is concluded in Section 6 with possible future direction of work.

2 PRELIMINARIES

Notations. In this work, "$\mathbb{K}$ stands for Galois field $\mathsf{GF}(p)$ of prime order p" and "$\mathbb{K}^n = \{\mathbf{x} = (x_1, x_2, \dots, x_n) | x_i \in \mathbb{K}$ for $i = 1, 2, \dots, n\}$". Denote "$f \circ g$ as composition of two functions f and g". By "$A||B$, we mean concatenation of A and B". For a positive integer q, define "the set $[1, 2, \dots, q]$ as $[q]$". By "$[[B]]$, we denote the bit that is 1 if the boolean statement B is true and 0 otherwise". We say that "$f : \mathbb{N} \to \mathbb{R}$ is a negligible function of n if it is $O(n^{-c})$ for all $c > 0$" and we use "$\mathsf{negl}(n)$ to denote a negligible function of n".

Definition 2.1. Isomorphism of Polynomials (IP): *Let $A : \mathbb{K}^n \to \mathbb{K}^m$ and $B : \mathbb{K}^n \to \mathbb{K}^m$ be two sets of "m quadratic multivariate polynomials in n variables $x_1, x_2, \dots, x_n$":*
$A = (A_1(x_1, x_2, \dots, x_n), A_2(x_1, x_2, \dots, x_n), \dots, A_m(x_1, x_2, \dots, x_n))$
$B = (B_1(x_1, x_2, \dots, x_n), B_2(x_1, x_2, \dots, x_n), \dots, B_m(x_1, x_2, \dots, x_n))$ *where*

$$A_i(x_1, x_2, \dots, x_n) = \sum_{j=1}^{n}\sum_{k=1}^{n} \alpha^i_{jk} x_j x_k + \sum_{j=1}^{n} \beta^i_j x_j + \gamma_i$$

$$B_i(x_1, x_2, \dots, x_n) = \sum_{j=1}^{n}\sum_{k=1}^{n} \hat{\alpha}^i_{jk} x_j x_k + \sum_{j=1}^{n} \hat{\beta}^i_j x_j + \hat{\gamma}_i$$

for $i = 1, 2 \dots, n$ and α^i_{jk}, β^i_j, γ_i, $\hat{\alpha}^i_{jk}$, $\hat{\beta}^i_j$, $\hat{\gamma}_i$, $x_i \in \mathbb{K} = \mathsf{GF}(p)$. If we can find a pair of invertible affine transformations $S : \mathbb{K}^m \to \mathbb{K}^m$ and $T : \mathbb{K}^n \to \mathbb{K}^n$ satisfying $B = S \circ A \circ T$, then we say that A and B are isomorphic *and (S, T) is an* isomorphism *from A to B. Given isomorphic sets A and B of m quadratic multivariate polynomials in n variables over $\mathbb{K}$, the IP problem asks to find an isomorphism (S, T) from A to B.*

The IP problem is NP-hard (Yang et al., 2011).

Signature of Knowledge from IP (Yang et al., 2011). SoK is a specialized version of *non-interactive zero-knowledge proof* (NIZK). In a signature of knowledge (SoK), a signer (SG) wishes to assure a verifier (VK) about the fact that he is having secret signing key and the verifier intends to verify the correctness of the claim. The SG is able to prove the VK that the claim is correct without disclosing the secret. We define in Figure 1 the signature of knowledge SoK = (Setup, KeyGen, $\mathsf{SigKnowledge}$, $\mathsf{VerKnowledge}$) of (Yang et al., 2011) is a signature scheme that relies on the isomorphism of polynomials (IP) problem.

- **Correctness:** The scheme $\mathsf{SoK} = (\mathsf{Setup}, \mathsf{Key Gen}, \mathsf{SigKnowledge}, \mathsf{VerKnowledge})$ described in Figure 1 satisfies the following correctness requirement: For all κ, all $\mathsf{pp} \leftarrow \mathsf{Setup}(1^\kappa)$, all $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(\mathsf{pp})$, all $V \leftarrow \mathsf{SigKnowledge}(\mathsf{pp}, u, \mathsf{sk}, \mathsf{pk})$, all message $u \in \{0,1\}^*$, it holds that $\mathsf{VerKnowledge}(\mathsf{pp}, u, V, \mathsf{pk}) = 1$. Note that for all $i \in [q]$, $\overline{C}_i = S_i \circ A \circ T_i = S^{'}_i \circ A \circ T^{'}_i = C_i$ when $H[i] = 0$ and $\overline{C}_i = S_i \circ B \circ T_i = S^{'}_i \circ S^{-1} \circ B \circ T^{-1} \circ T^{'}_i = S^{'}_i \circ A \circ T^{'}_i = C_i$ when $H[i] = 1$. Consequently, $\mathcal{H}(u \,\|\, \overline{C}_1 \,\|\, \cdots \,\|\, \overline{C}_q) = H^{'} = H$ and hence $\mathsf{VerKnowledge}(\mathsf{pp}, u, V, \mathsf{pk}) = 1$.

$\mathsf{pp} \leftarrow \mathsf{SoK.Setup}(1^{ˇ})$ A trusted authority runs this algorithm on input $1^{ˇ}$ and generates the public parameter $\mathsf{pp} = (\mathcal{H}, \mathbb{K}, m, n)$ by choosing a cryptographically secure collision-resistant hash function $\mathcal{H}: \{0,1\}^* \rightarrow \{0,1\}^q$ where q, m, n are positive integers and $\mathbb{K} = \mathsf{GF}(p)$ for some prime p.

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{SoK.KeyGen}(\mathsf{pp})$. On input the public parameter $\mathsf{pp} = (\mathcal{H}, \mathbb{K}, m, n)$, a signer chooses a pair (A, B) of isomorphic sets of m quadratic multivariate polynomials in n variables with the isomorphism (S, T) over $\mathbb{K}$ satisfying $B = S \circ A \circ T$ as defined in Definition 2.1. Here $A : \mathbb{K}^n \rightarrow \mathbb{K}^m$, $B : \mathbb{K}^n \rightarrow \mathbb{K}^m$ and $S : \mathbb{K}^m \rightarrow \mathbb{K}^m$, $T : \mathbb{K}^n \rightarrow \mathbb{K}^n$ are two invertible affine transformation. It then sets the public key $\mathsf{pk} = (A, B)$ and the secret key $\mathsf{sk} = (S, T)$.

$V \leftarrow \mathsf{SoK.SigKnowledge}(\mathsf{pp}, u, \mathsf{sk}, \mathsf{pk})$. The signer, with the knowledge of the isomorphism $\mathsf{sk} = (S, T)$ between A and B where $\mathsf{pk} = (A, B)$, performs the following steps to generate a signature of knowledge for a message $u \in \{0,1\}^*$:

(i) Chooses randomly q invertible affine transformation pairs $(S_1', T_1'), (S_2', T_2'), \ldots, (S_q', T_q')$ where $T_i' : \mathbb{K}^n \rightarrow \mathbb{K}^n$, $S_i' : \mathbb{K}^m \rightarrow \mathbb{K}^m$ for $i \in [q]$.

(ii) Computes $C_i = S_i' \circ A \circ T_i'$ for $i \in [q]$ (*i.e.* C_i and A are isomorphic with the isomorphism (S_1', T_i')).

(iii) Evaluates $\mathcal{H}(u \parallel C_1 \parallel \cdots \parallel C_q) = H = H[q]H[q-1] \cdots H[1] \in \{0,1\}^q$ where $H[i] \in \{0,1\}$.

(iv) For $i \in [q]$, sets $(S_i, T_i) = \begin{cases} (S_i', T_i') & \text{if } H[i] = 0 \\ (S_i' \circ S^{-1}, T^{-1} \circ T_i') & \text{if } H[i] = 1. \end{cases}$

(v) Outputs $V = \{H, (S_1, T_1), \ldots, (S_q, T_q)\}$ as signature of knowledge.

$0/1 \leftarrow \mathsf{SoK.VerKnowledge}(\mathsf{pp}, u, V, \mathsf{pk})$. Given the public parameter pp, message $u \in \{0,1\}^*$, public key $\mathsf{pk} = (A, B)$ and signature of knowledge $V = \{H, (S_1, T_1), \ldots, (S_q, T_q)\}$, the verifier does the following:

(i) Parse $H \in \{0,1\}^q$ as $H = H[q]H[q-1] \cdots H[1]$ where $H[i] \in \{0,1\}$.

(ii) For $i \in [q]$, evaluates $\overline{C}_i = \begin{cases} S_i \circ A \circ T_i & \text{if } H[i] = 0 \\ S_i \circ B \circ T_i & \text{if } H[i] = 1 \end{cases}$

(iii) Computes $\mathcal{H}(u \parallel \overline{C}_1 \parallel \cdots \parallel \overline{C}_q) = H'$.

(iv) Outputs 1 if $H = H'$; otherwise 0.

Figure 1: Signature of Knowledge from IP.

2.1 Identity Based Signature (Paterson and Schuldt, 2006)

We recall the definition of (IBS) which is a tuple of algorithms IBS = (Setup, Extract, Sign, Verify) satisfying the following requirements:

$(\mathsf{params}, \mathsf{msk}) \leftarrow \mathsf{IBS.Setup}(1^\kappa)$. A trusted PKG runs this algorithm on input 1^κ and generates public parameter params and a master secret key msk.

$\mathsf{usk_{id}} \leftarrow \mathsf{IBS.Extract}(\mathsf{params}, \mathsf{id}, \mathsf{msk})$. The PKG generates user secret key $\mathsf{usk_{id}}$ for the user with identity $\mathsf{id} \in \{0,1\}^*$ using the master secret key msk and public parameter params.

$\mu \leftarrow \mathsf{IBS.Sign}(\mathsf{params}, u, \mathsf{usk_{id}})$. Given a message input u, the user with public parameter params and secret key $\mathsf{usk_{id}}$ runs this algorithm and output a signature μ on the message u.

$0/1 \leftarrow \mathsf{IBS.Verify}(\mathsf{params}, u, \mathsf{id}, \mu)$. On input params, message u, user identity id and a signature μ, a verifier returns 1 if the signature is valid, 0 otherwise.

- **Correctness:** The aforementioned IBS must attaining the following correctness requirement: For all κ, all $(\mathsf{params}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\kappa)$, all $\mathsf{usk_{id}} \leftarrow \mathsf{Extract}(\mathsf{params}, \mathsf{id}, \mathsf{msk})$, all message u, it holds that $\mathsf{Verify}(\mathsf{params}, \mathsf{id}, u, \mathsf{Sign}(\mathsf{params}, u, \mathsf{usk_{id}})) = 1$.
- **Security:** We define the EUF-CMA advantage function of a forger $\mathcal{F}$ against IBS as $\mathsf{ADV}_{\mathsf{IBS}}^{\mathsf{EUF\text{-}CMA}}(\mathcal{F}) = \Pr[\mathsf{EXP}_{\mathsf{IBS},\mathcal{F}}^{\mathsf{EUF\text{-}CMA}}(1^\kappa) = 1]$ where experiment $\mathsf{EXP}_{\mathsf{IBS},\mathcal{F}}^{\mathsf{EUF\text{-}CMA}}(1^\kappa)$ is described below. An IBS scheme is said to satisfy EUF-CMA security if, for all PPT forger $\mathcal{F}$, there exists a negligible function negl such that $\mathsf{ADV}_{\mathsf{IBS}}^{\mathsf{EUF\text{-}CMA}}(\mathcal{F}) = \Pr[\mathsf{EXP}_{\mathsf{IBS},\mathcal{F}}^{\mathsf{EUF\text{-}CMA}}(1^\kappa) = 1] < \mathsf{negl}(\kappa)$.

Definition 2.2. EUF-CMA **security:** *An IBS scheme is said to satisfy the existential unforgeability against chosen message and chosen identity attack (*EUF-CMA*) security if, for all probabilistic polynomial time (PPT) forger $\mathcal{F}$, there exists a negligible function* negl *such that* $\mathsf{ADV}_{\mathsf{IBS}}^{\mathsf{EUF\text{-}CMA}}(\mathcal{F}) = \Pr[\mathsf{EXP}_{\mathsf{IBS},\mathcal{F}}^{\mathsf{EUF\text{-}CMA}}(1^\kappa) = 1] < \mathsf{negl}(\kappa)$.

3 OUR PROTOCOL MV-IBS

We describe below the construction of our proposed multivariate IBS scheme MV-IBS = (Setup, Extract, Sign, Verify) that uses the signature of knowledge SoK = (Setup, KeyGen, SigKnowledge, VerKnowledge) described in Section 2 which is based on the IP problem.

$(\mathsf{params}, \mathsf{msk}) \leftarrow \mathsf{MV\text{-}IBS.Setup}(1^\kappa)$. The private key generator PKG does the following:

(i) Runs $\mathsf{SoK.Setup}(1^\kappa)$ (see Figure 1) to generate $\mathsf{pp} = (\mathcal{H}, \mathbb{K}, m, n)$ by choosing a cryptographically secure collision-resistant hash function $\mathcal{H}: \{0,1\}^* \rightarrow \{0,1\}^q$ where q, m, n are positive integers and $\mathbb{K} = \mathsf{GF}(p)$ for some prime p.

(ii) Generates $(\mathsf{pk}_R, \mathsf{sk}_R) \leftarrow \mathsf{SoK.KeyGen}(\mathsf{pp})$ (see Figure 1) where $\mathsf{sk}_R = (L_1, L_2)$ and $\mathsf{pk}_R =$

```
$\mathsf{EXP}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{IBS},\mathcal{F}}(1^\kappa)$
    $(\mathsf{params},\mathsf{msk}) \leftarrow \mathsf{Setup}(1^\kappa)$
    $(\mathsf{id}^*,u^*,\mu^*) \leftarrow \mathcal{F}^{\mathsf{EXTRACT},\mathsf{SIGN}}(\mathsf{pp})$
    return $[[(\mathsf{id}^*,u^*) \notin \mathsf{SList}]] \wedge [[\mathsf{id}^* \notin \mathsf{XList}]]$
        $\wedge [[\mathsf{Verify}(\mathsf{params},\mathsf{id}^*,u^*,\mu^*) = 1]]$

Oracle $\mathsf{EXTRACT}(\mathsf{id})$
    $\mathsf{usk_{id}} \leftarrow \mathsf{Extract}(\mathsf{params},\mathsf{id},\mathsf{msk})$
    $\mathsf{SList} = \mathsf{SList} \cup \{\mathsf{id}\}$
    return $\mathsf{usk_{id}}$

Oracle $\mathsf{SIGN}(\mathsf{id},u)$
    $\mathsf{SList} = \mathsf{SList} \cup \{\mathsf{id},u\}$
    $\mathsf{usk_{id}} \leftarrow \mathsf{Extract}(\mathsf{params},\mathsf{id},\mathsf{msk})$
    $\mathsf{XList} = \mathsf{XList} \cup \{\mathsf{id}\}$
    $\mu \leftarrow \mathsf{Sign}(\mathsf{params},u,\mathsf{usk_{id}})$
    return $\mu$
```

Figure 2: EUF-CMA security game with EXTRACT and SIGN oracle.

(P,Q). Here (P,Q) is a pair of isomorphic sets of m quadratic multivariate polynomials in n variables with the isomorphism (L_1,L_2) over the fields $\mathbb{K}$ satisfying $Q = L_1 \circ P \circ L_2$ as in Definition 2.1 and $L_1 : \mathbb{K}^m \to \mathbb{K}^m$, $L_2 : \mathbb{K}^n \to \mathbb{K}^n$ are two invertible affine transformations, $P : \mathbb{K}^n \to \mathbb{K}^m$ and $Q : \mathbb{K}^n \to \mathbb{K}^m$.

(iii) Picks $k \in \{0,1\}^q$ at random, a cryptographically secure collision-resistant hash function $\widehat{\mathcal{H}} : \{0,1\}^* \to \mathbb{K}^d$ and sets $\mathsf{MAC}_k(\mathbf{y}) = \widehat{\mathcal{H}}(k||\mathbf{y})$ for $\mathbf{y} \in \{0,1\}^*$

(iv) Selects invertible affine map X as follows where $\mathbf{z} = (z_1,z_2,\ldots,z_d) \in \mathbb{K}^d$:

$$\begin{aligned} X &= X(x_1,x_2,\ldots,x_m;\mathbf{z}) \\ &= (X_1(x_1,x_2,\ldots,x_m;\mathbf{z}),\ldots,X_m(x_1,x_2,\ldots,x_m;\mathbf{z})) \end{aligned}$$

with

$$X_i(x_1,x_2\ldots,x_m;\mathbf{z}) = \sum_{j=1}^{m} X_{i,j}(\mathbf{z})x_j + X_{i,0}(\mathbf{z})$$

for $i \in [m]$ where each $X_{i,j}(\mathbf{z})$ is a linear function of $\mathbf{z} = (z_1,z_2,\ldots,z_d) \in \mathbb{K}^d$ and $x_1,x_2,\ldots,x_m \in \mathbb{K}$. Thus X is a function of $m+d$ variables $x_1,x_2,\ldots,x_m,z_1,z_2,\ldots,z_d$ over $\mathbb{K}$.

(v) Chooses invertible affine map Y as follows where $\mathbf{z} = (z_1,z_2,\ldots,z_d) \in \mathbb{K}^d$:

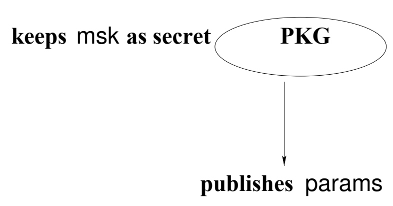
$$\begin{aligned} Y &= Y(x_1,x_2\ldots,x_n;\mathbf{z}) \\ &= (Y_1(x_1,x_2,\ldots,x_n;\mathbf{z}),\ldots,Y_n(x_1,x_2,\ldots,x_n;\mathbf{z})) \end{aligned}$$

with

$$Y_i(x_1,x_2,\ldots,x_n;\mathbf{z}) = \sum_{j=1}^{n} Y_{i,j}(\mathbf{z})x_j + Y_{i,0}(\mathbf{z})$$

for $i \in [n]$ where each $Y_{i,j}(\mathbf{z})$ is a linear function of $\mathbf{z} = (z_1,z_2,\ldots,z_d) \in \mathbb{K}^d$ and $x_1,x_2,\ldots,x_n \in \mathbb{K}$. Thus Y is a function of $n+d$ variables $x_1,x_2,\ldots,x_n,z_2,z_2,\ldots,z_d$ over $\mathbb{K}$.

(vi) Sets public parameter as $\mathsf{params} = (\mathsf{pp} = (\mathcal{H},\mathbb{K},m,n),\mathsf{pk}_R = (P,Q),\widehat{\mathcal{H}})$ and master secret key as $\mathsf{msk} = (\mathsf{sk}_R = (L_1,L_2),k,X,Y)$(see Figure 3).



$\mathsf{pp} = (\mathcal{H},\mathbb{K},m,n)$

$\mathsf{pk}_R = (P,Q)$, $\mathsf{sk}_R = (L_1,L_2)$

$Q = L_1 \circ P \circ L_2$, X, Y, k, $\widehat{\mathcal{H}}$

$\mathsf{msk} = (\mathsf{sk}_R = (L_1,L_2),k,X,Y)$

$\mathsf{params} = (\mathsf{pp} = (\mathcal{H},\mathbb{K},m,n),\mathsf{pk}_R = (P,Q),\widehat{\mathcal{H}})$

Figure 3: The algorithm MV-IBS.Setup(1ˇ).

$\mathsf{usk_{id}} \leftarrow \mathsf{MV\text{-}IBS.Extract}(\mathsf{params},\mathsf{id},\mathsf{msk})$. Given the identity $\mathsf{id} \in \{0,1\}^*$ of a user U_{id}, the PKG works as follows using $\mathsf{msk} = (\mathsf{sk}_R = (L_1,L_2),k,X,Y)$ and $\mathsf{params} = (\mathsf{pp} = (\mathcal{H},\mathbb{K},m,n),\mathsf{pk}_R = (P,Q),\widehat{\mathcal{H}})$:

(i) Computes

$$\begin{aligned} \mathsf{seed_{id}} &= \mathsf{MAC}_k(\mathsf{id}) = \widehat{\mathcal{H}}(k||\mathsf{id}) \in \mathbb{K}^d \\ \mathsf{sk_{id}} &= (X_{\mathsf{id}},Y_{\mathsf{id}}) \end{aligned}$$

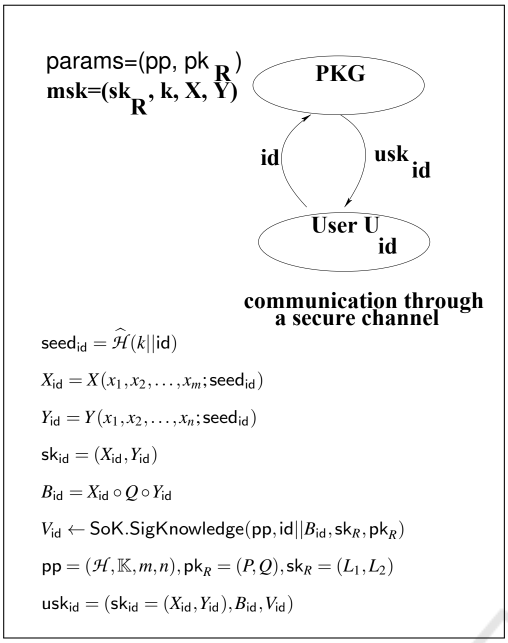
where

$$\begin{aligned} X_{\mathsf{id}} &= X(x_1,x_2,\ldots,x_m;\mathsf{seed_{id}}) \\ &= (X_1(x_1,\ldots,x_m;\mathsf{seed_{id}}),\ldots, \\ &\qquad X_m(x_1,\ldots,x_m;\mathsf{seed_{id}})) \end{aligned}$$

with

$$\begin{aligned} &X_i(x_1,x_2,\ldots,x_m;\mathsf{seed_{id}}) \\ &= \sum_{j=1}^{m} X_{i,j}(\mathsf{seed_{id}})x_j + X_{i,0}(\mathsf{seed_{id}}) \text{ for } i \in [m] \end{aligned}$$

and $Y_{\mathsf{id}} = Y(x_1,x_2,\ldots,x_n;\mathsf{seed_{id}}) = (Y_1(x_1,x_2,\ldots,x_n;\mathsf{seed_{id}}),\ldots,Y_n(x_1,x_2,\ldots,x_n;\mathsf{seed_{id}}))$ with $Y_i(x_1,x_2,\ldots,x_n;\mathbf{z} = \mathsf{seed_{id}}) = \sum_{j=1}^{n} Y_{i,j}(\mathsf{seed_{id}})x_j + Y_{i,0}(\mathsf{seed_{id}})$ for $i \in [n]$.



$\mathsf{seed}_{\mathsf{id}} = \widehat{\mathcal{H}}(k||\mathsf{id})$

$X_{\mathsf{id}} = X(x_1, x_2, \ldots, x_m; \mathsf{seed}_{\mathsf{id}})$

$Y_{\mathsf{id}} = Y(x_1, x_2, \ldots, x_n; \mathsf{seed}_{\mathsf{id}})$

$\mathsf{sk}_{\mathsf{id}} = (X_{\mathsf{id}}, Y_{\mathsf{id}})$

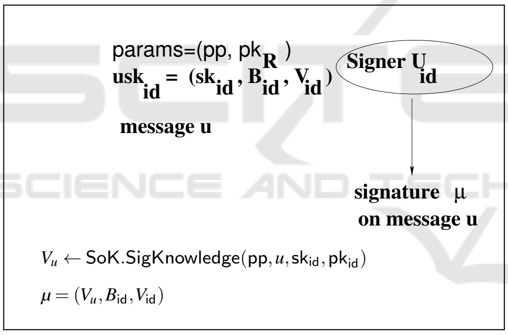
$B_{\mathsf{id}} = X_{\mathsf{id}} \circ Q \circ Y_{\mathsf{id}}$

$V_{\mathsf{id}} \leftarrow \mathsf{SoK.SigKnowledge}(\mathsf{pp}, \mathsf{id}||B_{\mathsf{id}}, \mathsf{sk}_R, \mathsf{pk}_R)$

$\mathsf{pp} = (\mathcal{H}, \mathbb{K}, m, n), \mathsf{pk}_R = (P, Q), \mathsf{sk}_R = (L_1, L_2)$

$\mathsf{usk}_{\mathsf{id}} = (\mathsf{sk}_{\mathsf{id}} = (X_{\mathsf{id}}, Y_{\mathsf{id}}), B_{\mathsf{id}}, V_{\mathsf{id}})$

Figure 4: The algorithm $\mathsf{MV\text{-}IBS.Extract}$ $(\mathsf{params}, \mathsf{id}, \mathsf{msk})$.



$V_u \leftarrow \mathsf{SoK.SigKnowledge}(\mathsf{pp}, u, \mathsf{sk}_{\mathsf{id}}, \mathsf{pk}_{\mathsf{id}})$

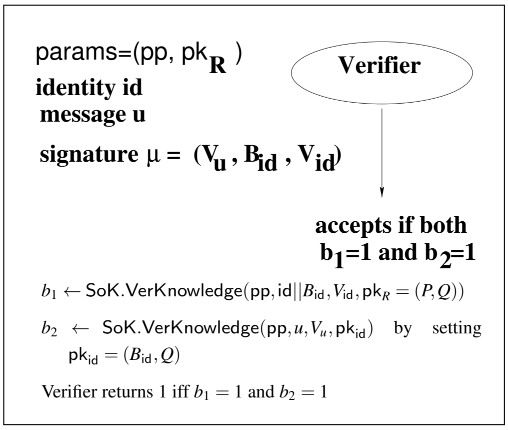
$\mu = (V_u, B_{\mathsf{id}}, V_{\mathsf{id}})$

Figure 5: The algorithm $\mathsf{MV\text{-}IBS.Sign}$ $(\mathsf{params}, u, \mathsf{usk}_{\mathsf{id}})$.

Here X, Y are obtained from msk where X is a function of $m+d$ variables $x_1, x_2, \ldots, x_m, z_1, z_2, \ldots, z_d$ and Y is a function of $n+d$ variables $x_1, x_2, \ldots, x_n, z_1, z_2, \ldots, z_d$. The PKG calculates X_{id} and Y_{id} by evaluating X and Y respectively at $\mathbf{z} = \mathsf{seed}_{\mathsf{id}} = \mathsf{MAC}_k(\mathsf{id}) = \widehat{\mathcal{H}}(k||\mathsf{id}) \in \mathbb{K}^d$ extracting k from msk and $\widehat{\mathcal{H}}$ from params.

(ii) Evaluates $B_{\mathsf{id}} = X_{\mathsf{id}} \circ Q \circ Y_{\mathsf{id}}$ where Q is obtained from params and sets $\mathsf{sk}_{\mathsf{id}} = (X_{\mathsf{id}}, Y_{\mathsf{id}})$. Note that B_{id} and Q are isomorphic sets of multivariate quadratic polynomials with the isomorphism $(X_{\mathsf{id}}, Y_{\mathsf{id}})$.

(iii) Generates $V_{\mathsf{id}} \leftarrow \mathsf{SoK.SigKnowledge}(\mathsf{pp} = (\mathcal{H}, \mathbb{K}, m, n), \mathsf{id}||B_{\mathsf{id}}, \mathsf{sk}_R = (L_1, L_2), \mathsf{pk}_R = (P, Q))$


params=(pp, pk R)
identity id
message u
signature μ = (V u , B id , V id)
Verifier
accepts if both b 1 =1 and b 2 =1

$b_1 \leftarrow \mathsf{SoK.VerKnowledge}(\mathsf{pp}, \mathsf{id}||B_{\mathsf{id}}, V_{\mathsf{id}}, \mathsf{pk}_R = (P, Q))$

$b_2 \leftarrow \mathsf{SoK.VerKnowledge}(\mathsf{pp}, u, V_u, \mathsf{pk}_{\mathsf{id}})$ by setting $\mathsf{pk}_{\mathsf{id}} = (B_{\mathsf{id}}, Q)$

Verifier returns 1 iff $b_1 = 1$ and $b_2 = 1$

Figure 6: The algorithm $\mathsf{MV\text{-}IBS.Verify}$ $(\mathsf{params}, u, \mathsf{id}, \mu)$.

(iv) Sends $\mathsf{usk}_{\mathsf{id}} = (\mathsf{sk}_{\mathsf{id}} = (X_{\mathsf{id}}, Y_{\mathsf{id}}), B_{\mathsf{id}}, V_{\mathsf{id}})$ to the user U_{id} (see Figure 4).

$\mu \leftarrow \mathsf{MV\text{-}IBS.Sign}(\mathsf{params}, u, \mathsf{usk}_{\mathsf{id}})$. Given a message $u \in \{0,1\}^*$, the user U_{id} with its secret key $\mathsf{usk}_{\mathsf{id}} = (\mathsf{sk}_{\mathsf{id}} = (X_{\mathsf{id}}, Y_{\mathsf{id}}), B_{\mathsf{id}}, V_{\mathsf{id}})$ computes the signature of knowledge $V_u \leftarrow \mathsf{SoK.SigKnowledge}(\mathsf{pp}, u, \mathsf{sk}_{\mathsf{id}}, \mathsf{pk}_{\mathsf{id}})$ (see Figure 1) using (B_{id}, Q) as $\mathsf{pk}_{\mathsf{id}}$ which is a pair of isomorphic sets of m quadratic multivariate polynomials in n variables with the isomorphism $\mathsf{sk}_{\mathsf{id}} = (X_{\mathsf{id}}, Y_{\mathsf{id}})$ over $\mathbb{K}$ satisfying $B_{\mathsf{id}} = X_{\mathsf{id}} \circ Q \circ Y_{\mathsf{id}}$. Here pp and Q are extracted from $\mathsf{params} = (\mathsf{pp} = (\mathcal{H}, \mathbb{K}, m, n), \mathsf{pk}_R = (P, Q), \widehat{\mathcal{H}})$. The user U_{id} outputs the signature of the message u as $\mu = (V_u, B_{\mathsf{id}}, V_{\mathsf{id}})$ (see Figure 5).

$0/1 \leftarrow \mathsf{MV\text{-}IBS.Verify}(\mathsf{params}, u, \mathsf{id}, \mu)$. Given a message $u \in \{0,1\}^*$, signature $\mu = (V_u, B_{id}, V_{\mathsf{id}})$, public parameter $\mathsf{params} = (\mathsf{pp} = (\mathcal{H}, \mathbb{K}, m, n), \mathsf{pk}_R = (P, Q), \widehat{\mathcal{H}})$ and an identity id, the verifier first runs $\mathsf{SoK.VerKnowledge}(\mathsf{pp}, \mathsf{id}||B_{\mathsf{id}}, V_{\mathsf{id}}, \mathsf{pk}_R = (P, Q))$. If the output is 1 then the verifier runs $\mathsf{SoK.VerKnowledge}(\mathsf{pp}, u, V_u, \mathsf{pk}_{\mathsf{id}})$ (see Figure 1) by setting $\mathsf{pk}_{\mathsf{id}} = (B_{\mathsf{id}}, Q)$ and checks whether the output is 1. If it is so then the verifier accepts the message signature pair and outputs 1. On the other hand, if output of $\mathsf{SoK.VerKnowledge}$ is 0 for either of the inputs $(\mathsf{pp}, \mathsf{id}||B_{\mathsf{id}}, V_{\mathsf{id}}, \mathsf{pk}_R = (P, Q))$ and $(\mathsf{pp}, u, V_u, \mathsf{pk}_{\mathsf{id}} = (B_{\mathsf{id}}, Q))$ then the verifier rejects the message-signature pair and outputs 0 (see Figure 6).

- **Correctness:** The correctness of our scheme MV-IBS follows from the following argument: Let $(\mathsf{params}, \mathsf{msk}) \leftarrow \mathsf{MV\text{-}IBS.Setup}(1^\kappa)$, $\mathsf{usk}_{\mathsf{id}} \leftarrow \mathsf{MV\text{-}IBS.Extract}(\mathsf{params}, \mathsf{id}, \mathsf{msk})$,

Table 1: Comparison summary of multivariate IBS.

	Our MV-IBS	IBS of (Chen et al., 2019)	IBS-Rainbow of (Luyen et al., 2019)	IBUOV of (Shen et al., 2013)
$\lvert\mathsf{msk}\rvert$	n^2+m^2+m+n	$m\cdot((\frac{n(n+1)(n+2)}{2})\cdot d)+m^2$ $+n^2+m\cdot(m+1)\cdot d$ $+n\cdot(n+1)\cdot d$	$m\cdot(m+1)+n\cdot(n+1)+$ $o_1\cdot(\frac{(v_1)(v_1+1)}{2}$ $+v_1\cdot o_1+v_1+o_1+1)$ $+o_2\cdot(\frac{(v_1+o_1)(v_1+o_1+1)}{2}$ $+(v_1+o_1)\cdot o_2+n+1)$	$n^2+m\binom{n+2}{2}$
$\lvert\mathsf{pk}_R\rvert$	$m\cdot\binom{n+2}{2}$	$m\cdot(n\cdot(\frac{d(d+1)(d+2)}{3!})$ $+(\frac{d(d+1)}{2})+(\frac{n(n+1)}{2})\cdot$ $(\frac{d(d+1)(d+2)(d+3)}{4!}))$	$m\cdot(\frac{(n+1)(n+2)}{2})$	$m\binom{n+2}{2}$
$\lvert\mathsf{usk}\rvert$	n^2+m^2+m+n	$n^2+m^2+m+n+m\cdot\binom{n+2}{2}$	$m\cdot(\frac{(n+1)(n+2)}{2})+n+2l$ $+m\cdot(m+1)+n\cdot(n+1)+$ $o_1\cdot(\frac{(v_1)(v_1+1)}{2}+v_1\cdot o_1+v_1+o_1+1)+$ $o_2\cdot(\frac{(v_1+o_1)(v_1+o_1+1)}{2}$ $+(v_1+o_1)\cdot o_2+n+1)$	$n^2+n+2m\binom{n+2}{2}$
$\lvert\mathsf{sig}\rvert$	$2(n^2+m^2)q+m\binom{n+2}{2}+\delta$	m	$2m+m\binom{n+2}{2}+\eta$	$2n+m\binom{n+2}{2}$

$n=v_1+o_1+o_2$, $m=o_1+o_2$, $\delta=2q/\log p$, $\eta=l/\log p$, q and l are security parameters, d indicates the size of user's ID, v_1 is the number of vinegar variables and $o=o_1+o_2$ is the number of oil variables in a 2-layer UOV scheme.

$\mu \leftarrow \mathsf{MV\text{-}IBS.Sign}(\mathsf{params},u,\mathsf{usk_{id}})$ where

$$\mathsf{params}=(\mathsf{pp}=(\mathcal{H},\mathbb{K},m,n),\mathsf{pk}_R=(P,Q),\widehat{\mathcal{H}}),$$
$$\mathsf{msk}=(\mathsf{sk}_R=(L_1,L_2),k,X,Y),$$
$$\mathsf{usk_{id}}=(\mathsf{sk_{id}}=(X_{\mathsf{id}},Y_{\mathsf{id}}),B_{\mathsf{id}},V_{\mathsf{id}})),$$
$$\mu=(V_u,B_{\mathsf{id}},V_{\mathsf{id}})).$$

Note that $\mathsf{pk}_R=(P,Q)$ is a pair of isomorphic sets with isomorphism $\mathsf{sk}_R=(L_1,L_2)$ as $Q=L_1\circ P\circ L_2$. Consequently, if $V_{\mathsf{id}} \leftarrow \mathsf{SoK.SigKnowledge}(\mathsf{pp},\mathsf{id}||B_{\mathsf{id}},\mathsf{sk}_R,\mathsf{pk}_R)$ then by the correctness of SoK, we have $\mathsf{SoK.VerKnowledge}(\mathsf{pp},\mathsf{id}||B_{\mathsf{id}},V_{\mathsf{id}},\mathsf{pk}_R)=1$. Also $\mathsf{pk_{id}}=(B_{\mathsf{id}},Q)$ is a pair of isomorphic sets with isomorphism $\mathsf{sk_{id}}=(X_{\mathsf{id}},Y_{\mathsf{id}})$ as $B_{\mathsf{id}}=X_{\mathsf{id}}\circ Q\circ Y_{\mathsf{id}}$. Hence, if $V_u \leftarrow \mathsf{SoK.SigKnowledge}(\mathsf{pp},u,\mathsf{sk_{id}},\mathsf{pk_{id}}=(B_{\mathsf{id}},Q))$ then $\mathsf{SoK.VerKnowledge}(\mathsf{pp},u,V_u,\mathsf{pk_{id}}=(B_{\mathsf{id}},Q))=1$ by the correctness of SoK. Consequently, $\mathsf{MV\text{-}IBS.Verify}(\mathsf{params},u,\mathsf{id},\mu)=1$.

4 SECURITY ANALYSIS

Theorem 4.1. *If the IP problem is hard then the* MV-IBS *described above is* EUF-CMA *secure as defined in Definition 2.2 when the hash function $\mathcal{H}$ is designed as a random oracle.*

Proof: Due to page limit, the full proof will be appeared in the full version of this paper.

5 EFFICIENCY ANALYSIS

In the literature of MPKC, several practical encryption and signature schemes can be found like MI (Matsumoto and Imai, 1988), HFE (Patarin, 1996), UOV (Kipnis et al., 1999), Rainbow (Ding and Schmidt, 2005), etc. Although, there are several IBS schemes (Zhang et al., 2019; Rückert, 2010; Xie et al., 2020; Wang et al., 2017) based on other candidates of PQC, there are only a few multivariate IBS schemes. (Shen et al., 2013) designed the first IBS, namely IBUOV, employing standard UOV (Kipnis et al., 1999) as a building block. Later, (Luyen et al., 2019) used the technique of (Sakumoto et al., 2011) to develop IBS-Rainbow a multivariate IBS by modifying UOV and Rainbow (Ding and Schmidt, 2005). Recently, (Chen et al., 2019) proposed a general construction of multivariate IBS which is compatible with any MPKC. On the other hand, we use signature of knowledge as the underlying primitive in our MV-IBS design.

We refer Table 1 for a comparison summary of our IBS with the existing multivariate IBS schemes (Chen et al., 2019; Luyen et al., 2019; Shen et al., 2013). All the schemes use finite field $\mathbb{K}=\mathsf{GF}(p)$ and the sizes are compared by counting the number of field elements. As explain in Table 1 our IBS scheme has smaller master secret key size ($\lvert\mathsf{msk}\rvert$), master public key size ($\lvert\mathsf{pk}_R\rvert$) and user's private key size ($\lvert\mathsf{usk}\rvert$). However, the size of the signature remains large. The IBUOV of (Shen et al., 2013) is not EUF-CMA secure in contrast to IBUOV our MV-IBS.

6 CONCLUSION

This paper presented a provably secure multivariate identity based signature (IBS) utilizing the *signature of knowledge* as the underlying primitive which is a variant of non-interactive zero knowledge proof. Our proposed IBS performs significantly better over the existing MPKC based IBS in terms of master secret key size, master public key size and user secret key size with a trade-off in signature size. Moreover, our scheme does not claim it security theoretically or experimentally as opposed to most of the MPKC schemes in the literature. Rather, it achieves EUF-CMA security in the random oracle model under the hardness of the IP problem which is known to be harder than Graph Isomorphism problem. Extending our work to achieve security in the standard model and reducing the signature size while retaining similar key sizes is an interesting open problem and our future direction of work.

REFERENCES

Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., et al. (2020). Status report on the second round of the nist post-quantum cryptography standardization process. *US Department of Commerce, NIST*.

Barreto, P. S., Libert, B., McCullagh, N., and Quisquater, J.-J. (2005). Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In *International conference on the theory and application of cryptology and information security*, pages 515–532. Springer.

Chen, J., Ling, J., Ning, J., and Ding, J. (2019). Identity-based signature schemes for multivariate public key cryptosystems. *The Computer Journal*, 62(8):1132–1147.

Choon, J. C. and Cheon, J. H. (2003). An identity-based signature from gap diffie-hellman groups. In *International workshop on public key cryptography*, pages 18–30. Springer.

Debiao, H., Jianhua, C., and Jin, H. (2011). An id-based proxy signature schemes without bilinear pairings. *Annals of telecommunications-annales des télécommunications*, 66(11-12):657–662.

Ding, J. and Schmidt, D. (2005). Rainbow, a new multivariable polynomial signature scheme. In *International Conference on Applied Cryptography and Network Security*, pages 164–175. Springer.

Ducas, L., Lyubashevsky, V., and Prest, T. (2014). Efficient identity-based encryption over ntru lattices. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 22–41. Springer.

Huang, Y.-J., Liu, F.-H., and Yang, B.-Y. (2012). Public-key cryptography from new multivariate quadratic assumptions. In *International Workshop on Public Key Cryptography*, pages 190–205. Springer.

Hung, Y.-H., Tseng, Y.-M., and Huang, S.-S. (2017). Revocable id-based signature with short size over lattices. *Security and Communication Networks*, 2017.

Kipnis, A., Patarin, J., and Goubin, L. (1999). Unbalanced oil and vinegar signature schemes. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 206–222. Springer.

Kravitz, D. W. (1993). Digital signature algorithm. US Patent 5,231,668.

Luyen, L. V. et al. (2019). An improved identity-based multivariate signature scheme based on rainbow. *Cryptography*, 3(1):8.

Matsumoto, T. and Imai, H. (1988). Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 419–453. Springer.

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*, pages 33–48. Springer.

Patarin, J. (1997). The oil and vinegar signature scheme. In *Dagstuhl Workshop on Cryptography September, 1997*.

Paterson, K. G. and Schuldt, J. C. (2006). Efficient identity-based signatures secure in the standard model. In *Australasian Conference on Information Security and Privacy*, pages 207–222. Springer.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126.

Rückert, M. (2010). Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles. In *International Workshop on Post-Quantum Cryptography*, pages 182–200. Springer.

Sakumoto, K., Shirai, T., and Hiwatari, H. (2011). On provable security of uov and hfe signature schemes against chosen-message attack. In *International Workshop on Post-Quantum Cryptography*, pages 68–82. Springer.

Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In *Workshop on the theory and application of cryptographic techniques*, pages 47–53. Springer.

Shen, W., Tang, S., and Xu, L. (2013). Ibuov, a provably secure identity-based uov signature scheme. In *2013 IEEE 16th International Conference on Computational Science and Engineering*, pages 388–395. IEEE.

Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332.

Wang, Z., Chen, X., and Wang, P. (2017). Adaptive-id secure identity-based signature scheme from lattices in the standard model. *IEEE Access*, 5:20791–20799.

Xie, C., Weng, J., Weng, J., and Hou, L. (2020). Scalable revocable identity-based signature over lattices in the standard model. *Information Sciences*, 518:29–38.

Xinyin, X. (2015). Adaptive secure revocable identity-based signature scheme over lattices. *Computer Engineering*, 10:25.

Yang, G., Tang, S., and Yang, L. (2011). A novel group signature scheme based on mpkc. In *International Conference on Information Security Practice and Experience*, pages 181–195. Springer.

Zhang, Y., Hu, Y., Gan, Y., Yin, Y., and Jia, H. (2019). Efficient fuzzy identity-based signature from lattices for identities in a small (or large) universe. *Journal of Information Security and Applications*, 47:86–93.