MQIBS: An Efficient Post-Quantum Identity-based Signature from Multivariate Polynomials

Le Van Luyen[1,2]
[1]Faculty of Mathematics and Computer Science, University of Science, Ho Chi Minh City, Vietnam
[2]Vietnam National University, Ho Chi Minh City, Vietnam
E-mail: lvluyen@hcmus.edu.vn

Keywords: Identity-based signatures, multivariate polynomials, MQ problem

Received: September 5, 2024

Identity-based signature (IBS) is an important cryptographic primitive which allows authentication of a party's public key without the need for certificates. In this paper, we construct a post-quantum provable identity-based signature scheme from multivariate polynomials. Our scheme is constructed from the sigma protocols with helper by Beullens at Eurocrypt 2020 and the Fiat-Shamir paradigm. Concrete choice of parameters shows that our scheme is more efficient than existing multivariate IBS schemes in terms of public key/signature sizes.

Povzetek: Predstavljena je postkvantna identitetna podpisna shema MQIBS, zasnovano na multivariatnih polinomih. Z uporabo sigma protokolov in Fiat-Shamirjevega pristopa izboljšuje varnost in učinkovitost, potrjuje manjše velikosti javnih ključev in podpisov, kar prispeva k večji praktičnosti v postkvantni kriptografiji.

1 Introduction

Post-quantum Cryptography (PQC) has become an emerging research direction since the announcement of NIST (National Institute of Standards and Technology) for the PQC standardization process since 2016 [1]. NIST selected several candidates for standardization in 2022 and called for additional digital signatures whose the first round deadline was June 2023 [2]. Among the candidates for PQC, multivariate cryptography is one of the main candidates for this standardization [1, 2]. It is shown in [11, 12] that multivariate schemes are very fast in general and suitable for limited computational resources, such as smart cards that run RFID chips. The security of multivariate schemes is normally based on the hardness of the *MQ-Problem*, which is proven to be NP-Hard $\mathbb{F}_2$ [3], that asks for a solution of a given system of multivariate quadratic polynomials over the field $\mathbb{F}_q$.

Multivariate cryptography is dated back to the early work of Matsumoto and Imai in 1988 [6], and since then, there has been a rich development of designing multivariate schemes in several directions. Notably in the history is the (Unbalanced) Oil and Vinegar (UOV) signature scheme by Patarin et al. after he broke the Matsumoto-Imai scheme [7, 8]. Since then, there has been the main direction on improving the UOV schemes, including the multilayer variant Rainbow by Ding and Schmidt [10], and its cyclic version [14]. Rainbow was one of the main candidates in the NIST PQC Process until Round 3, but it was not selected due to the attack by Beullens [30] which reduced the proposed security levels, i.e., in order to achieve the required level of security, Rainbow needs to update the parameters which will result in large key and signature sizes. Since then, the intention focuses back to improving the UOV scheme. Especially there have been many such submissions in the round 1 of NIST Additional PQC Signatures [2] including for example MAYO, PROV, QR-UOV and TUOV; see [2] for the details.

One drawback of UOV signatures is that they do not have a provable security proof. Recent submissions like MAYO or PROV do have such a proof but it was reduced to a new assumption, not the NP-complete MQ problem as expected. For a provable secure construction, another direction of construction multivariate signatures is to follow the Fiat-Shamir paradigm [5]. In this case, one needs first an identification scheme and the Fiat-Shamir transformation converts it into a secure digital signature. The first multivariate identification schemes were proposed by Sakumoto et al. [17]. They include a 3-pass and 5-pass identification schemes. The 5-pass identification was used to design the MQDSS signature [20, 19] which was a candidate for NIST PQC Round 2. However, it was broken by Kales and Zaverucha [27]. All work in this direction is hence focusing on improving one from 3-pass identification scheme by Sakumoto et al. [17], including [25]. Recently, Beullens [26, 26] developed sigma protocols with helper, inspiring from the work by Katz et al. [21], and applied to the 3-pass identification scheme by Sakumoto et al. [17] to obtain a more efficient multivariate digital signature compared to MQDSS [20].

Identity-Based Signature (IBS), proposed by Shamir [4], allows for the generation of a public key for an entity using only some basic scheme parameters and an identifier string (such as an email address or phone number). A private key generator (PKG) derives private keys from a master secret and distributes them to the entities involved in the scheme. This approach removes the requirement for certificates, unlike in traditional public key infrastructure. There have been many post-quantum constructions of IBS. In the area of multivariate cryptography, there have been several proposals for IBS based on UOV such as [18, 24] or Rainbow such as [23, 24]. Recently, there has been a proposal for identity-based signature by Debnath et al. [31].

In this paper, we investigate the sigma protocol with helper by Beullens and design an identity-based signature scheme from multivariate polynomials, which we call MQIBS. Our MQIBS scheme enjoys the security reduction to the underlying MQ problem and is more efficient than existing schemes; see Table 2 for the details.

Related work There are basically two approaches to construct an IBS. One is called the certification approach [13], transforms a standard signature scheme into an IBS scheme, from which this paper follows. The other one [9] is to transform a 2-level hierarchical identity-based encryption (HIBE) scheme to an IBS scheme. For post-quantum identity-based signatures, there exist several constructions. The most dominant candidates come from lattice-based constructions ([15, 28, 32]) which follow the second approach, since there exist trapdoors in lattices which enable efficient HIBE constructions ([16]). The remaining post-quantum identity-based signature candidates follow the first approach. Isogeny-based [33, 29] and group actions-based [34] constructions follow a variant [22] of the first approach to achieve schemes with tight reduction; however, due to the less flexibility of group actions, the constructions require a lot of “layers” which may result in in-efficient schemes compared to the efficient digital counterparts. In multivariate cryptography, there have been several constructions based on Rainbow such as [23, 24, 31]. In this paper, we propose a new one which is more efficient than the aforementioned schemes.

The rest of the paper is organized as the following. In Section 2, we recall some basic notions on commitment schemes and identity-based signatures including their definition and security model. We recall the sigma protocols with helper from Beullens [30] in Section 3 and our construction of MQIBS is presented in Section 4. In Section 5, we provide the choice of parameters and compute the key and signature size of MQIBS as well as a comparison between MQIBS with existing multivariate IBS. Section 6 concludes the paper.

2 Preliminaries

2.1 Commitment schemes

A commitment scheme $\mathsf{Com} : \{0,1\}^\lambda \times \{0,1\}^* \to \{0,1\}^{2\lambda}$, where λ is the security parameter, is a function that takes as input λ uniformly random bit $r \in \{0,1\}^\lambda$ and a message $m \in \{0,1\}^*$, outputs a 2λ bit long commitment $\mathsf{Com}(r,m)$. We require the following two properties of a commitment scheme ([26]).

Definition 1 (Computational binding). *For an adversary $\mathcal{A}$ we define its advantage for the commitment binding game as*

$$\mathsf{Adv}^{\mathsf{Binding}}_{\mathsf{com}}(\mathcal{A}) = \Pr[\mathsf{Com}(r,m) = \mathsf{Com}(r',m') | (r,m,r',m') \leftarrow \mathcal{A}(1^\lambda)].$$

We say that Com is computationally binding if for all polynomial-time algorithms $\mathcal{A}$, the advantage $\mathsf{Adv}^{\mathsf{Binding}}_{\mathsf{com}}(\mathcal{A})$ is a negligible function of the security parameter λ.

Definition 2 (Computational hiding). *For an adversary $\mathcal{A}$ we define the advantage for the commitment hiding game for a pair of messages m, m' as*

$$\mathsf{Adv}^{\mathsf{Hiding}}_{\mathsf{Com}}(\mathcal{A}, \mathsf{m}, \mathsf{m'}) = |\Pr_{r \leftarrow \{0,1\}^\lambda}[1 = \mathcal{A}(\mathsf{Com}(r,m)] - \Pr_{r \leftarrow \{0,1\}^\lambda}[1 = \mathcal{A}(\mathsf{Com}(r,m')]|.$$

We say that Com is computationally hiding if for all polynomial-time algorithms $\mathcal{A}$, and every pair of messages m, m' the advantage $\mathsf{Adv}^{\mathsf{Hiding}}_{\mathsf{Com}}(\mathcal{A}, \mathsf{m}, \mathsf{m'})$ is a negligible function of the security parameter λ.

2.2 Identity-based signature scheme

An identity-based signature (IBS) scheme is a tuple of polynomial-time algorithms $\mathsf{IBS} = (\mathsf{Setup}, \mathsf{KeyDer}, \mathsf{Sign}, \mathsf{Verify})$ as follows:

$\mathsf{Setup}(1^\lambda)$: On input the security parameter λ, it outputs the master public key and secret key pair $(\mathsf{mpk}, \mathsf{msk})$.

$\mathsf{KeyDer}(\mathsf{msk}, \mathsf{id})$: On input the master secret key msk and a user identity ID, it generates the user secret key usk.

$\mathsf{Sign}(\mathsf{mpk}, \mathsf{usk}, M)$: On input the master public key mpk, the user secret key usk and a message M, it outputs a signature σ.

$\mathsf{Verify}(\mathsf{mpk}, \mathsf{id}, \sigma, M)$: On input the master public key mpk, user identity ID, a signature-message pair (σ, M), it outputs 1 for acceptance and 0 for rejection.

We consider the following properties for an IBS scheme. First, the correctness guarantees that a signature generated by an honest signer will always pass the verification algorithm.

Definition 3 (Correctness)**.** *We say that an identity-based signature* IBS *is correct, if for all* $\lambda \in \mathbb{N}$*, all identity* $\mathsf{id} \in \mathcal{ID}$ *and all message* $M \in \mathcal{M}$ *that if* $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$*,* $\mathsf{usk}_{\mathsf{id}} \leftarrow \mathsf{KeyDer}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$*,* $\sigma \leftarrow \mathsf{Sign}(\mathsf{mpk}, \mathsf{usk}_{\mathsf{id}}, M)$ *then it holds that*

$$\Pr[\mathsf{Verify}(\mathsf{mpk}, \mathsf{id}, \sigma, M) = 1] = 1 - \mathsf{negl}(\lambda).$$

Second, it is requires that an adversary cannot create a new tuple (id, message, signature) for an identity and a message that it hasn't been queried before, given that it has already seen some identities' secret keys and signatures for some tuples (identity, message) of its choice.

Definition 4 (EUF-ID-CMA)**.** *We say that an identity-based signature* IBS *is* EUF-ID-CMA *if, for every PPT adversary* $\mathcal{A}$*, it holds that* $\mathcal{A}$ *has a negligible advantage in the following experiment.*
$\mathsf{Exp}_{\mathcal{A}}^{\text{EUF-ID-CMA}}(\lambda)$:

1. *The challenger generates* $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$ *and sets* $\mathcal{Q}_{\mathsf{id}} \leftarrow \emptyset$*,* $\hat{\mathcal{Q}}_{\mathsf{id}} \leftarrow \emptyset$*,* $\mathcal{Q}_{\mathsf{usk}_{\mathsf{id}}} \leftarrow \emptyset$ *and* $\mathcal{Q}_M \leftarrow \emptyset$*.*
2. *The challenger gives* mpk *to the adversary* $\mathcal{A}$*. Moreover,* $\mathcal{A}$ *can access two signing oracles* $\mathcal{O}_{\mathsf{KeyDer}}$*,* $\mathcal{O}_{\mathsf{Sign}}$*, where*
   i. *Key derivation oracle* $\mathcal{O}_{\mathsf{KeyDer}}$*: On input a key derivation query* $\mathsf{id} \in \mathcal{ID}$*, the oracle* $\mathcal{O}_{\mathsf{KeyDer}}$ *checks whether* $(\mathsf{id}, \cdot) \in \mathcal{Q}_{\mathsf{id}}$*. If* $(\mathsf{id}, \cdot) \in \mathcal{Q}_{\mathsf{id}}$ *for some* $\mathsf{usk}_{\mathsf{id}} \in \mathcal{USK}$*, it returns* $\mathsf{usk}_{\mathsf{id}}$*. Otherwise, it returns* $\mathsf{usk}_{\mathsf{id}} \leftarrow \mathsf{KeyDer}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$ *and sets* $\mathcal{Q}_{\mathsf{id}} \leftarrow \mathcal{Q}_{\mathsf{id}} \cup \{(\mathsf{id}, \mathsf{usk}_{\mathsf{id}})\}$
   ii. *Signing oracle* $\mathcal{O}_{\mathsf{Sign}}$*: On input a signing query* $(\mathsf{id}, M) \in \mathcal{ID} \times \mathcal{M}$*, the oracle* $\mathcal{O}_{\mathsf{Sign}}$ *sets* $\mathcal{Q}_M \leftarrow \mathcal{Q}_M \cup \{(\mathsf{id}, M)\}$ *and checks whether* $(\mathsf{id}, \cdot) \in \mathcal{Q}_{\mathsf{id}}$
      - *If* $(\mathsf{id}, \cdot) \in \mathcal{Q}_{\mathsf{id}}$ *for some* $\mathsf{usk}_{\mathsf{id}} \in \mathcal{USK}$*, returns* $\sigma \leftarrow \mathsf{Sign}(\mathsf{mpk}, \mathsf{usk}_{\mathsf{id}}, \mathsf{M})$*.*
      - *If there does not exist* $(\mathsf{id}, \cdot) \in \mathcal{Q}_{\mathsf{id}}$ *for any* $\mathsf{usk}_{\mathsf{id}} \in \mathcal{USK}$*, it computes* $\mathsf{usk}_{\mathsf{id}} \leftarrow \mathsf{KeyDer}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$*, return* $\sigma \leftarrow \mathsf{Sign}(\mathsf{mpk}, \mathsf{usk}_{\mathsf{id}}, \mathsf{M})$ *and sets* $\mathcal{Q}_{\mathsf{id}} \leftarrow \mathcal{Q}_{\mathsf{id}} \cup \{(\mathsf{id}, \mathsf{usk}_{\mathsf{id}})\}$*.*
3. *In the end, the adversary outputs a forgery* $(\mathsf{id}^*, M^*, \sigma^*)$*.*
4. *The challenger outputs 1 if the following three conditions are hold:*
   - *There does not exist* $(\mathsf{id}^*, \cdot) \in \mathcal{Q}_{\mathsf{id}}$ *for any* $\mathsf{usk}_{\mathsf{id}^*} \in \mathcal{USK}$*,*
   - $(\mathsf{id}^*, M^*) \notin \mathcal{Q}_M$*,*
   - $\mathsf{Verify}(\mathsf{mpk}, \mathsf{id}^*, \mathsf{M}^*, \sigma^*) = 1$

The advantage of $\mathcal{A}$ *is defined by* $\mathsf{Adv}_{\mathcal{A}}^{\text{EUF-ID-CMA}}(\lambda) = \Pr[\mathsf{Exp}_{\mathcal{A}}^{\text{EUF-ID-CMA}}(\lambda) = 1]$*.*

3 Sigma protocols with helper

Beullens [26] introduced a sigma protocol with a helper, which involves a three-round sigma protocol that includes a trusted third party, known as the helper. At the start of each protocol execution, the helper runs a setup algorithm using a random seed. The helper then sends auxiliary information to the verifier and provides the seed value used in the setup algorithm to the prover. The syntax can be summarized in the Figure 1.

Definition 5 (Sigma protocol with helper [26])**.** *A protocol is a sigma protocol with helper for relation* R *with challenge space* $\mathcal{C}$ *if it is of the form of Fig. 1 and satisfies:*

Completeness. *If all parties* (Helper, Prover, Verifier) *follow the protocol on input* $(x, w) \in R$*, then the verifier always accepts.*

2-Special soundness. *From an adversary* $\mathcal{A}$ *that outputs with noticeable probability two valid transcripts* $(x, \mathsf{aux}, \mathsf{com}, \mathsf{ch}, \mathsf{rsp})$ *and* $(x, \mathsf{aux}, \mathsf{com}, \mathsf{ch}', \mathsf{rsp}')$ *with* $ch \neq ch'$ *and where* $\mathsf{aux} = \mathsf{Setup}(\mathsf{seed})$ *for some seed value* seed *(not necessarily known to the extractor) one can efficiently extract a witness* w *such that* $(x, w) \in R$*.*

Special honest-verifier zero-knowledge. *There exists a PPT simulator* S *that on input* x*, a random seed value* seed *and a random challenge* ch *outputs a transcript* $(x, \mathsf{aux}, \mathsf{com}, \mathsf{ch}, \mathsf{rsp})$ *with* $\mathsf{aux} = \mathsf{Setup}(\mathsf{seed})$ *that is computationally indistinguishable from the probability distribution of transcripts of honest executions of the protocol on input* (x, w) *for some* w *such that* $(x, w) \in R$*, conditioned on the auxiliary information being equal to* aux *and the challenge being equal to* ch*.*

Beullens then transformed sigma protocols with helper in Figure 1 into a standard zero-knowledge proof of knowledge without helper using the "Cut-and-choose" approach by Katz et al. [21]. We recall it in Figure 2.

Theorem 1 ([26, Theorem 3])**.** *Let* $(\mathsf{Setup}, P_1, P_2, V)$ *be a sigma protocol with helper and challenge space* $\mathcal{C}$*, if the used commitment scheme is hiding, then the protocol of Fig. 2 is an honest-verifier zero-knowledge proof of knowledge with challenge space* $\{1, \ldots, k\} \times \mathcal{C}$ *and* $\max(k, |\mathcal{C}|) + 1$*-special soundness (and hence it has soundness error* $\max(\frac{1}{k}, \frac{1}{|\mathcal{C}|})$*.*

Helper(x)

seed $\xleftarrow{\$} \{0,1\}^{\lambda}$

aux $\leftarrow$ Setup(seed)

Send seed to the prover and aux to the verifier.

Prover(x, w, seed) **Verifier**(x, aux)

$\mathsf{com}, \mathsf{P_{state}} \leftarrow \mathsf{P_1(x, w, seed)}$

$\xrightarrow{\mathsf{com}}$

$ch \xleftarrow{\$} \mathcal{C}$

$\xleftarrow{\mathsf{c}}$

$\mathsf{rsp} \leftarrow \mathsf{P_2(P_{state}, ch)}$

$\xrightarrow{\mathsf{rsp}}$

return $\leftarrow V(x, \mathsf{aux}, \mathsf{com}, ch, \mathsf{rsp})$

Figure 1: The structure of a sigma protocol with trusted setup

4 Construction of MQIBS

4.1 Sigma protocol with helper for MQ problem

In this section, we recall the sigma protocol with helper for MQ Problem from [26] in proving knowledge of a solution of a system of multivariate quadratic equations over a finite field $\mathbb{F}_q$. This scheme improves the previous two schemes by Sakumoto et al.. In particular, the two schemes by Sakumoto et al. have soundness errors $\frac{2}{3}$ and $\frac{1}{2}+\frac{1}{2q}$ respectively while the one with helper has soundness error to only $\frac{1}{q}$.

Let $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is a multivariate quadratic map of m polynomials in n variables, define the polar form of $\mathcal{F}$ as

$$\mathcal{G}(\mathbf{x}, \mathbf{y}) := \mathcal{F}(\mathbf{x}+\mathbf{y}) - \mathcal{F}(\mathbf{x}) - \mathcal{F}(\mathbf{y}).$$

Note that $\mathcal{G}$ is linear in both $\mathbf{x}$ and $\mathbf{y}$. The sigma protocol is described in Figture 3.

Theorem 2 ([26, Theorem 1]). *Suppose the used commitment scheme is computationally binding and computationally hiding, then the protocol of Fig. 3 is a sigma protocol with trusted setup as in Definition 5 with challenge space* $\mathbb{F}_q$.

4.2 Our identity-based signature construction

In this Section, we propose a construction of an identity-based signature from the sigma protocol with helper presented in Figure 3, which we call MQIBS. The idea is to follow the construction by Kiltz et al. [13]. The MQIBS scheme consists of the following polynomial-time algorithms.

$\mathsf{Setup}(1^{\lambda})$**:** Given security parameter λ, output public parameters consisting of m, n, q, k, a random system of polynomials $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, and a hash function $H : \{0,1\}^* \to \{1, \ldots, k\} \times \mathbb{F}_q$, and do the following:

- Choose $\mathbf{s} \xleftarrow{\$} \mathbb{F}_q$ and compute $\mathbf{v} := \mathcal{F}(\mathbf{s}) \in \mathbb{F}_q^m$.
- Output $\mathsf{mpk} = (\mathcal{F}, \mathbf{v})$ and $\mathsf{msk} = \mathbf{s}$.

$\mathsf{KeyDer}(\mathsf{msk}, \mathrm{id})$**:** Given the master secret key $\mathsf{msk} = \mathbf{s}$ and a user identity id, do the following:

- Choose a random system $\mathcal{F}_{\mathrm{id}} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, $\mathbf{s}_{\mathrm{id}} \xleftarrow{\$} \mathbb{F}_q^n$ and compute $\mathbf{v}_{\mathrm{id}} = \mathcal{F}_{\mathrm{id}}(\mathbf{s}_{\mathrm{id}})$.
- For $i \in \{1, \ldots, k\}$ do
  - $\mathsf{seed}_i \xleftarrow{\$} \{0,1\}^{\lambda}$
  - Compute aux_i as in the procedure of Helper($\mathcal{F}$) in Figure 3.
  - Compute com_i as in the first step of the Prover as in Figure 3.
- Set $\mathsf{COM}_{\mathrm{id}} := (\mathsf{com}_i, \mathsf{aux}_i)_{i \in \{1,\ldots,k\}}$.
- Compute $(I, \alpha) := H(\mathsf{COM}_{\mathrm{id}}, \mathcal{F}_{\mathrm{id}} \| \mathrm{id})$
- Retrieve seed_I and compute the response rsp (using $\mathbf{s}$) as in the response by the Prover as in Figure 3. Set $\mathsf{RSP}_{\mathrm{id}} = (\mathsf{rsp}, \mathsf{seed}_i \ \forall i \neq I)$.
- Output the user secret key as $\mathsf{usk} = (\mathbf{s}_{\mathrm{id}}, \mathbf{v}_i, \mathcal{F}_{\mathrm{id}}, \mathsf{COM}_{\mathrm{id}}, \mathsf{RSP}_{\mathrm{id}})$.

$\mathsf{Sign}(\mathsf{mpk}, \mathsf{usk}, M)$**:** Given the master public key mpk, the user secret key usk of a user id and a message M, do the following:

```
Prover                                                  Verifier

for $i \in \{1,\ldots,k\}$ do
    $\mathsf{seed_i} \xleftarrow{\$} \{0,1\}^\lambda$
    $\mathsf{aux_i} \leftarrow \mathsf{Setup(seed_i)}$
    $\mathsf{com_i} \leftarrow \mathsf{P_1(x, w, seed_i)}$
end for
                      $\xrightarrow{\mathsf{aux_i, com_i}\ \forall \mathsf{i}}$
                                                        $I \xleftarrow{\$} \{1,\ldots,k\}$
                                                        $ch \xleftarrow{\$} \mathcal{C}$
                      $\xleftarrow{\text{(I,ch)}}$
$\mathsf{rsp} \leftarrow \mathsf{P_2(x, w, seed_I, com, ch)}$
                      $\xrightarrow{\mathsf{seed_i}\ \forall \mathsf{i} \neq \mathsf{I}, \mathsf{rsp}}$
                                                        if $\exists i \neq I$ : $\mathsf{aux_i} \neq \mathsf{Setup(seed_i)}$
                                                        then
                                                            return 0
                                                        end if
                                                        return $\leftarrow V(x, \mathsf{aux}, \mathsf{com}, ch, \mathsf{rsp})$
```

Figure 2: Zero-knowledge proof without helper

- Parse usk as $(\mathbf{s}_{\text{id}}, \mathbf{v}_{\text{id}}, \mathcal{F}_{\text{id}}, \mathsf{COM}_{\text{id}}, \mathsf{RSP}_{\text{id}})$.
- For $i \in \{1,\ldots,k\}$ do
  - $\mathsf{seed}_i \xleftarrow{\$} \{0,1\}^\lambda$
  - Compute aux_i as in the procedure of Helper($\mathcal{F}_{\text{id}}$) in Figure 3.
  - Compute com_i as in the first step of the Prover as in Figure 3.
- Set **COM** $:= (\mathsf{com}_i, \mathsf{aux}_i)_{i\in\{1,\ldots,k\}}$.
- Compute $(J, c) := H(\mathbf{COM}, M)$
- Retrieve seed_J and compute the response rsp (using $\mathbf{s}_{\text{id}}$) as in the response by the Prover as in Figure 3. Set $\mathsf{RSP} = (\mathsf{rsp}, \mathsf{seed}_i\ \forall i \neq I)$.
- Output a signature as $\sigma = (\mathbf{v}_{\text{id}}, \mathcal{F}_{\text{id}}, \mathsf{COM}_{\text{id}}, \mathsf{RSP}_{\text{id}}, \mathsf{COM}, \mathsf{RSP})$.

$\mathsf{Verify}(\mathsf{mpk}, \mathsf{id}, \sigma, M)$**:** Given a master public key mpk, an identity id, a signature-message pair σ and M, do the following:

- Parse the signature σ as $\sigma = (\mathbf{v}_{\text{id}}, \mathcal{F}_{\text{id}}, \mathsf{COM}_{\text{id}}, \mathsf{RSP}_{\text{id}}, \mathsf{COM}, \mathsf{RSP})$.
- Use $(\mathbf{v}_{\text{id}}, \mathcal{F}_{\text{id}}, \mathsf{COM}, \mathsf{RSP})$ and M do the verification as by the Verifier in Figure 3. Let the result of the verification be b_1.
- Use mpk, $\mathcal{F}_{\text{id}}||\text{id}$, $\mathsf{COM}_{\text{id}}, \mathsf{RSP}_{\text{id}}$ as an input for the verification procedure as in Figure 3. Call the result of this process to be b_2.
- If $b_1 = b_2 = 1$ then output 1, otherwise output 0.

Correctness The correctness is straight-forward with noting that $(\mathsf{COM}, \mathsf{RSP})$ is a signature for the message M under the public key $\mathbf{v}_{\text{id}}, \mathcal{F}_{\text{id}}$ and secret key $\mathbf{s}_{\text{id}}$ of the user id, and $\mathsf{COM}_{\text{id}}, \mathsf{RSP}_{\text{id}}$ is a signature for the message $\mathcal{F}_{\text{id}}||\text{id}$ under the master public key mpk and master secret key msk.

Security The security is also straightforward following the result by Kitlz et al. [13]. In fact, the MQIBS is EUF-ID-CMA secure provided that the underlying signature is EUF-CMA secure. Note that the underlying signature is obtained from applying the Fiat-Shamir transformation to the sigma protocol in Figure 3. Hence if there is an adversary that breaks the EUF-CMA of the underlying signature, then, it is folklore [5] that, there exists an adversary that breaks the soundness of the sigma protocol in Figure 3. It follows from [26, Section 5] that we can construct an algorithm to solve the underlying MQ problem.

[htb]

```
Helper($\mathcal{F}$)
  seed $\xleftarrow{\$} \{0,1\}^\lambda$
  Generate $\mathbf{e} \in \mathbb{F}_q^m$ and $\mathbf{t}, \mathbf{r}_0 \in \mathbb{F}_q^n$ from seed.
  for each $c \in \mathbb{F}_q$ do
    $\mathbf{e}_c \leftarrow c\mathcal{F}(\mathbf{r}_0) - \mathbf{e}$
    $\mathbf{t}_c \leftarrow c\mathbf{r}_0 - \mathbf{t}$
    Generate commitment randomness $\mathbf{r_c} \in \{\mathbf{0},\mathbf{1}\}^\lambda$ from seed.
    $\mathsf{com}_c \leftarrow \mathsf{Com}(\mathbf{r_c}, (\mathbf{e_c}, \mathbf{t_c}))$
  end for
  $\mathsf{aux} \leftarrow [\mathsf{com}_c | c \in \mathbb{F}_q]$
  Send seed to the prover and aux to the verifier.

          Prover($\mathcal{F}$, $\mathbf{s}$, seed)                          Verifier($\mathcal{F}$, $\mathbf{v}$, aux)

          Regenerate $\mathbf{e}, \mathbf{t}, \mathbf{r}_0$ from seed
          $\mathbf{r} \leftarrow \{0,1\}^\lambda$
          $\mathsf{com} \leftarrow \mathsf{Com}(\mathbf{r}, (\mathbf{r}_1, \mathbf{e} + \mathcal{G}(\mathbf{r}_1, \mathbf{t})))$
                                        $\xrightarrow{\mathsf{com}}$
                                                                      $\alpha \xleftarrow{\$} \mathbb{F}_q$
                                        $\xleftarrow{\alpha}$
          Recompute $\mathbf{r}_\alpha, \mathbf{e}_\alpha, \mathbf{t}_\alpha$ from seed
                                        $\xrightarrow{(\mathbf{r}, \mathbf{r}_\alpha, \mathbf{r}_1, \mathbf{e}_\alpha, \mathbf{t}_\alpha)}$
                                                                      $\mathbf{x} \leftarrow \alpha(\mathbf{v} - \mathcal{F}(\mathbf{r}_1)) - \mathbf{e}_\alpha - \mathcal{G}(\mathbf{r}_1, \mathbf{t}_\alpha)$
                                                                      $b_1 \leftarrow \mathsf{com} = \mathsf{Com}(\mathbf{r}, (\mathbf{r}_1, \mathbf{x}))$
                                                                      $b_2 \leftarrow \mathsf{com}_\alpha = \mathsf{Com}(\mathbf{r}, (\mathbf{e}_\alpha, \mathbf{t}_\alpha))$
                                                                      Return $b_1 \wedge b2$
```

Figure 3: Sigma protocol with helper for MQ problem

5 Parameters

5.1 Optimizations

In this section, we review about the techniques presented in [26], which was followed by Katz et al. [21], for optimizations. Some are as follows; see [26, Section 7] for the details.

- Build a Merkle tree on the commitments com_i computed in the KeyDer process as well as the Sign process to reduce the user secret key usk as well as signature size σ. In particular, instead of including all com_i in $\mathsf{COM}_{\mathsf{id}}$ (resp. COM), we use only the root of the Merkle tree created by the com_i, and hence $\mathsf{RSP}_{\mathsf{id}}$ (resp. RSP) consists only $\lceil \log_2(q) \rceil$ nodes required to reconstruct the root of the Merkle tree. Similarly, we can do the same for aux_i in $\mathsf{COM}_{\mathsf{id}}$ (resp. COM), and seed_i in $\mathsf{RSP}_{\mathsf{id}}$ (resp. RSP).
- For some applications, the finite field $\mathbb{F}_q$ is large and hence not practical to compute Merkle trees of size q. We then can reduce the challenge space to $\mathbb{F}_{q'}$ with $q' < q$. It then makes the protocol in Figure 3 has soundness error $\frac{1}{q'}$ (instead of $\frac{1}{q}$). Katz et al. [21] suggested that, instead of letting the verifier choose 1 out of k setups to execute, we now let him choose τ out of M setups to execute, which results to the soundness error bounded by

$$\max_{0 \le e \le \tau} \frac{\binom{M-e}{\tau-e}}{\binom{M}{\tau} q'^{\tau-e}}.$$

See [26, Section 7] or [21] for the details.

5.2 Parameters

We follow [26] for the choice of parameters m, n, q, τ, M. First of all, $q = 4$ and $m = n = 88, 128, 160$ respectively following [20] in the MQDSS submission to the NIST PQC standardization project. Note that we choose the number of equations m equal to the number of variables n, i.e., $m = n$,

Table 1: Parameters for MQIBS

Security Level	q	n	M	τ	|mpk| (B)	|msk| (B)	Signature (B)
I	4	88	191	68	38	16	28,838
III	4	128	256	111	56	24	65,856
V	4	160	380	136	72	32	111,272

Table 2: Comparison between our MQIBS with other existing multivariate IBS

Scheme	|mpk| (B)	|msk| (B)	Signature (B)
Ours (MQIBS)	38	16	28,838
IBS-Rainbow [23]	148,300	103,700	304,300
ID-Rainbow [24]	4,220,000	142,600	46
Mul-IBS-Rainbow [31]	136,100	90,900	33,400

to ensure that we get the hardest instance of an MQ problem [20]. The parameters τ and M are chosen to balance between the signature size and running time: increasing τ impacts signature size, while decreasing M impacts signing and verification time [26]. The parameters for MQIBS, key and signature sizes are summarized in Table 1.

In Table 2, we provide a comparison between existing IBS scheme from multivariate polynomials at the security level I. It can be seen from Table that our scheme outperforms the existing ones (except the ID-Rainbow [24]) in terms of signature size. In addition, our scheme has the smallest public key size. Compared to the ID-Rainbow by Chen et al. [24], our scheme has much bigger signature size (28,838 B vs. 46 B) but has much smaller master public key (38 B vs. 4,220,000B) and secret key (16 B vs. 142,600 B). We note that due to the recent attack by Beullens [30] against Rainbow scheme, those existing schemes mentioned in Table 2 would be vulnerable to Beullens' attack and hence need to update the parameters to attain the same security level which will result in much larger key/signature sizes compared to those mentioned in Table 2.

6 Conclusion

In this paper, we propose a design for an identity-based signature, called MQIBS, from multivariate polynomials. Our scheme is derived from the sigma protocol with helper for MQ from Beullens [26] from which our MQIBS inherits the efficiency. Compared to existing schemes, our scheme has advantage on both signature size as well as public key and secret key size. Further optimizations and implementations are one of the goals for our future work.

Acknowledgement

The author would like to thank Dung Duong for useful discussions.

Funding

This research is funded by Vietnam National University, Ho Chi Minh City (VNU-HCM) under grant number C2022-18-03.

References

[1] National Institute of Standards and Technology post-quantum cryptography. https://csrc.nist.gov/projects/post-quantum-cryptography. Accessed: 2024-07-24.

[2] National Institute of Standards and Technology additional post-quantum signatures. https://csrc.nist.gov/projects/pqc-dig-sig/round-1-additional-signatures. Accessed: 2024-07-24.

[3] Michael R. Garey and David S. Johnson (1979). *Computers and Intractability: A Guide to the Theory of Np-Completeness*. W. H. Freeman. https://doi.org/10.2307/2273574

[4] Adi Shamir (1984). Identity-based cryptosystems and signature schemes. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer. https://doi.org/10.1007/3-540-39568-7_5

[5] Amos Fiat and Adi Shamir (1986). How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *Advances in Cryptology - CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194.

Springer.
https://doi.org/10.1007/3-540-47721-7_12

[6] Tsutomu Matsumoto and Hideki Imai (1988). Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption. In: Barstow, D., et al. *Advances in Cryptology — EUROCRYPT '88. EUROCRYPT 1988. Lecture Notes in Computer Science*, vol 330. Springer, Berlin, Heidelberg.
https://doi.org/10.1007/3-540-45961-8_39

[7] Jacques Patarin (1995). Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88. In: Coppersmith, D. (eds) *Advances in Cryptology — CRYPT0' 95. CRYPTO 1995. Lecture Notes in Computer Science*, vol 963. Springer, Berlin, Heidelberg.
https://doi.org/10.1007/3-540-44750-4_20

[8] Kipnis, A., Patarin, J., Goubin, L. (1999). Unbalanced Oil and Vinegar Signature Schemes. In: Stern, J. (eds) *Advances in Cryptology — EUROCRYPT '99. EUROCRYPT 1999. Lecture Notes in Computer Science*, vol 1592. Springer, Berlin, Heidelberg.
https://doi.org/10.1007/3-540-48910-X_15

[9] Craig Gentry, Alice Silverberg (2002). Hierarchical ID-Based Cryptography. *ASIACRYPT 2002*: 548-566.
https://doi.org/10.1007/3-540-36178-2_34

[10] Jintai Ding and Dieter Schmidt (2005). Rainbow, a new multivariable polynomial signature scheme. In John Ioannidis, Angelos D. Keromytis, and Moti Yung, editors, *Applied Cryptography and Network Security, Third International Conference, ACNS 2005, New York, NY, USA, June 7-10, 2005, Proceedings*, volume 3531 of *Lecture Notes in Computer Science*, pages 164–175.
https://doi.org/10.1007/11496137_12

[11] Andrey Bogdanov, Thomas Eisenbarth, Andy Rupp, and Christopher Wolf (2008). Time-area optimized public-key engines: Mq-cryptosystems as replacement for elliptic curves? *IACR Cryptol. ePrint Arch.*, page 349.
https://doi.org/10.1007/978-3-540-85053-3_4

[12] Anna Inn-Tung Chen, Ming-Shing Chen, Tien-Ren Chen, Chen-Mou Cheng, Jintai Ding, Eric Li-Hsiang Kuo, Frost Yu-Shuang Lee, and Bo-Yin Yang (2009). SSE implementation of multivariate pkcs on modern x86 cpus. In Christophe Clavier and Kris Gaj, editors, *Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lausanne, Switzerland, September 6-9, 2009, Proceedings*, volume 5747 of *Lecture Notes in Computer Science*, pages 33–48. Springer.
https://doi.org/10.1007/978-3-642-04138-9_3

[13] Eike Kiltz and Gregory Neven (2009). Identity-based signatures. In Marc Joye and Gregory Neven, editors, *Identity-Based Cryptography*, volume 2 of *Cryptology and Information Security Series*, pages 31–44. IOS Press.
https://doi.org/10.3233/978-1-58603-947-9-31

[14] Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann (2010). Cyclicrainbow - A multivariate signature scheme with a partially cyclic public key. In Guang Gong and Kishan Chand Gupta, editors, *Progress in Cryptology - INDOCRYPT 2010 - 11th International Conference on Cryptology in India, Hyderabad, India, December 12-15, 2010. Proceedings*, volume 6498 of *Lecture Notes in Computer Science*, pages 33–48. Springer.
https://doi.org/10.1007/978-3-642-17401-8_4

[15] Markus Rückert (2010). Strongly Unforgeable Signatures and Hierarchical Identity-Based Signatures from Lattices without Random Oracles. *PQCrypto 2010*: 182-200.
https://doi.org/10.1007/978-3-642-12929-2_14

[16] Shweta Agrawal, Dan Boneh, Xavier Boyen (2010). Efficient Lattice (H)IBE in the Standard Model. *EUROCRYPT 2010*: 553-572
https://doi.org/10.1007/978-3-642-13190-5_28

[17] Koichi Sakumoto, Taizo Shirai, and Harunaga Hiwatari (2011). Public-key identification schemes based on multivariate quadratic polynomials. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*, pages 706–723. Springer.
https://doi.org/10.1007/978-3-642-22792-9_40

[18] Wuqiang Shen, Shaohua Tang, and Lingling Xu (2013). Ibuov, A provably secure identity-based UOV signature scheme. In *16th IEEE International Conference on Computational Science and Engineering, CSE 2013, December 3-5, 2013, Sydney, Australia*, pages 388–395. IEEE Computer Society.
https://doi.org/10.1109/CSE.2013.66

[19] Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe (2016). From 5-pass *MQ* -based identification to *MQ* -based signatures. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security,*

Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II, volume 10032 of *Lecture Notes in Computer Science*, pages 135–165.
`https://doi.org/10.1007/978-3-662-53890-6_5`

[20] Ming-Shing Chen, Andreas H lsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe (2017). MQDSS-Submission to the NIST post-quantum cryptography project. In *NIST Post-quantum Cryptography*. available at `https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/MQDSS.zip`

[21] Jonathan Katz, Vladimir Kolesnikov, and Xiao Wang (2017). Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures. In *CCS '18: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 525 – 537. ACM.
`https://doi.org/10.1145/3243734.3243805`

[22] Masayuki Fukumitsu, Shingo Hasegawa (2018). A Galindo-Garcia-Like Identity-Based Signature with Tight Security Reduction, Revisited. *CANDAR 2018*: 92-98
`https://doi.org/10.1109/CANDAR.2017.79.`

[23] Le Van Luyen (2019). An improved identity-based multivariate signature scheme based on rainbow. *Cryptography*, 3(1):8.
`https://doi.org/10.3390/cryptography3010008`

[24] Jiahui Chen, Jie Ling, Jianting Ning, and Jintai Ding (2019). Identity-based signature schemes for multivariate public key cryptosystems. *Comput. J.*, 62(8):1132–1147.
`https://doi.org/10.1093/comjnl/bxz013`

[25] Hiroki Furue, Dung Hoang Duong, and Tsuyoshi Takagi (2019). An efficient mq-based signature in the QROM. In *2019 Seventh International Symposium on Computing and Networking, CANDAR 2019, Nagasaki, Japan, November 25-28, 2019*, pages 10–17. IEEE.
`https://doi.org/10.1109/CANDAR.2019.00010`

[26] Ward Beullens (2020). Sigma Protocols for MQ, PKP and SIS, and Fishy Signature Schemes. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part III*, volume 12107 of *Lecture Notes in Computer Science*, pages 183–211. Springer.
`https://doi.org/10.1007/978-3-030-45727-3_7`

[27] Daniel Kales and Greg Zaverucha (2020). An attack on some signature schemes constructed from five-pass identification schemes. In Stephan Krenn, Haya Schulmann, and Serge Vaudenay, editors, *Cryptology and Network Security - 19th International Conference, CANS 2020, Vienna, Austria, December 14-16, 2020, Proceedings*, volume 12579 of *Lecture Notes in Computer Science*, pages 3–22. Springer.
`https://doi.org/10.1007/978-3-030-65411-5_1`

[28] Jiaxin Pan, Benedikt Wagner (2021). Short Identity-Based Signatures with Tight Security from Lattices. *PQCrypto 2021*: 360-379
`https://doi.org/10.1007/978-3-030-81293-5_19`

[29] Surbhi Shaw, Ratna Dutta (2021). Identification Scheme and Forward-Secure Signature in Identity-Based Setting from Isogenies. *ProvSec 2021*: 309-326.
`https://doi.org/10.1007/978-3-030-90402-9_17`

[30] Ward Beullens (2022). Breaking rainbow takes a weekend on a laptop. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II*, volume 13508 of *Lecture Notes in Computer Science*, pages 464–479. Springer.
`https://doi.org/10.1007/978-3-031-15979-4_16`

[31] Sumit Kumar Debnath, Sihem Mesnager, Vikas Srivastava, Saibal Kumar Pal, and Nibedita Kundu (2023). Mul-ibs: a multivariate identity-based signature scheme compatible with iot-based NDN architecture. *J. Cryptogr. Eng.*, 13(2):187–199.
`https://doi.org/10.1007/s13389-022-00308-8`

[32] Ernest Foo, Qinyi Li (2023). Tightly Secure Lattice Identity-Based Signature in the Quantum Random Oracle Model. *ACISP 2023*: 381-402.
`https://doi.org/10.1007/978-3-031-35486-1_17`

[33] Jiawei Chen, Hyungrok Jo, Shingo Sato, Junji Shikata (2023). A Tightly Secure Identity-Based Signature Scheme from Isogenies. *PQCrypto 2023*: 141-163.
`https://doi.org/10.1007/978-3-031-40003-2_6`

[34] Xuan Thanh Khuc, Willy Susilo, Dung Hoang Duong, Fuchun Guo, Hyungrok Jo, Tsuyoshi Takagi (2024).

Tightly Secure Identity-based Signature from Cryptographic Group Actions. *ProSec 2024*.