Mul-IBS: A Multivariate Identity-Based Signature Scheme Compatible with IoT-based NDN Architecture

Sumit Kumar Debnath[1,2], Sihem Mesnager[3,*], Vikas Srivastava[4], Saibal Kumar Pal[5], and Nibedita Kundu[6]

[1]Department of Mathematics, National Institute of Technology Jamshedpur, Jamshedpur-831014, India; sdebnath.math@nitjsr.ac.in
[2]Department of Mathematics, Indian Institute of Information Technology Kalyani, Kalyani-741235, India; sumit@iiitkalyani.ac.in
[3]Department of Mathematics, University of Paris VIII, F-93526 Saint-Denis, University Sorbonne Paris Cité, LAGA, UMR 7539, CNRS, 93430 Villetaneuse, and Télécom Paris, 91120 Palaiseau, France; smesnager@univ-paris8.fr
[4]Department of Mathematics, National Institute of Technology Jamshedpur, Jamshedpur-831014, India; vikas.math123@gmail.com
[5]SAG Lab, Defense Research & Development Organization, Delhi-110054, India; skptech@yahoo.com
[6]Department of Mathematics, The LNM Institute of Information Technology, Jaipur -302031, India; nknkundu@gmail.com

Abstract

It has been forty years since the TCP/IP protocol blueprint, which is the core of modern worldwide Internet, was published. Over this long period, technology has made rapid progress. These advancements are slowly putting pressure and placing new demands on the underlying network architecture design. Therefore, there was a need for innovations that can handle the increasing demands of new technologies like IoT while ensuring secrecy and privacy. It is how Named Data Networking (NDN) came into the picture. NDN enables robust data distribution with interest-based content retrieval and leave-copy-everywhere caching policy. Even though NDN has surfaced as a future envisioned and decisive machinery for data distribution in IoT, it suffers from new data security challenges like content poisoning attacks. In this attack, an attacker attempts to introduce poisoned content with an invalid signature into the network. Given the circumstances, there is a need for a cost-effective signature scheme, requiring inexpensive computing resources and fast when implemented. An identity-based signature scheme (IBS) seems to be the natural choice to address this problem. Herein, we present an IBS, namely Mul-IBS relying on multivariate public key cryptography (MPKC), which leads the race among the post-quantum cryptography contenders. A 5-pass identification scheme accompanying a safe and secure signature scheme based on MPKC works as key ingredients of our design. Our Mul-IBS attains optimal master public key size, master secret key size, and user's secret key size in the context of multivariate identity-based signatures. The proposed scheme Mul-IBS is proven to be secure in the model "existential unforgeability under chosen-message and chosen identity attack (uf-cma)" contingent upon the fact that Multivariate Quadratic (MQ) problem is NP-hard. The proposed design Mul-IBS can be utilized as a crucial cryptographic building block to build a robust and resilient IoT-based NDN architecture.

Keywords: Multivariate public key cryptography; post-quantum cryptography; identity based signature; IoT; NDN.

MSC 2010: 94A60; 94A62; 68M12; 68P30.

1 Introduction

The currently used host-centric nature of the network architecture is not fit for IoT-based systems due to hurdles like high latency, inadequate address spacing, and caching. A novel network architecture model called Named Data Networking (NDN) [9, 29] is swiftly gaining popularity to ensure efficient content distribution. NDN is decorated with features like leave copy everywhere (LCE) caching policy and name-based routing, making it ideal for content distribution among IoT devices. To cut a long story short, a network dispatches and transfers data. Designing a network architecture becomes a pivotal task as it describes and explains how these bits of data will be dispatched in the real world. The core question that any network design should address is what namespaces are used for data transfer. Currently used TCP/IP protocol architecture [20] uses a namespace design where locations are named. It is very similar to a telephone network where each telephone is assigned a phone number. In TCP/IP network protocol, these phone numbers are replaced by IP addresses. In short, TCP/IP is a location-based, host-centric, point-to-point communication model. NDN uses an entirely different namespace design. In an NDN-based network architecture, data bits are named themselves. Let John be a client who is interested in some content, say Γ. His interest request is transferred to the original publisher of the content. Due to the LCE caching policy, the response sent by the publisher is cached by the intermediate routers for future use. In the future, if another user, Michael, displays interest in the same content Γ, then local routers will serve the interest request of Michael instead of forwarding it again to the publisher. In this way, the network's overall efficiency is increased as contents are provided to users locally from the caches. It also enhances the response time since the content request must not be dispatched to the original broadcaster of the content (Figure 1).

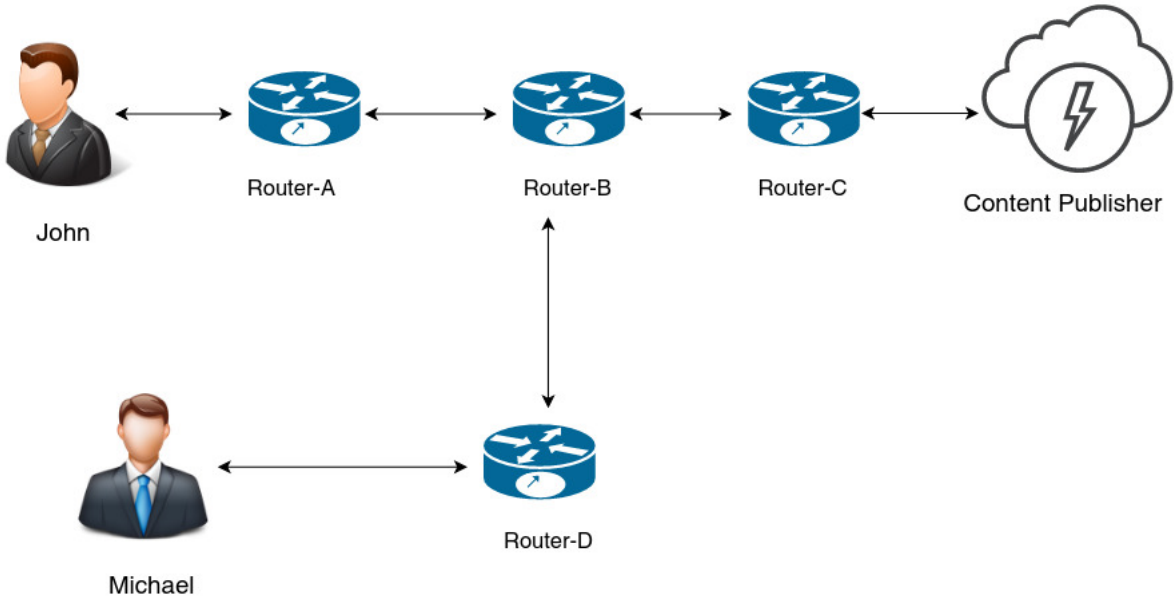

Figure 1 : Caching Policy and Routing in NDN Architecture

NDN brings with itself a lot of advantages over the currently used host-centric architecture. It includes advanced features like built-in multicasting, LCE caching policy. In NDN, security is built into data itself rather than a function of where or how it is obtained. Even though

NDN has surfaced as a future envisioned and decisive machinery for data distribution in IoT, it suffers from new data security challenges. Among all major hurdles, a content poisoning attack is the most prevalent one. In this attack, an attacker attempts to introduce poisoned content with an invalid signature into the network. A possible solution to mitigate the network from a content poisoning attack is to append a signature of the contents to every data package. The circumstances demand a cost-effective identity-based signature (IBS), requiring inexpensive computing resources and fast when implemented.

In 1984, Shamir [24] put forward the concept of the first IBS. The key idea behind IBS is that a user's public key can be directly derived from its identity, such as names and email addresses, instead of randomly generated keys. This removes the requirement of digital certificates for linking public keys with identities. In the identity-based setting, a trusted secret key generator or key distribution center SKG derives users' private keys from a master secret key and issues the secret keys to the respective users. Note that the master secret key is only known to the SKG, who is having an out-of-band way for verifying the users' identities. The inherent key escrow feature of IBS is the SKG can generate all users' secret keys. This property ensures that SKG has to be trusted; otherwise, it can misuse its power. In contrast to IBS, the traditional PKI does not allow CA to get information about users' secret keys. Thus, from the security perspective, inherent key escrow property is a major drawback of IBS, unlike traditional PKI. However, a similar kind of fraud is possible in PKI. For instance, a fake certificate can be generated by a cheating CA for a public key of which it has knowledge of the corresponding secret key. As a consequence, the CA can generate valid signatures. Note that the victim may try to prove its honesty by revealing its original certificate to a judge, but it is impossible to prevent the CA from demanding that the user registered two distinct public keys. The escrow feature is not a serious issue in the signature scheme as opposed to the encryption scheme, where the SKG can decrypt ciphertexts associated with any of its users. Still, a limited form of key escrow property inherently appears in both identity-based and PKI-based signatures. Almost all of the currently used IBS schemes rely on challenging classical problems [11, 12, 21]. Unfortunately, these IBS schemes will become obsolete once quantum computers come into the market. This is since Shor's algorithm [26] can be employed to break these classical hard problems in polynomial time. It makes the requirements of finding an alternative solution, i.e., quantum computer resistant IBS, which falls under post-quantum cryptography (PQC) [1]. In the last two decades, PQC becomes a new direction of research to overcome the threat of Shor's algorithm. Since 2013, a working group of the National Institute of Standards and Technologies (NIST) studied the standardization of Post-Quantum cryptography. The European Telecommunications Standards Institute (ETSI) is also organizing a regular Quantum-Safe-Crypto Workshop. Apart from lattice-based, code-based, isogeny based and hash-based cryptosystems, multivariate cryptography is one of the leading candidates for PQC. Mathematical operations used in multivariate cryptographic schemes are elementary. Mainly, addition and multiplications over finite fields are the most used mathematical operations. This makes them fast and efficient, making them suitable for low-cost devices [2, 3].

A system of multivariate polynomials works as the public key of an MPKC. The security of MPKC stands on the fact MQ problem is NP-hard [7, 16]. In the current state of art, there are several practical multivariate encryption and signature schemes such as MI [14], HFE [15], UOV [10], Rainbow [6], Gui [19], etc. However, there is a deficiency of signature schemes with special properties such as IBS. Thus the development of secure and efficient multivariate IBS becomes an exciting direction of research work. The first multivariate IBS, namely IBUOV, was proposed by Shen et al. [25]. They employed standard UOV [10] as building blocks of their

construction. In the following, Luyen [13] designed a multivariate IBS by modifying UOV and Rainbow [6] using the technique of Sakumoto et al. [22]. Recently, Chen et al. [4] developed a general construction of multivariate IBS that is compatible with any MPKC.

1.1 Our Contribution

The unprecedented advancements that the Internet has made over the last few decades have put a lot of pressure and placed new demands on the underlying network architecture design. The situation demands new ingenious ideas to handle the requirements of modern technologies like IoT while ensuring secrecy and privacy. These circumstances manifested a novel network architecture design, Named Data Networking (NDN), enabling robust data distribution with interest-based content retrieval and leave-copy-everywhere caching policy. Although NDN-based architecture brings significant advantages to IoT, it has to fight against shortcomings. One of the most prevalent ones is content poisoning attacks. In this attack, an attacker attempts to introduce poisoned content with an invalid signature into the network. Hence, a growing need for a cost-effective signature scheme requires inexpensive computing resources and fast when implemented. An IBS seems to be the natural choice to address this problem. Almost all of the existing IBS rely upon the intractability of classical hard problems like discrete logarithm or number factorization. However, these IBS will become outdated as given a quantum computer, classical problems on which their hardness lies can be broken easily. This demands an IBS that is post-quantum-safe.

Herein, we propose the multivariate-based IBS, namely Mul-IBS which offers resistance against attacks by quantum computers. We utilize a multivariate signature scheme (say Rainbow [6]) along with 5-pass identification scheme [22] as the cryptographic building blocks of Mul-IBS. The technique by Hülsing et al. [5] in our design. The Mul-IBS involves four algorithms: (i) Setup, (ii) Extract, (iii) Signature Generation, and (iv) Signature Verification. On the input security parameter κ, the SKG runs Setup to generate Mpk and Msk. It publishes Mpk as master public key and keeps with itself Msk as master secret key. In the following, the SKG produces user's private key $\mathbf{u}_{ID}$ by running Extract for an user with identity $ID \in \{0,1\}^*$. Given a message $\mathsf{Mg} \in \{0,1\}^*$, an user having identity $ID \in \{0,1\}^*$ and signing key $\mathbf{u}_{ID}$, runs Signature Generation, to produce a signature $\theta = Sign(\mathsf{Mg})$. In order to validate the correctness of the signature θ, a verifier runs Signature Verification on input $(Mpk, \mathsf{Mg}, \theta, ID)$. Size of Mpk and Msk are respectively $\frac{m(n+2)(n+1)}{2}$ and n^2+m^2+c field ($\mathbb{F}_q$) elements, where c is the size of the central map and, m and n are the number of public polynomials and the number of variables of the underlying MQ based signature scheme respectively. Identity of user and private key sizes are m and n field ($\mathbb{F}_q$) elements respectively. The signature size is 2α $|commitment| + \alpha(m+2n)$-$\mathbb{F}_q$ elements, α being the number of rounds needed for the underlying identification protocol. Luyen [13] claimed that the authors of [25] selected wrong parameters with the corresponding desired security level, as well as evaluated the wrong corresponding key sizes. While, in our scheme, we have correctly chosen the parameters. Moreover, IBS of [25] does not achieve uf-cma security, unlike ours.

The IBS of [13] is similar to PKI, where each user has a different public key and SKG needs to link the user's public key with the user's identity by providing a digital certificate. In other words, the work of [13] seems to be attaching a certificate to a non-identity-based signature. In contrast to the work of [13], we do not require any such digital certificate for linking the user's public key with the user's identity. In the IBS of [4], the master public key $\overline{F}$ is a function of

user's identity $ID_u = (z_1, \ldots, z_d)$. Thus, if a verifier wants to verify the signature produced by a user with identity ID_u then he first needs to evaluate the expression of the master public key $\overline{F}$ for the user's identity ID_u. Thereby, it increases the computation complexity of the verifier. While our scheme does not have this issue as the master public of our IBS is not a function of the user's identity. Similar to [13], our signature scheme is provable secure since it attains uf-cma security. While, [4] is not provable secure. The most attractive point of our scheme is that it performs better over [4, 13, 25] given the sizes of the master public key, user's private key size, and Msk. The size of the signature of Mul-IBS is less than that of [13, 25]. Our scheme is ideally suited for an IoT-based NDN network where a lightweight IBS is needed for building a resilient network system.

2 Organization

The paper is structured as follows. Basic preliminaries are described in Section 3. We give the construction of our IBS in Section 4. Security analysis of our scheme is discussed in Section 5 followed by efficiency analysis in Section 6. Application of Mul-IBS in IoT-Based NDN Architecture is provided in Section 7. Finally, we conclude the paper in Section 8.

3 Preliminaries

We first give some basic notations. Throughout the paper, κ represents "security parameter", $x \in_R S$ denote that "x is chosen uniformly at random from a set S", finite field with q elements is denoted by $\mathbb{F}_q$, $\mathbb{F}_{q^\eta}$ represent an extension field of $\mathbb{F}_q$ of degree η and $(\mathbb{F}_q)^\eta = \{\mathbf{y} = (y_1, \ldots, y_\eta) | y_i \in \mathbb{F}_q \text{ for } i = 1, \ldots, \eta\}$ is a vector space.

3.1 Hardness Assumption

Our proposed design Mul-IBS rests its security on the hardness of MQ problem. The problem is expressed as:

Definition 3.1. *Given a system* $\mathcal{Q} = (q_{(1)}(\rho_1, \ldots, \rho_n), \ldots, q_{(m)}(\rho_1, \ldots, \rho_n))$ *of* m *quadratic equations in variables* $(\rho_1, \ldots, \rho_n)$*, find a* n *tuple* $(\bar{\rho}_1, \ldots, \bar{\rho}_n)$ *such that*

$$w_{(1)}(\bar{\rho}_1, \ldots, \bar{\rho}_n) = \cdots = w_{(m)}(\bar{\rho}_1, \ldots, \bar{\rho}_n) = 0.$$

3.2 Multivariate Identification Scheme [23]

Zero-knowledge schemes empower clients to exhibit that they possess a particular set of information without disclosing it to the person they are trying to convince. Let us understand through an example. Take for granted that Alice understands how to solve the Tower of Hanoi puzzle [28]. She wishes to assure Bob of the truth that she knows the solution. In the process, she also wants to ensure that she does not disclose the puzzle's solution. One way to proceed is that Alice provides Bob a particular Tower of Hanoi puzzle. Then Alice faces in a different direction and solves it. After decoding, she hands over the solved puzzle to Bob. So Bob is

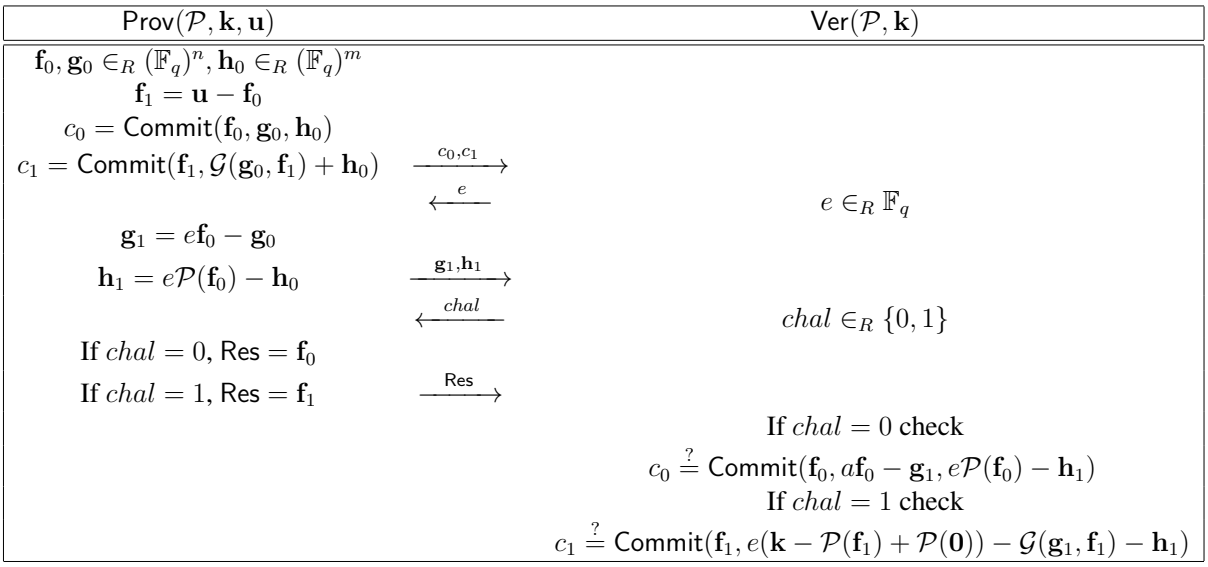

Figure 2 : 5-pass identification protocol

convinced that Alice solved the Tower of Hanoi problem without her disclosing the solution to him. The idea mentioned above can be easily adapted to an identification scheme.

A multivariate identification scheme make use of a random chosen MQ system $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$. The security of a multivariate identification scheme is contingent on the presumption that the MQ problem is hard. Suppose a user, Alice desires to identify herself to another user Bob. Alice is also called prover, and Bob, to whom Alice is trying to convince, is called verifier. Now Alice wants to exhibit to Bob that he understand how to compute $\widetilde{s}$, a solution of $\mathcal{P}(\widetilde{x}) = \widetilde{v}$ without disclosing any details about $\widetilde{s}$. Such a scheme can be constructed using the technique of zero-knowledge proof (ZKP). To construct a ZKP of knowledge of $\widetilde{s}$, we define a new function called the polar form of $\mathcal{P}$ which is mathematically formulated as $\mathcal{G}(\gamma_{\mathbf{1}}, \gamma_{\mathbf{2}}) = \mathcal{P}(\gamma_{\mathbf{1}} + \gamma_{\mathbf{2}}) - \mathcal{P}(\gamma_{\mathbf{1}}) - \mathcal{P}(\gamma_{\mathbf{1}}) + \mathcal{P}(\mathbf{0})$. Presuming the existence of a computationally binding and statistically hiding commitment scheme, Commit Sakumoto et. al. [23] constructed a 5-pass identification scheme for the knowledge of $\widetilde{s}$.

Assume that SE denotes the soundness error of the scheme; then we have $\mathsf{SE} = 1/2 + 1/2q$. To achieve the desired security level and reduce impersonation probability, we need to execute the protocol in multiple rounds. The numbers of rounds required to reach the security level of η is given by $r = \left\lceil \frac{-\eta}{\log_2(\mathsf{KE})} \right\rceil$.

3.3 General Construction of Identity Based Signature (IBS)[17]

An identity based signature (IBS) scheme consists of the four algorithms the algorithms Setup, Extract, Signature Generation and Signature Verification, which execute as follows:

Setup(1^κ): On input the security parameter κ, the secret key generator or key distribution center SKG, generates master public key-secret key pair (Mpk, Msk).

Extract(Msk, ID): On input Msk and an identity $ID \in \{0, 1\}^*$, the SKG runs Extract algorithm for generating the signing key u_{ID} corresponding to the user having identity ID.

Signature Generation(u_{ID}, Mg): On input u_{ID} and message $\mathsf{Mg} \in \{0,1\}^*$, the user with identity ID runs Signature Generation to generate a signature θ of Mg.

Signature Verification$(\mathsf{Mpk}, \mathsf{Mg}, \theta, ID)$: On input $\mathsf{Mpk}, \mathsf{Mg}, \theta, ID$, the verifier runs Signature Verification to check the correctness of the message-signature pair (Mg, θ). It it is a valid pair corresponding to the identity ID then Signature Verification outputs 1; otherwise, outputs 0.

3.4 Existential Unforgeability under Chosen-Message and Chosen-Identity Attack (uf-cma) [8]

The notion of uf-cma is considered as the standard security notion for an IBS. It is defined by a "game", or an experiment, run between a forger FG and a challenger CH. Let us consider an IBS that consists of the algorithms Setup, Extract, Signature Generation and Signature Verification. Then the experiment $\mathsf{Ex}^{\text{uf-cma}}_{IBS(1^\kappa)}$ is described below:

The CH runs Setup(1^κ) to generate (Mpk, Msk) and sends Mpk to FG.

The FG adaptively makes a number of following queries to CH:

Extract-query : For any $ID \in \{0,1\}^*$, the FG can ask the corresponding secret key to the CH. In order to give response, the CH runs Extract(Mpk, Msk, ID) to extract the secret key $\mathbf{u}_{ID}$ and sends it to the FG.

Sign-query : For any $ID \in \{0,1\}^*$ and message Mg, the FG can ask the corresponding signature to the CH. In order to give response, the CH first runs Extract(Mpk, Msk, ID) to extract the secret key $\mathbf{u}_{ID}$ and then runs the Signature Generation$(Mpk, ID, \mathbf{u}_{ID}, \mathsf{Mg})$ to get the signature $\theta = Sign(Mg)$, which is sent to FG.

The FG outputs an identity ID^*, message Mg^* and a signature θ^*.

The FG will win the game i.e., output of the experiment $\mathsf{Ex}^{\text{uf-cma}}_{IBS(1^\kappa)}$ will be 1 if Signature Verification$(Mpk, \mathsf{Mg}^*, \theta^*, ID^*) = 1$ and FG has neither made any Extract-query on ID^* nor made any Sign-query on (ID^*, Mg^*). We denote the advantage or the success probability of FG by $\mathsf{Adv}^{\mathsf{Ex}^{\text{uf-cma}}_{IBS(1^\kappa)}}_{\mathsf{FG}}$ which is defined as $\mathsf{Adv}^{\mathsf{Ex}^{\text{uf-cma}}_{IBS(1^\kappa)}}_{\mathsf{FG}} = \mathsf{Prob}[\mathsf{Ex}^{\text{uf-cma}}_{IBS(1^\kappa)} = 1]$ = Prob[FG *wins the game*].

Definition 3.2. *An IBS is said to be uf-cma secure if* $\mathsf{Adv}^{\mathsf{Ex}^{uf-cma}_{IBS(1^\kappa)}}_{\mathsf{FG}}$ *is negligible in security parameter* κ *for any probabilistic polynomial time (PPT) forger* FG *who is allowed to make at most* Q_e *(polynomial time)* Extract − query *and* Q_s *(polynomial time)* Sign − query.

4 Proposed Multivariate Identity Based Signature (Mul-IBS)

In this section, we present the multivariate based IBS, namely Mul-IBS. We take advantage of a multivariate signature scheme (say Rainbow [6]) together with 5-pass identification scheme as fundamental blocks of our proposed design. We make use of the technique by Hülsing et

al. [5] of transforming identification scheme into a signature scheme. TheMul-IBS consist of four algorithms: (i) Setup, (ii) Extract, (iii) Signature Generation, and (iv) Signature Verification. On the input of κ (security parameter), the secret key generator SKG runs Setup to produce master public key Mpk and mater secret key Msk During Extract, the SKG generates clients private key $\mathbf{u}_{ID}$ for a client having identity $ID \in \{0,1\}^*$. Given a message $\mathsf{Mg} \in \{0,1\}^*$, the algorithm Signature Generation is run by a client having identity $ID \in \{0,1\}^*$ and signing key $\mathbf{u}_{ID}$ to produce a signature $\theta = Sign(\mathsf{Mg})$. A verifier runs Signature Verification on input $(Mpk, \mathsf{Mg}, \theta, ID)$ to validate the correctness of the signature θ. A computationally binding and statistically hiding commitment scheme commit is employed in our Mul-IBS.

Protocol 1. Mul-IBS

Setup(1^κ)*: The secret key generator* SKG *runs the algorithm* Key Gen *on input* 1^κ *for the underlying MQ based signature scheme in order to generate master public key* $Mpk = \mathcal{P} = S \circ F \circ T : \mathbb{F}_q^n \to \mathbb{F}_q^m$ *and master secret key* $Msk = \{S, F, T\}$.

Extract(Msk, ID)*: Given* Msk *and an identity* $ID \in \{0,1\}^*$ *of an user, the* SKG

1. *derives* $\mathbf{k}_{ID} \in \mathbb{F}_q^m$ *by computing* $\mathsf{Hash}(ID) = \mathbf{k}_{ID}$ *for some cryptographically secure collision-resistant hash function* Hash*,*
2. *evaluates* $\mathbf{u}_{ID} = \mathcal{P}^{-1}(\mathbf{k}_{ID}) \in \mathbb{F}_q^n$ *using* $Msk = \{S, F, T\}$*,*
3. *sends* $\mathbf{u}_{ID}$ *as the secret key to the user with identity* ID*.*

Signature Generation($\mathbf{u}_{ID}, \mathsf{Mg}$)*: The user with identity* ID *makes a signature over a message* $\mathsf{Mg} \in \{0,1\}^*$ *with the signing key* $\mathbf{u}_{ID}$ *as follows:*

1. *Computes* $\mathbf{a} = \mathsf{Hash}_1(\mathcal{P}||\mathsf{Mg})$ *using cryptographically secure collision resistant hash function* Hash_1*.*
2. *Selects* $\mathbf{f}_{0,1}, \ldots, \mathbf{f}_{0,\alpha}, \mathbf{g}_{0,1}, \ldots, \mathbf{g}_{0,\alpha}, \in_R \mathbb{F}_q^n, \mathbf{h}_{0,1}, \ldots, \mathbf{h}_{0,\alpha} \in_R \mathbb{F}_q^m$ *and for* $j = 1, \ldots, \alpha$*,*
   (a) *writes* $\mathbf{f}_{1,j} = \mathbf{u}_{ID} - \mathbf{f}_{0,j}$*,*
   (b) *evaluates* $\beta_{0,j} = \mathsf{Commit}(\mathbf{f}_{0,j}, \mathbf{g}_{0,j}, \mathbf{h}_{0,j})$*,* $\beta_{1,j} = \mathsf{Commit}(\mathbf{f}_{1,j}, \mathcal{G}(\mathbf{g}_{0,j}, \mathbf{f}_{1,j}) + \mathbf{h}_{0,j})$*.*
3. *Sets* $\mathsf{COMM} = (\beta_{0,1}, \beta_{1,1}, \ldots, \beta_{0,\alpha}, \beta_{1,\alpha})$
4. *Computes challenges* $\mathsf{Hash}_2(\mathbf{a}||\mathsf{COMM}) = (\delta_1, \ldots, \delta_\alpha) \in \mathbb{F}_q^\alpha$ *for cryptographically secure collision resistant hash function* Hash_2*.*
5. *Evaluates* $\mathbf{g}_{1,j} = \delta_j \mathbf{f}_{0,j} - \mathbf{g}_{0,j}$ *and* $\mathbf{h}_{1,j} = \delta_j \mathcal{P}(\mathbf{f}_{0,j}) - \mathbf{h}_{0,j}$ *for* $j = 1, \ldots, \alpha$*.*
6. *Writes* $\mathsf{Res}_1 = (\mathbf{g}_{1,1}, \mathbf{h}_{1,1} \ldots, \mathbf{g}_{1,\alpha}, \mathbf{h}_{1,\alpha})$*.*
7. *Computes challenges* $\mathsf{Hash}_3(\mathbf{a}||\mathsf{COMM}||\mathsf{Res}_1) = (\gamma_1, \ldots, \gamma_\alpha) \in \{0,1\}^\alpha$ *using cryptographically secure collision resistant hash function* Hash_3*.*
8. *Sets* $\mathsf{Res}_2 = (\mathbf{f}_{\gamma_1,1} \ldots, \mathbf{f}_{\gamma_\alpha,\alpha})$*.*
9. *Outputs the signature as* $\theta = Sign(\mathsf{Mg}) = (\mathsf{COMM}, \mathsf{Res}_1, \mathsf{Res}_2)$*.*

Length of the signature is $2\alpha \cdot |\mathsf{Commitment}| + \alpha \cdot (m + 2n)$ $\mathbb{F}_q$ elements*.*

Signature Verification($Mpk, \mathsf{Mg}, \theta = Sign(\mathsf{Mg}), ID$)*: The verifier performs the following steps to check the validity of the message-signature pair* $(\mathsf{Mg}, Sign(\mathsf{Mg}))$ *with respect to the user with identity* ID *:*

1. *Computes* $\mathsf{Hash}(ID) = \mathbf{k}_{ID}$*.*
2. *Evaluates* $\mathbf{a} = \mathsf{Hash}_1(\mathcal{P}||\mathsf{Mg})$ *and derives challenges* $(\delta_1, \ldots, \delta_\alpha) = \mathsf{Hash}_2(\mathbf{a}||\mathsf{COMM}) \in \mathbb{F}_q^\alpha$ *and* $(\gamma_1, \ldots, \gamma_\alpha) = \mathsf{Hash}_3(\mathbf{a}||\mathsf{COMM}||\mathsf{Res}_1) \in \{0,1\}^\alpha$ *utilizing* $\mathbf{a}$*,* COMM *and* Resp_1*.*
3. *Parses* COMM *into* $(\beta_{0,1}, \beta_{1,1}, \ldots, \beta_{0,\alpha}, \beta_{1,\alpha})$*,* Res_1 *into* $(\mathbf{g}_{1,1}, \mathbf{h}_{1,1} \ldots, \mathbf{g}_{1,\alpha}, \mathbf{h}_{1,\alpha})$ *and* Res_2 *into* $(\mathbf{f}_{\gamma_1,1}, \ldots, \mathbf{f}_{\gamma_\alpha,\alpha})$*.*

4. *In order to check that* $\mathbf{f}_{\gamma_j,j}$ *is correct response to* γ_j *with respect to* COMM, $\mathbf{g}_{1,j}$ *and* $\mathbf{h}_{1,j}$, *verifies the following equalities for each* $j = 1, \ldots, \alpha$*:*

   (a) *if* $\gamma_j = 0$ *then*

$$\beta_{0,j} \stackrel{?}{=} \mathsf{Commit}(\mathbf{f}_{\gamma_j,j}, \delta_j \mathbf{f}_{\gamma_j,j} - \mathbf{g}_{1,j}, \delta_j \mathcal{P}(\mathbf{f}_{\gamma_j,j}) - \mathbf{h}_{1,j})$$

   (b) *for* $\gamma_j = 1$,

$$\beta_{1,j} \stackrel{?}{=} \mathsf{Commit}(\mathbf{f}_{\gamma_j,j}, \delta_j(\mathbf{k}_{ID} - \mathcal{P}(\mathbf{f}_{\gamma_j,j}) + \mathcal{P}(\mathbf{0})) - \mathcal{G}(\mathbf{g}_{1,j}, \mathbf{f}_{\gamma_j,j}) - \mathbf{h}_{1,j})$$

5. *The message-signature pair* $(\mathsf{Mg}, \theta = Sign(\mathsf{Mg}))$ *is accepted i.e.,* Signature Verification$(Mpk, \mathsf{Mg}, \theta = Sign(\mathsf{Mg}), ID) = 1$ *if all the equalities hold, otherwise rejected i.e.,* Signature Verification$(Mpk, \mathsf{Mg}, \theta = Sign(\mathsf{Mg}), ID) = 0$.

Correctness: We now give the correctness of the Mul-IBS by proving that the following equalities in the step 4 of Signature Verification algorithm hold:

$$\begin{aligned} &\text{for } \gamma_j = 0, \\ &\beta_{0,j} = \mathsf{Commit}(\mathbf{f}_{\gamma_j,j}, \delta_j \mathbf{f}_{\gamma_j,j} - \mathbf{g}_{1,j}, \delta_j \mathcal{P}(\mathbf{f}_{\gamma_j,j}) - \mathbf{h}_{1,j}) \end{aligned} \tag{4.1}$$

$$\begin{aligned} &\text{for } \gamma_j = 1, \\ &\beta_{1,j} = \mathsf{Commit}(\mathbf{f}_{\gamma_j,j}, \delta_j(\mathbf{k}_{ID} - \mathcal{P}(\mathbf{f}_{\gamma_j,j}) + \mathcal{P}(\mathbf{0})) - \mathcal{G}(\mathbf{g}_{1,j}, \mathbf{f}_{\gamma_j,j}) - \mathbf{h}_{1,j}), \end{aligned} \tag{4.2}$$

where $j = 1, \ldots, \alpha$. Let us consider the following two cases:

- **Case I:** Suppose $\gamma_j = 0$. Then $\mathbf{f}_{\gamma_j,j} = \mathbf{f}_{0,j}$. Therefore, $\delta_j \mathbf{f}_{\gamma_j,j} - \mathbf{g}_{1,j} =, \delta_j \mathbf{f}_{0,j} - \mathbf{g}_{1,j} = \mathbf{g}_{0,j}$ and $\delta_j \mathcal{P}(\mathbf{f}_{\gamma_j,j}) - \mathbf{h}_{1,j} = \delta_j \mathcal{P}(\mathbf{f}_{0,j}) - \mathbf{h}_{1,j} = \mathbf{h}_{0,j}$.

  Hence we may conclude that for each $j = 1, \ldots, \alpha$, the equation 4.1 holds.

- **Case II:** Let $\gamma_j = 1$. Then $\mathbf{f}_{\gamma_j,j} = \mathbf{f}_{1,j}$. Therefore

$$\begin{aligned} &\delta_j(\mathbf{k}_{ID} - \mathcal{P}(\mathbf{f}_{\gamma_j,j}) + \mathcal{P}(\mathbf{0})) - \mathcal{G}(\mathbf{g}_{1,j}, \mathbf{f}_{\gamma_j,j}) - \mathbf{h}_{1,j} \\ &= \delta_j(\mathcal{P}(\mathbf{u}_{ID}) - \mathcal{P}(\mathbf{f}_{1,j}) + \mathcal{P}(\mathbf{0})) - \mathcal{G}(\mathbf{g}_{1,j}, \mathbf{f}_{1,j}) - \mathbf{h}_{1,j} \\ &= \delta_j(\mathcal{P}(\mathbf{f}_{0,j} + \mathbf{f}_{1,j}) - \mathcal{P}(\mathbf{f}_{1,j}) + \mathcal{P}(\mathbf{0})) - \mathcal{G}(\mathbf{g}_{1,j}, \mathbf{f}_{1,j}) - \mathbf{h}_{1,j} \text{ since } \mathbf{u}_{ID} = \mathbf{f}_{0,j} + \mathbf{f}_{1,j} \\ &= \delta_j(\mathcal{P}(\mathbf{f}_{0,j}) + \mathcal{G}(\mathbf{f}_{0,j}, \mathbf{f}_{1,j})) - \mathcal{G}(\mathbf{g}_{1,j}, \mathbf{f}_{1,j}) - \mathbf{h}_{1,j} \\ &= \mathcal{G}(\delta_j \mathbf{f}_{0,j} - \mathbf{g}_{1,j}, \mathbf{f}_{1,j}) + \delta_j \mathcal{P}(\mathbf{f}_{0,j}) - \mathbf{h}_{1,j} \\ &= \mathcal{G}(\mathbf{g}_{0,j}, \mathbf{f}_{1,j}) + \mathbf{h}_{0,j} \end{aligned}$$

Thus for each $j = 1, \ldots, \alpha$, the equation 4.2 holds.

5 Security

Theorem 5.1. *The proposed* Mul-IBS *is uf-cma secure in the random oracle model under the hardness of MQ problem, if*

(i) the commitment scheme Commit *is computationally binding and perfectly hiding,*

ii) the hash functions Hash, Hash_1, Hash_2 *and* Hash_3 *are designed as random oracles.*

Proof: We now show that the proposed Mul-IBS possesses uf-cma security under the hardness of the MQ assumption by the method of contradiction. Let us consider a forger FG with non-negligible success probability in the uf-cma game for Mul-IBS. We will prove that it is possible to design an oracle machine $\mathcal{O}^{\mathsf{FG}}$ for solving the MQ problem by using FG and managing outputs of the random oracles Hash, Hash_1, Hash_2 and Hash_3 in a series of games $\mathbf{Game}_0, \ldots, \mathbf{Game}_6$. Here $\mathbf{Game}_i$ slightly modifies $\mathbf{Game}_{i-1}$ for $i = 1, \ldots, 6$. In the game $\mathbf{Game}_i$, $\mathsf{Prob}[\mathbf{Game}_i]$ is considered as FG's success probability FG.

$\mathbf{Game}_0$: $\mathbf{Game}_0$ corresponds to uf-cma game for Mul-IBS. Thereby, $\mathsf{Adv}_{\mathsf{FG}}^{\mathsf{Ex}^{\text{uf-cma}}_{Mul\text{-}IBS(1^\kappa)}} = \mathsf{Prob}[\mathsf{Ex}^{\text{uf-cma}}_{Mul\text{-}IBS(1^\kappa)} = 1] = \mathsf{Prob}[\mathbf{Game}_0]$

$\mathbf{Game}_1$: It is identical to $\mathbf{Game}_0$, except that during $\mathsf{Extract\text{-}query}$, $\mathcal{O}^{\mathsf{FG}}$ substitutes the output of the random oracle Hash query of $ID \in \{0,1\}^*$ by $\mathbf{k} = P(\mathbf{u}) \in \mathbb{F}_q^m$ and the corresponding secret key by $\mathbf{u}$ for randomly chosen $\mathbf{u} \in \mathbb{F}_q^n$. Note that if $|\mathsf{Prob}[\mathbf{Game}_1] - \mathsf{Prob}[\mathbf{Game}_0]|$ is non-negligible then FG can be utilized for distinguishing Hash's output distributions, which is impossible. Consequently, there exists negligible function $\epsilon_1(\kappa)$ such that $|\mathsf{Prob}[\mathbf{Game}_1] - \mathsf{Prob}[\mathbf{Game}_0]| = \epsilon_1(\kappa)$.

$\mathbf{Game}_2$: $\mathbf{Game}_2$ is analogues to $\mathbf{Game}_1$ apart from the fact that during $\mathsf{Sign\text{-}query}$, the oracle $\mathcal{O}^{\mathsf{FG}}$ replaces the output of Hash of $ID \in \{0,1\}^*$ by $\mathbf{k} = P(\mathbf{u}) \in \mathbb{F}_q^m$ and the signature by σ which is generated using secret key $\mathbf{u}$ for the system $\mathbf{k} = P(\mathbf{u})$. Note that one may use FG for distinguishing Hash's distributions if $|\mathsf{Prob}[\mathbf{Game}_2] - \mathsf{Prob}[\mathbf{Game}_1|$ is non-negligible. This is impossible. As a consequence, $|\mathsf{Prob}[\mathbf{Game}_2] - \mathsf{Prob}[\mathbf{Game}_1]| = \epsilon_2(\kappa)$, where $\epsilon_2(\kappa)$ is a negligible function.

$\mathbf{Game}_3$: It is equivalent to $\mathbf{Game}_2$ excepting $\mathcal{O}^{\mathsf{FG}}$ substitutes Hash_1's output by randomly chosen bit-string. Note that one may use FG for distinguishing Hash_1's distributions if $|\mathsf{Prob}[\mathbf{Game}_3] - \mathsf{Prob}[\mathbf{Game}_2|$ is non-negligible. This is impossible. Note that if $|\mathsf{Prob}[\mathbf{Game}_3] - \mathsf{Prob}[\mathbf{Game}_2]|$ is non-negligible then FG may be utilized for distinguishing Hash_1's output distributions, which is impossible. Thus there exists negligible function $\epsilon_3(\kappa)$ such that $|\mathsf{Prob}[\mathbf{Game}_3] - \mathsf{Prob}[\mathbf{Game}_2]| = \epsilon_3(\kappa)$.

$\mathbf{Game}_4$: $\mathbf{Game}_4$ is identical to $\mathbf{Game}_3$ apart from the fact that $\mathcal{O}^{\mathsf{FG}}$ replaces Hash_2's output by randomly selected element from $\mathbb{F}_q^\alpha$. Note that one can utilize FG for distinguishing Hash_2's distributions if $|\mathsf{Prob}[\mathbf{Game}_4] - \mathsf{Prob}[\mathbf{Game}_3|$ is non-negligible. This is impossible. Thereby, for some non-negligible function $\epsilon_4(\kappa)$, we can write $|\mathsf{Prob}[\mathbf{Game}_4] - \mathsf{Prob}[\mathbf{Game}_3]| = \epsilon_4(\kappa)$.

$\mathbf{Game}_5$: It is analogues to $\mathbf{Game}_4$ excepting $\mathcal{O}^{\mathsf{FG}}$ substitutes Hash_3's output by randomly chosen α-length bit-string. Note that if $|\mathsf{Prob}[\mathbf{Game}_5] - \mathsf{Prob}[\mathbf{Game}_4]|$ is non-negligible then FG can be utilized for distinguishing Hash_3's output distributions, which is impossible. As a consequence, there exists some negligible function $\epsilon_5(\kappa)$ such that $|\mathsf{Prob}[\mathbf{Game}_5] - \mathsf{Prob}[\mathbf{Game}_4]| = \epsilon_5(\kappa)$.

$\mathbf{Game}_6$: $\mathbf{Game}_2$ identical to $\mathbf{Game}_5$ excepting $\mathcal{O}^{\mathsf{FG}}$ replaces Hash query on ID^* using randomly chosen $\mathbf{k}^* \in \mathbb{F}_q^m$, the output of Hash_1 by randomly selected bit-string, Hash_2's output by randomly chosen element from $\mathbb{F}_q^\alpha$ and Hash_3's using α-length randomly selected

bit-string. We can argue that $|\mathsf{Prob}[\mathbf{Game}_6] - \mathsf{Prob}[\mathbf{Game}_5]| = \epsilon_6(\kappa)$ (negligible function) by taking into account the arguments of $\mathbf{Game}_2$, $\mathbf{Game}_3$, $\mathbf{Game}_4$ and $\mathbf{Game}_5$, we can argue that $|\mathsf{Prob}[\mathbf{Game}_6] - \mathsf{Prob}[\mathbf{Game}_5]| = \epsilon_6(\kappa)$ for some negligible function $\epsilon_6(\kappa)$.

Therefore,

$$\begin{aligned}
&|\mathsf{Prob}[\mathbf{Game}_6] - \mathsf{Prob}[\mathsf{Ex}^{\text{uf-cma}}_{Mul\text{-}IBS(1^\kappa)} = 1]| = |\mathsf{Prob}[\mathbf{Game}_6] - \mathsf{Prob}[\mathbf{Game}_0]| \\
&\leq |\mathsf{Prob}[\mathbf{Game}_6] - \mathsf{Prob}[\mathbf{Game}_5]| + |\mathsf{Prob}[\mathbf{Game}_5] - \mathsf{Prob}[\mathbf{Game}_4]| \\
&+|\mathsf{Prob}[\mathbf{Game}_4] - \mathsf{Prob}[\mathbf{Game}_3]| + |\mathsf{Prob}[\mathbf{Game}_3] - \mathsf{Prob}[\mathbf{Game}_2]| \\
&+|\mathsf{Prob}[\mathbf{Game}_2] - \mathsf{Prob}[\mathbf{Game}_1]| + |\mathsf{Prob}[\mathbf{Game}_1] - \mathsf{Prob}[\mathbf{Game}_0]| \\
&= \epsilon_6(\kappa) + \epsilon_5(\kappa) + \epsilon_4(\kappa) + \epsilon_3(\kappa) + \epsilon_2(\kappa)\epsilon_1(\kappa) = \rho(\kappa)(\text{negligible function})),
\end{aligned}$$

Thereby, $\mathsf{Adv}^{\mathsf{Ex}^{\text{uf-cma}}_{Mul\text{-}IBS(1^\kappa)}}_{\mathsf{FG}} = \mathsf{Prob}[\mathsf{Ex}^{\text{uf-cma}}_{Mul\text{-}IBS(1^\kappa)} = 1]$ is identical to $\mathsf{Prob}[\mathbf{Game}_6]$ of FG in the game $\mathbf{Game}_6$. Hence, $\mathsf{Adv}^{\mathsf{Ex}^{\text{uf-cma}}_{Mul\text{-}IBS(1^\kappa)}}_{\mathsf{FG}}$ is non-negligible implies $\mathsf{Prob}[\mathbf{Game}_6]$ non-negligible.

If possible let $\mathsf{Prob}[\mathbf{Game}_6]$ be non-negligible. We now prove that $\mathcal{O}^{\mathsf{FG}}$ can easily solve the MQ problem by finding a solution $\mathbf{u}^*$ of the system $\mathbf{k}^* = P(\mathbf{x})$ with the help FG.

1. The oracle machine $\mathcal{O}^{\mathsf{FG}}$ generates four valid transcripts $(\mathsf{COMM}, \Delta^{(i)}, \mathsf{Res}_1^{(i)}, \Gamma^{(j)}, \mathsf{Res}_2^{(i,j)})_{\{i,j=0,1\}}$ with the help of FG and controlling the output of random oracles Hash, Hash_1, Hash_2 and Hash_3, where

$$\begin{aligned}
&\mathsf{COMM} = (\beta_{0,1}, \beta_{1,1}, \ldots, \beta_{0,\alpha}, \beta_{1,\alpha}) \\
&\Delta^{(i)} = \{\delta_1^{(i)}, \ldots, \delta_\alpha^{(i)}\} \text{ with } \delta_l^{(0)} \neq \delta_\alpha^{(1)} \text{ for } l = 1, \ldots, \alpha \\
&\mathsf{Res}_1^{(i)} = (\mathbf{g}_{1,1}^{(i)}, \mathbf{h}_{1,1}^{(i)}, \ldots, \mathbf{g}_{1,\alpha}^{(i)}, \mathbf{h}_{1,\alpha}^{(i)}) \\
&\Gamma^{(j)} = (\gamma_1^{(j)}, \ldots, \gamma_\alpha^{(j)}) \text{ with } \gamma_l^{(j)} = j \in \{0,1\} \text{ for } l = 1, \ldots, \alpha \\
&\mathsf{Res}_2^{(i,j)} = (\mathbf{f}_{j,1}^{(i)}, \ldots, \mathbf{f}_{j,\alpha}^{(i)})
\end{aligned}$$

2. Note that for $l = 1, \ldots, \alpha$,

$$\begin{aligned}
\beta_{0,l} &= \mathsf{Commit}\left(\mathbf{f}_{0,l}^{(0)},\ \delta_l^{(0)}\mathbf{f}_{0,l}^{(0)} - \mathbf{g}_{1,l}^{(0)},\ \delta_l^{(0)}\mathcal{P}(\mathbf{f}_{0,l}^{(0)}) - \mathbf{h}_{1,l}^{(0)}\right) \\
&= \mathsf{Commit}\left(\mathbf{f}_{0,l}^{(1)},\ \delta_l^{(1)}\mathbf{f}_{0,l}^{(1)} - \mathbf{g}_{1,l}^{(1)},\ \delta_l^{(1)}\mathcal{P}(\mathbf{f}_{0,l}^{(1)}) - \mathbf{h}_{1,\rho}^{(1)}\right) \qquad (5.1) \\
\beta_{1,l} &= \mathsf{Commit}\left(\mathbf{f}_{1,l}^{(0)},\ \delta_l^{(0)}(\mathbf{k}^* - \mathcal{P}(\mathbf{f}_{1,l}^{(0)}) + \mathcal{P}(\mathbf{0})) - \mathcal{G}(\mathbf{g}_{1,l}^{(0)}, \mathbf{f}_{1,l}^{(0)}) - \mathbf{h}_{1,l}^{(0)}\right) \\
&= \mathsf{Commit}\left(\mathbf{f}_{1,l}^{(1)},\ \delta_l^{(1)}(\mathbf{k}^* - \mathcal{P}(\mathbf{f}_{1,l}^{(1)}) + \mathcal{P}(\mathbf{0})) - \mathcal{G}(\mathbf{g}_{1,l}^{(1)}, \mathbf{f}_{1,l}^{(1)}) - \mathbf{h}_{1,l}^{(1)}\right) \qquad (5.2)
\end{aligned}$$

3. Using the computationally binding property of the commitment scheme Comit, we argue that the arguments of Commit for $\beta_{0,l}$ are equal in 5.2. Similarly, the arguments of Commit

for $\beta_{1,l}$ are equal in 5.2 due to the binding property of Commit. Thus, we have

$$\mathbf{f}_{0,l}^{(0)} = \mathbf{f}_{0,l}^{(1)} \tag{5.3}$$

$$\delta_l^{(0)}\mathbf{f}_{0,l}^{(0)} - \mathbf{g}_{1,l}^{(0)} = \delta_l^{(1)}\mathbf{f}_{0,l}^{(1)} - \mathbf{g}_{1,l}^{(1)} \tag{5.4}$$

$$\delta_l^{(0)}\mathcal{P}(\mathbf{f}_{0,l}^{(0)}) - \mathbf{h}_{1,l}^{(0)} = \delta_l^{(1)}\mathcal{P}(\mathbf{f}_{0,l}^{(1)}) - \mathbf{h}_{1,l}^{(1)} \tag{5.5}$$

$$\mathbf{f}_{1,l}^{(0)} = \mathbf{f}_{1,l}^{(1)} \tag{5.6}$$

$$\begin{aligned}&\delta_l^{(0)}(\mathbf{k}^* - \mathcal{P}(\mathbf{f}_{1,l}^{(0)}) + \mathcal{P}(\mathbf{0})) - \mathcal{G}(\mathbf{g}_{1,l}^{(0)}, \mathbf{f}_{1,l}^{(0)}) - \mathbf{h}_{1,l}^{(0)} \\ &= \delta_l^{(1)}(\mathbf{k}^* - \mathcal{P}(\mathbf{f}_{1,l}^{(1)}) + \mathcal{P}(\mathbf{0})) - \mathcal{G}(\mathbf{g}_{1,l}^{(1)}, \mathbf{f}_{1,l}^{(1)}) - \mathbf{h}_{1,l}^{(1)}\end{aligned} \tag{5.7}$$

4. From the equations 5.6 and 5.7,

$$\begin{aligned}&(\delta_l^{(0)} - \delta_l^{(1)})(\mathbf{k}^* - \mathcal{P}(\mathbf{f}_{1,l}^{(0)}) + \mathcal{P}(\mathbf{0})) = \mathcal{G}(\mathbf{g}_{1,l}^{(0)}, \mathbf{f}_{1,l}^{(0)}) - \mathcal{G}(\mathbf{g}_{1,l}^{(1)}, \mathbf{f}_{1,l}^{(1)}) + \mathbf{h}_{1,l}^{(0)} - \mathbf{h}_{1,l}^{(1)} \\ &\Rightarrow (\delta_l^{(0)} - \delta_l^{(1)})(\mathbf{k}^* - \mathcal{P}(\mathbf{f}_{1,\rho}^{(0)}) + \mathcal{P}(\mathbf{0})) = \mathcal{G}(\mathbf{g}_{1,l}^{(0)} - \mathbf{g}_{1,l}^{(1)}, \mathbf{f}_{1,l}^{(0)}) + \mathbf{h}_{1,l}^{(0)} - \mathbf{h}_{1,l}^{(1)}\end{aligned} \tag{5.8}$$

5. From 5.3, 5.4, 5.5 and 5.8

$$\begin{aligned}&(\delta_l^{(0)} - \delta_l^{(1)})(\mathbf{k}^* - \mathcal{P}(\mathbf{f}_{1,l}^{(0)}) + \mathcal{P}(\mathbf{0})) = \mathcal{G}((\delta_l^{(0)} - \delta_l^{(1)})\mathbf{f}_{0,l}^{(0)}, \mathbf{f}_{1,l}^{(0)}) + (\delta_l^{(0)} - \delta_l^{(1)})\mathcal{P}(\mathbf{f}_{0,l}^{(0)}) \\ &\Rightarrow \mathbf{k}^* - \mathcal{P}(\mathbf{f}_{1,l}^{(0)}) + \mathcal{P}(\mathbf{0}) = \mathcal{G}(\mathbf{f}_{0,l}^{(0)}, \mathbf{f}_{1,l}^{(0)}) + \mathcal{P}(\mathbf{f}_{0,l}^{(0)}) \text{ since } \delta_l^{(0)} \neq \delta_l^{(1)} \\ &\Rightarrow \mathbf{k}^* = \mathcal{P}(\mathbf{f}_{1,l}^{(0)}) + \mathcal{G}(\mathbf{f}_{0,l}^{(0)}, \mathbf{f}_{1,l}^{(0)}) + \mathcal{P}(\mathbf{f}_{0,l}^{(0)}) - \mathcal{P}(\mathbf{0}) \\ &\qquad = \mathcal{P}(\mathbf{f}_{0,l}^{(0)} + \mathbf{f}_{1,l}^{(0)})\end{aligned}$$

6. Hence, the oracle machine $\mathcal{O}^{\mathsf{FG}}$ extracts a solution $\mathbf{f}_{0,l}^{(0)} + \mathbf{f}_{1,l}^{(0)}$ of $\mathbf{k}^* = \overline{\mathcal{P}}(x)$

Thus, $\mathsf{Prob}[\mathbf{Game}_6]$ is non-negligible implies $\mathcal{O}^{\mathsf{FG}}$ is able to determine a solution of the MQ problem $\mathbf{k}^* = \overline{\mathcal{P}}(x)$. It contradicts the assumption that MQ problem is NP-hard. Consequently, $\mathsf{Prob}[\mathbf{Game}_6]$ is negligible, which ensures $\mathsf{Adv}_{\mathsf{FG}}^{\mathsf{Ex}^{\text{uf-cma}}_{Mul\text{-}IBS(1^\kappa)}} = \mathsf{Prob}[\mathsf{Ex}^{\text{uf-cma}}_{Mul\text{-}IBS(1^\kappa)} = 1]$ is negligible. Therefore, we conclude that the proposed Mul-IBS is uf-cma secure. ■

6 Efficiency Analysis

In this part, we discuss the communication, storage and computation complexity of our scheme. Size of Mpk and Msk are respectively $\frac{m(n+2)(n+1)}{2}$ and n^2+m^2+c field ($\mathbb{F}_q$) elements, C being the size of the central map. User's identity and secret key sizes are m and n field ($\mathbb{F}_q$) elements respectively. Moreover, the signature size is 2α $|commitment|+$ $\alpha(m+2n)$-$\mathbb{F}_q$ elements. The round complexity of our scheme is 2, one for Extract algorithm to send the user's secret key and one for Signature Generation algorithm to send the signature.

The signer evaluates the system P 3α times for the computation of G in $\beta_{1,j}$ and α times for the computation of $\mathbf{h}_{1,j}$. While, the verifier need to compute the system P around $(1+4)\alpha/2$ i.e.,

2.5α times. Thus, total number of executions of the system P is approximately 6.5α. To evaluate the system P, one has to perform $m(n^4+n)$ modulo multiplications. Therefore, we require total $\alpha(n^4+n)$ modulo multiplications for signature generation and signature verification.

We direct to Table 1 for a comparative summary of proposed design with multivariate IBS in the current state of art in terms of signature size, master public key (verification key) size, signer's secret key size, user's identity size, and master secret key size for 128-bit security level over $GF(256)$. Let us write Mul-IBS-Rainbow (q, v, o_1, o_2, α) for denoting that Rainbow with parameter (q, v, o_1, o_2, α) is used in our scheme and Mul-IBS-UOV (q, o, v, α) for denoting that UOV with parameter (q, o, v, α) is used in our scheme. Here, α denotes the number of rounds. By using the result stated in Section 3.2, we may choose the number of rounds for a 128-bit security level over $GF(256)$ as 129. We follow [18] for selecting parameters of the underlying signature in our scheme. While, for the existing schemes [4, 13, 25], we follow their respective parameter representations. We instantiate the output lengths of the commitment scheme and with SHA3-256 in our Mul-IBS. However, to reduce the signature size, one may use a weaker commitment scheme.

Table 1 : Comparison for 128-bit security level over $GF(256)$

Scheme	Mpk size(kB)	Msk size (kB)	signature size(kB)	user's secret key size(kB)	uf-cma security
IBUOV[25] $(256, 45, 90)$	409.4	381.8	714.4	942.2	×
IBS-Rainbow[13] $(256, 40, 24, 24)$	187.7	140.0	395.7	431.7	✓
ID-UOV[4] $(256, 48, 96, 8)$	51200	4770.1	0.1	596.3	×
ID-Rainbow [4] $(256, 28, 20, 20, 8)$	46694.4	551.8	0.1	70	×
Mul-IBS-UOV $(256, 45, 90, 129)$	409.4	363.9	47.7	0.1	✓
Mul-IBS-Rainbow $(256, 36, 28, 15, 129)$	136.1	90.9	33.4	0.1	✓

We compare the time complexity of Mul-IBS in terms of signature generation and verification time for 80-bit security level over the field $GF(256)$. We implemented Mul-IBS in SageMath. The hardware configuration is a workspace with an Intel Core i7-8700 3.20GHz processor with 8GB of RAM and a 64-bit operating system. We make use of Rainbow with parameters $(256, 18, 17, 9)$ [18] as the underlying multivariate signature scheme. Results are summarized in Table 2.

Table 2 : Comparison of time complexity for 80-bit security level over $GF(256)$

Scheme and Parameters	Signature Generation (ms)	Verification (ms)
ID-UOV (256,26,52, 5) [4]	183	301
ID-Rainbow (256, 14, 14, 20, 5) [4]	54	366
Mul-IBS-Rainbow (256, 18,17,9)	47.7	30.5

7 Application of Mul-IBS in IoT-Based NDN Architecture

In this section, we will see how Mul-IBS can be employed in IoT-based NDN architecture to prevent content poisoning attacks. First, we briefly describe the content poisoning attack (refer to Figure 3). Let Michael be a client who is interested in some content, say Γ. His interest

request (shown by black arrow) is transferred to the original publisher of the content. Due to the LCE caching policy, the response sent by the publisher (indicated by green color) is cached by the intermediate routers for future use (here Router-D, Router-E, and Router-C). Suppose an adversary takes charge of the Router-C and introduces poisoned content with a counterfeit signature. Suppose another user, John, tied up with Router-C, exhibits interest (shown by yellow color) for Γ. In that case, the local router (Router-C) will serve the interest of John instead of forwarding it again to the publisher. But since the content cached in Router-C is poisoned, John will receive the maligned copy of Γ. In addition to that, Router-A and Router-B will also store the poisonous content due to the LCE caching policy of NDN.

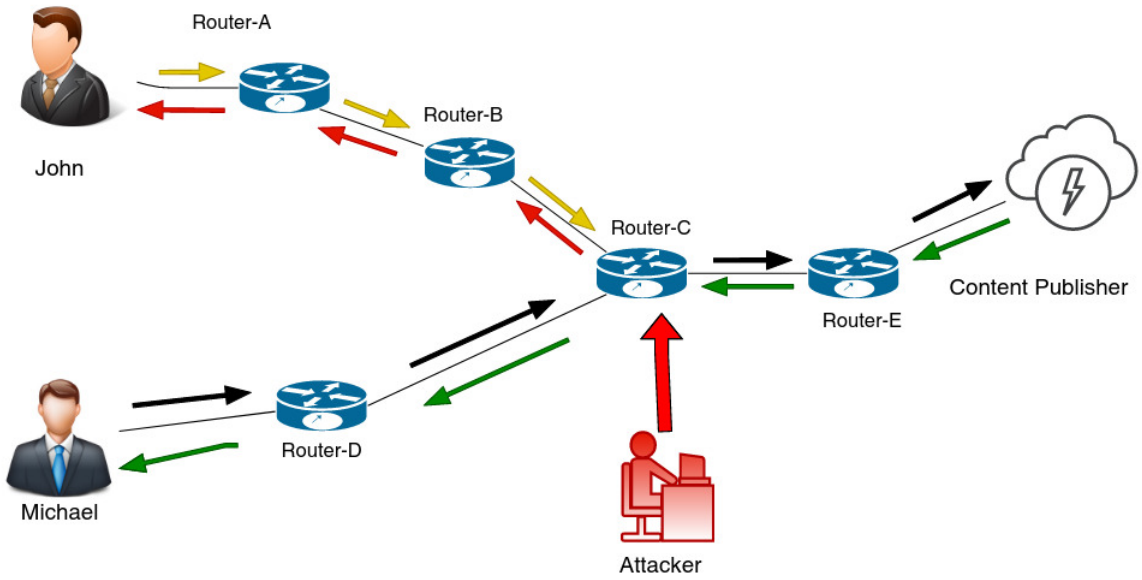

Figure 3 : Content Poisoning Attack in IoT-Based NDN Systems

Now we will see how Mul-IBS can be employed in IoT-based NDN architecture to prevent content poisoning attacks. In the first step, content providers and users submit their identities to the network executive to complete the registration process. Network-executive generates public and secret keys for the users and providers using Extract. Suppose a user named Michael displays his interest in some content, say Δ. As soon as the interest request is received, routers in NDN dispatch the particular interest to the content publisher. After receiving the interest, the content provider uses a cryptographically secure hash like SHA3-256 on Δ to get the checksum (chk). In the following, the content publisher uses his private key to generate a digital signature for chk with the help of the algorithm Signature Generation. After that, the requested content is distributed to the user along with the signature sign-chk and checksum chk of the provider. NDN architecture follows a leave copy everywhere (LCE) caching policy. Therefore, content requested by Michael, i.e. Δ is stored in caches of Router-C, Router-D, and Router-E.

Now imagine a situation where an attacker $\mathcal{Z}$ poisoned Δ in Router-C. Suppose John also displays his interest for Δ and his interest request is obtained at Router-C. Since at Router-C, Δ is already poisoned by $\mathcal{Z}$, a poisoned copy will be received by John. If John wants to ensure whether he has received the right content or not, he proceeds as follows. First, he asks the network executive for the original provider's public key. With the help of the public key of the broadcaster, John attempts to verify the signature sign-chk using Signature Verification. If the Signature Verification outputs 1, then John concludes that the content provider is registered

with NE and hence authentic.

Post authentication, if John wishes to confirm the integrity of Δ, he uses secure hash SHA3-256 on Δ to obtain chk_1. If chk is equal to chk_1, John concludes that received content Δ is not poisoned. In case chk is not equal to chk_1, John concludes that content has been poisoned. To remove the poisoned content from the network, John proceeds as follows. Using a secure multivariate encryption scheme like ABC [27], and the public key of the original content publisher, John encrypts the poisoned Δ and chk_1 and dispatch it to the publisher. Broadcaster decrypts with the help of his private key and compares $\mathsf{chk}, \mathsf{chk}_1$. In the end, the publisher disseminates a message regarding the poisoned content, which is then removed from the caches of the router. Mul-IBS being a very lightweight signature scheme is ideal for IoT systems. It mitigates the threat of content poisoning with solid security guarantees and with modest and inexpensive computing resources. Verifying a signature generated by Mul-IBS requires only doing field multiplications and additions. Due to this low verification overhead, our proposed design addresses the threat of content poisoning with low latency. The lightweight nature of Mul-IBS also ensures that caches remain clean from invalid content. The proposed design Mul-IBS can be utilized as a key cryptographic building block to build a robust and resilient IoT-based NDN architecture. Our scheme is provably secure in the random oracle model. It is built on the hardness assumption of the MQ problem; thus, it also provides safety against attacks by quantum computers. Mul-IBS presents an economical yet efficient solution for resource-constrained IoT networks.

8 Conclusion

In this paper, we constructed a provably secure multivariate IBS, namely Mul-IBS utilizing a secure MPKC signature scheme accompanying a 5-pass identification scheme of [23] as its building blocks. Our construction performs better over the existing multivariate IBS in terms of master public key size, user secret key size, and master secret key size. In contrast to [4, 25], our scheme achieves uf-cma security using random oracles. Mathematical operations used in multivariate cryptographic schemes are elementary. Mainly, addition and multiplications over finite fields are the most used mathematical operations. Hence, Mul-IBS is very fast and inexpensive. The Mul-IBS, being a very lightweight signature scheme, is ideal for IoT systems. It mitigates the threat of content poisoning with strong security guarantees and with modest and inexpensive computing resources. The lightweight nature of Mul-IBS also ensures that caches remain clean from invalid content. The proposed design Mul-IBS can be utilized as a key cryptographic building block to build a robust and resilient IoT-based NDN system.

References

[1] Daniel J Bernstein. Introduction to post-quantum cryptography. In *Post-quantum cryptography*, pages 1–14. Springer, 2009.

[2] Andrey Bogdanov, Thomas Eisenbarth, Andy Rupp, and Christopher Wolf. Time-area optimized public-key engines: $\mathcal{MQ}$-cryptosystems as replacement for elliptic curves? In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 45–61, 2008.

[3] 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. Sse implementation of multivariate pkcs on modern x86 cpus. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 33–48, 2009.

[4] Jiahui Chen, Jie Ling, Jianting Ning, and Jintai Ding. Identity-based signature schemes for multivariate public key cryptosystems. *The Computer Journal*, 62(8):1132–1147, 2019.

[5] Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe. From 5-pass mq-based identification to mq-based signatures. *IACR Cryptology ePrint Archive*, 2016:708, 2016.

[6] Jintai Ding and Dieter Schmidt. Rainbow, a new multivariable polynomial signature scheme. In *International Conference on Applied Cryptography and Network Security*, pages 164–175. Springer, 2005.

[7] Michael R Garey and David S Johnson. *Computers and intractability*, volume 174. freeman San Francisco, 1979.

[8] Shafi Goldwasser, Silvio Micali, and Ronald L Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2):281–308, 1988.

[9] Van Jacobson, Diana K Smetters, James D Thornton, Michael F Plass, Nicholas H Briggs, and Rebecca L Braynard. Networking named content. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies*, pages 1–12, 2009.

[10] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 206–222. Springer, 1999.

[11] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.

[12] David W Kravitz. Digital signature algorithm, July 27 1993. US Patent 5,231,668.

[13] Le Van Luyen et al. An improved identity-based multivariate signature scheme based on rainbow. *Cryptography*, 3(1):8, 2019.

[14] Tsutomu Matsumoto and Hideki Imai. 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, 1988.

[15] Jacques Patarin. 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, 1996.

[16] Jacques Patarin and Louis Goubin. Trapdoor one-way permutations and multivariate polynomials. In *International Conference on Information and Communications Security*, pages 356–368. Springer, 1997.

[17] Kenneth G Paterson and Jacob CN Schuldt. Efficient identity-based signatures secure in the standard model. In *Australasian Conference on Information Security and Privacy*, pages 207–222. Springer, 2006.

[18] Albrecht Petzoldt. *Selecting and reducing key sizes for multivariate cryptography.* PhD thesis, tuprints, 2013.

[19] Albrecht Petzoldt, Ming-Shing Chen, Bo-Yin Yang, Chengdong Tao, and Jintai Ding. Design principles for hfev-based multivariate signature schemes. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 311–334. Springer, 2015.

[20] Jonathan B Postel, Carl A Sunshine, and Danny Cohen. The arpa internet protocol. *Computer Networks (1976)*, 5(4):261–271, 1981.

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

[22] Koichi Sakumoto, Taizo Shirai, and Harunaga Hiwatari. On provable security of uov and hfe signature schemes against chosen-message attack. In *International Workshop on Post-Quantum Cryptography*, pages 68–82. Springer, 2011.

[23] Koichi Sakumoto, Taizo Shirai, and Harunaga Hiwatari. Public-key identification schemes based on multivariate quadratic polynomials. In *Annual Cryptology Conference*, pages 706–723. Springer, 2011.

[24] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Workshop on the theory and application of cryptographic techniques*, pages 47–53. Springer, 1984.

[25] Wuqiang Shen, Shaohua Tang, and Lingling Xu. Ibuov, a provably secure identity-based uov signature scheme. In *2013 IEEE 16th International Conference on Computational Science and Engineering*, pages 388–395. IEEE, 2013.

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

[27] Chengdong Tao, Adama Diene, Shaohua Tang, and Jintai Ding. Simple matrix scheme for encryption. In *International Workshop on Post-Quantum Cryptography*, pages 231–242. Springer, 2013.

[28] Yaoda Xu and Suzanne Corkin. Hm revisits the tower of hanoi puzzle. *Neuropsychology*, 15(1):69, 2001.

[29] Lixia Zhang, Alexander Afanasyev, Jeffrey Burke, Van Jacobson, KC Claffy, Patrick Crowley, Christos Papadopoulos, Lan Wang, and Beichuan Zhang. Named data networking. *ACM SIGCOMM Computer Communication Review*, 44(3):66–73, 2014.