# A Multivariate Based Provably Secure Certificateless Signature Scheme with Applications to the Internet of Medical Things

VIKAS SRIVASTAVA<sup>1</sup> AND SUMIT KUMAR DEBNATH<sup>2,3,\*</sup>

<sup>1</sup>Department of Mathematics, National Institute of Technology Jamshedpur, Jamshedpur-831014, India;

<sup>2</sup> Department of Mathematics, Indian Institute of Information Technology Kalyani, Kalyani-741235, India

<sup>3</sup>Department of Mathematics, National Institute of Technology Jamshedpur, Jamshedpur-831014, India; \* Corresponding author

Email: vikas.math123@gmail.com, sd.iitkgp@gmail.com

Over the last few years, Internet of Medical Things (IoMT) has completely transformed the healthcare industry. It is bringing out the most notable, and unprecedented impacts on human health, and has totally changed the way we look at the healthcare industry. The healthcare sector all around the globe are leapfrogging, and adopting the technology, helping in transforming drastically in a very short span of time. However, as more and more number of medical devices are being connected to IoMT, security issues like ensuring authenticity and integrity of the transmitted data are also on the rise. In view of the context, there is a need of an efficient cryptographic primitive that can address these issues in a viable manner. A signature scheme seems to be the natural choice to mitigate the security concerns. But, traditional signature schemes, both PKI-based and Identity-based have their own disadvantages which makes them unsuitable for IoMT networks. Thus, to address the security issues and problems like certificate management and key escrow, herein, we put forward the *first* multivariate based certificateless signature scheme, namely Mul-CLS, which is built on top of the intractability of multivariate-quadratic (MQ) problem. The fact that multivariate public key cryptosystem (MPKC) provides fast, post-quantum safe, and efficient primitives, makes it a front runner candidate among the other post-quantum cryptography candidates. Our scheme Mul-CLS provides existential unforgeability against chosen message and chosen identity Super Type I and Super Type II adversary if solving the MQ problem is NP-hard. In addition to that, our proposed Mul-CLS presents itself as a robust and cost-friendly cryptographic building block for building IoMT networks.

Keywords: Internet of Medical Things; Certificateless signature; Multivariate public key cryptography; Post-quantum cryptography

#### 1. INTRODUCTION

The Internet of Medical Things (IoMT) is a subcategory of Internet of Things (IoT). It can be thought of as an ecosystem of wirelessly connected medical devices and applications. IoMT technology offers myriads of advantages. To name a few, it can help in reducing the hospital visits as doctors, and other healthcare providers can remotely monitor and assess the patients health. It results in better overall healthcare, and ease of access by enabling doctors to get more connected to their clients. To sum up, with reducing costs, better and easy access to healthcare facilities, remote monitoring of patients, and other numerous benefits, IoMT is having one of the most profound impacts on humankind.

A typical IoMT system comprises huge number of medical devices like wearable biosensors, blood pressure monitor, etc. Devices connected to IoMT are equipped with sensors and electronic chips which enable them to collect and transmit data. This data exchange usually takes place over a public channel which means a malicious party can carryout several attacks on the transmitted data. Thus, ensuring integrity, authenticity, and undeniability of exchanged data in an IoMT setting is of utmost importance. Designing an efficient solution to address security issues mentioned above becomes more challenging due to the fact that computational and storage capabilities of a typical IoMT device is limited. With each passing day, newer devices are being added to IoMT systems, and these advancements are slowly putting pressure and placing new demands on the underlying network architecture design. Therefore, there is a need for innovations to handle the increasing demands of IoMT while providing strong security guarantees. Given the context of the situation, a signature scheme appears to be an efficient cryptographic primitive that helps to address the aforementioned security issues. Conventional signature schemes can be broadly classified into two categories. First is public-key infrastructure (PKI)-based [1], and the second is Identity-based cryptosystem (IBC)-based PKI-based protocols are very cumbersome in [2].nature. This is due to the fact that distribution and management of certificates require a large overhead. Hence, it is not a viable solution for a computationally limited IoMT system. On the other hand, IBC-based signature primitives circumvents the heavy task of certificate management. In an IBC-based cryptographic setting, public key of a signer is obtained directly from signer's public information (like IP address or email address). IBC provides an alternative to PKI-based cryptosystem, but they are prone to key escrow problem. Key generation center (KGC) knows the private key of the users, and thus can forge signature without being detected. This makes IBCbased signatures highly unsuitable for IoMT networks. Given the situation at hand, certificateless signature scheme (CLS) appears to be the most practical solution.

Concept of CLS was first put forwarded by Al-Riami and Paterson in [3]. The novel idea in a CLS scheme is that user generates his secret key by First, a partial private key is generated himself. by a semi-trusted intermediary, called key generation center (KGC). Later, user outputs his secret key using this partial private key, and some secret information only known to him. To summarize, process of generating secret key of a signer is split between KGC and the signer. Thus, CLS overcomes the issue of key escrow - as unlike identity based cryptosystem, KGC is not in possession of final private key of a signer. Over the last fifteen years, many CLS schemes have emerged. Almost all of the currently used CLS [4, 5, 6, 7, 8, 9, 10, 11, 12, 13] relies on classical hard problems, but unfortunately, these CLS will become obsolete once quantum computers come into the market. In the groundbreaking work [14], Shor pointed out that classical schemes built on the intractability of the number-theoretic problems [15, 16, 17] would fall under attacks by quantum computers. Thus, once efficient quantum computers come into the picture, the classical interpretation of soundness and security of cryptographic primitives may not encapsulate the right notion of security. In an endeavor to ensure our privacy and security of cryptographic applications, and to tackle the challenge brought by quantum algorithms, efforts are being taken to find an efficient and robust alternative which can replace these classical schemes. Multivariate public-key cryptosystem (MPKC) appears to be at the forefront among the post-quantum cryptography [18] candidates as a replacement of classical schemes. A system of multivariate polynomials works as a public key in MPKC. The security of MPKC is based on the fact that finding a solution to a system of a random quadratic multivariate polynomial is NP-hard [19]. Unlike number-theoretic problems, which form the base of classical schemes, the MQ problem is conjectured to withstand quantum attacks. There has been no construction of *multivariate* CLS in the current state of the art. This indicates the requirement of designing a secure and efficient multivariate CLS.

#### 1.1. Our Contribution

IoMT is shaping the health industry in a completely different way. With reducing costs, better and easy access to healthcare facilities, remote monitoring of patients, and other numerous benefits, IoMT is having one of the most profound impacts on humankind. A generic IoMT system consists of large number of medical devices and equipment (like wearable biosensors, blood-pressure monitors, thermometers, etc), each fitted with sensors and electronic chips. These sensors and chips are responsible for collection and transmission of medical data. The exchange of data takes place over a public channel which leads to multiple security threats. Out of all major threats, ensuring authenticity, integrity, and undeniability of the transmitted IoMT data is of utmost importance. Given the context of the situation, a signature scheme appears to be an efficient cryptographic primitive that helps to address the aforementioned security issues. Since traditional primitives like PKI-based signatures and IBC-based signatures are highly unsuitable for large scale IoMT networks, a CLS seems to be the natural choice to mitigate the security concerns. Almost all of the existing CLS relies upon the hardness assumption of discrete logarithm or prime factorization. However, these conventional schemes will become useless in the future due to the advent of quantum computers. In order to provide a smooth sailing into a world, where large-scale quantum computers are a reality, we need to transition to a CLS that offers post-quantum security.

Herein, we introduce the *first* multivariate based CLS, namely Mul-CLS which provides security against the threat of quantum computers since it hinges on the intractability assumption of MQ problem. The Mul-CLS consists of seven different algorithms, namely (i) Mul-CLS.Setup, Mul-CLS.Partial Private Key Extract, (ii) Mul-CLS.Set Secret Value, (iii) (iv)Mul-CLS.Set Secret Key, (v) Mul-CLS.Set Public Key, (vi) Mul-CLS.Signature Generation. and (vii) Mul-CLS.Signature Verification. In CLS, there is a semi-trusted third party called key generation center (KGC). The process of key generation is split between KGC and the user. KGC generates the master secret key (msk) and master public key (mpk) using Mul-CLS.Setup. Note that KGC is not in the possession of full secret key of the signers rather it only produces the partial private key of a signer. Given public parameter pp, msk, and user identity ID, KGC produces the partial private key  $(\mathbf{s}_{\text{ID}})$  of the signer using Mul-CLS.Partial Private Key Extract. In the next step, the partial secret key is transferred to the signer via a secure channel. Consequently, the signer makes use of the public parameter pp to generate a secret information w<sub>ID</sub> by running Mul-CLS.Set Secret Value. In the following, combining this secret information  $\mathbf{w}_{\mathsf{ID}}$ , and his partial private key  $s_{ID}$ , signer generates his full private key  $sk_{ID}$  by using Mul-CLS.Set Secret Key. Then the signer runs Mul-CLS.Set Public Key on input (pp,  $sk_{\rm ID}$ ) to generate the corresponding public key  $pk_{\rm ID}$ . Given secret key  $sk_{\rm ID}$ , public parameter pp, and public key  $pk_{\rm ID}$  as input, the signer outputs the signature  $\chi$  on a message msg by running Mul-CLS.Signature Generation. In the following, a message-signature pair  $(msg, \chi)$  is verified by a verifier using Mul-CLS.Signature Verification by making use of the public key of the signer  $pk_{\rm ID}$ , public parameter pp, and signer's identity ID.

Our scheme is proven to be existentially unforgeable against Super Type I and Super Type II adversary in the random oracle model. Mul-CLS belongs to the family of MPKCs and hence, it is naturally very efficient and only requires computing field multiplications and additions for its implementation. Sizes of master public key, master secret key msk, secret key of user, and signature are respectively  $\frac{m(n+2)(n+1)}{2}$  field  $(\mathbb{F}_q)$ elements,  $n^2 + m^2 + c$  field ( $\mathbb{F}_q$ ) elements, 2n field ( $\mathbb{F}_q$ ) elements, and  $2\delta \cdot |\mathsf{Comm}| + \delta \cdot (m+4n)\log_2 q + n\log_2 q$ bits. Here  $n, m, c, \delta$ , |Comm|, and q denote respectively the number of variables, number of equations, size of the central map, number of rounds of the underlying identification scheme, size of the commitment scheme, and the cardinality of the underlying field. Moreover, we analyze the applicability of Mul-CLS within the confines of IoMT systems. Our scheme is optimally suited for IoMT networks. It is very fast and computationally inexpensive to implement on IoMT devices. In addition, it addresses all the security issues like authenticity, integrity, and non-repudiation in a robust and efficient manner while also provides strong post-quantum security guarantees.

#### 2. PRELIMINARIES

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

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

where  $\mathbf{z} = (z_1, \ldots, z_n)$  and the coefficients  $a_{ij}, b_i$ , and  $c \in \mathbb{F}_q$ . The fundamental concept behind the construction of multivariate based cryptosystem is the following. In the first step, we take  $\mathcal{W} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ , a system of m multivariate quadratic polynomial in n variables with the property that finding preimage under  $\mathcal{W}$  is easy. In the second step, two affine invertible transformations  $\mathcal{C}_1 : \mathbb{F}_q^m \to \mathbb{F}_q^m$  and  $\mathcal{C}_2 : \mathbb{F}_q^n \to \mathbb{F}_q^n$ are picked with the aim of hiding the structure of  $\mathcal{W}$ . The public key is then defined to be the composition  $\mathcal{X} = \mathcal{C}_1 \circ \mathcal{W} \circ \mathcal{C}_2 : \mathbb{F}_q^n \to \mathbb{F}_q^m$ , while the private key is set to be  $(\mathcal{C}_1, \mathcal{W}, \mathcal{C}_2)$ . List of notations and symbols used in the article is given in Table 3.

#### 2.1. Hardness Assumption

The mathematical problem which lies at the heart of nearly all the multivariate public key cryptosystem is the so called MQ problem. Succinctly speaking, it says that solving a system of quadratic multivariate polynomials is NP-hard [19]. So far there has been no algorithm that can solve it in polynomial time. The MQ problem is formulated mathematically as follows.

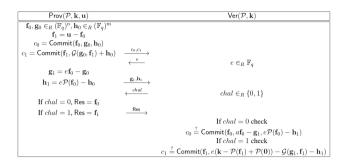
DEFINITION 2.1. Given a system  $\mathcal{R} = (r_{(1)}(\Delta, \ldots, \Delta_n), \ldots, r_{(k)}(\Delta_1, \ldots, \Delta_n))$  of k quadratic polynomials with each  $r_{(i)} \in \mathbb{F}_q[\Delta_1, \ldots, \Delta_n]$ , find values  $(\bar{\Delta}_1, \ldots, \bar{\Delta}_n) \in \mathbb{F}_q^n$  such that

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

#### 2.2. Multivariate signature scheme

A multivariate signature scheme consists of following algorithms:

- $(PK, SK) \leftarrow \text{Key Gen}(\kappa)$ : On input a security parameter  $\kappa$ , Key Gen outputs the pair of public key and private key as  $(PK, SK) = (\mathcal{X}, \{\mathcal{C}_1, \mathcal{W}, \mathcal{C}_2\})$ .
- $$\begin{split} & \sigma \leftarrow \mathsf{Sign}(\mathsf{msg}, SK) \text{: The signature } \sigma \text{ for a given} \\ & \text{message } \mathsf{msg} \in \mathbb{F}_q^m \text{ is generated by executing} \\ & \text{recursively } \alpha = \mathcal{C}_1^{-1}(\mathsf{msg}), \beta = \mathcal{W}^{-1}(\alpha) \text{ and } \sigma = \\ & \mathcal{C}_2^{-1}(\beta). \end{split}$$
- $0/1 \leftarrow \text{Verify}(\sigma, PK)$ : On input the message-signature pair msg,  $\sigma$ , a verifier calculates msg' =  $\mathcal{X}(\sigma)$  by making use of the public key  $PK = \mathcal{X}$ . If the equality msg = msg' holds, the verifier accepts the signature and outputs 1; otherwise, outputs 0 and the signature is rejected.



4

FIGURE 1. 5-pass identification protocol

## 2.3. Multivariate Identification Scheme [20]

A multivariate identification scheme makes use of a randomly chosen MQ system  $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ . The security of the protocol is contingent on the presumption that MQ problem is hard. General idea of the scheme is following. Suppose we are given public key of the underlying MPKC as  $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ . Prover who wish to identify himself, chooses  $\mathbf{u} \in \mathbb{F}_q^n$  as his secret key and evaluates  $\mathcal{P}$  at  $\mathbf{u}$  to derive  $\mathbf{k} = \mathcal{P}(\mathbf{u})$ , which works as the public key or identity of the prover. To prove his identity to a verifier, he is expected to satisfy the verifier of his knowledge of the secret  $\mathbf{u}$  without revealing  $\mathbf{u}$ . Polar form of  $\mathcal{P}$  is formulated as

$$\mathcal{G}(\iota,\tau) = \mathcal{P}(\iota+\tau) - \mathcal{P}(\iota) - \mathcal{P}(\tau), \quad (1)$$

where  $\mathcal{G}$  is a bilinear map. To construct the identification, we split the secret into various parts by using the bilinearity of  $\mathcal{G}$ . Presuming the existence of a computationally binding and statistically hiding commitment scheme Comm, Sakumoto et al. [20] constructed a 5-pass identification scheme (see Figure 1) for the knowledge of **u** that satisfies the relation  $\mathbf{k} = \mathcal{P}(\mathbf{u})$ .

## 2.4. General Construction of Certificateless Signature (CLS)

The concept of CLS first appeared in the work of Al-Riyami & Kenneth G. Paterson in Asiacrypt 2003 [3]. Later, the CLS and its security model was discussed at length in [21]. The preliminary definition and security model of CLS is taken from [21]. A certificateless signature scheme consist of seven algorithms: Setup, Partial Private Key Extract, Set Secret Value, Set Secret Key, Set Public Key, Signature Generation, and Signature Verification.

- $(pp,msk) \leftarrow Setup(\kappa)$ : On input a security parameter  $\kappa$ , KGC runs Setup to produce public parameter pp and master secret key msk.
- $\mathbf{s}_{\mathsf{ID}} \leftarrow \mathsf{Partial} \ \mathsf{Private} \ \mathsf{Key} \ \mathsf{Extract}(\mathsf{pp},\mathsf{msk},\mathsf{ID}) \texttt{:} \\ Given public parameter $\mathsf{pp}$, master secret key $$\mathsf{msk}$, and user identity $\mathsf{ID}$, $\mathsf{KGC}$ generates the partial secret key $$\mathsf{s}_{\mathsf{ID}}$ of the signer using $$\mathsf{Partial}$ \mathsf{Private} $\mathsf{Key}$ \mathsf{Extract}$. }$

- $\mathbf{w}_{\mathsf{ID}} \leftarrow \mathsf{Set} \; \mathsf{Secret} \; \mathsf{Value}(\mathsf{pp}) \text{: } \mathrm{On \; input \; pp, \; user \; runs} \\ \mathsf{Set} \; \mathsf{Secret} \; \mathsf{Value} \; \mathrm{to \; produce \; secret \; information \; } \mathbf{w}_{\mathsf{ID}}.$
- $sk_{\mathsf{ID}} \leftarrow \mathsf{Set} \mathsf{Secret} \mathsf{Key}(\mathbf{s}_{\mathsf{ID}}, \mathbf{w}_{\mathsf{ID}})$ : Given  $\mathbf{w}_{\mathsf{ID}}$  and  $\mathbf{s}_{\mathsf{ID}}$ , the signer with identity ID generates his full secret key  $sk_{\mathsf{ID}}$  by running Set Secret Key.
- $pk_{\mathsf{ID}} \leftarrow \mathsf{Set} \mathsf{Public} \mathsf{Key}(\mathsf{pp}, sk_{\mathsf{ID}})$ : On input  $\mathsf{pp}$ , and unique identity  $\mathsf{ID}$ , the signer produces his public key  $pk_{\mathsf{ID}}$  by putting in use the algorithm  $\mathsf{Set} \mathsf{Public} \mathsf{Key}$ .
- $\chi \leftarrow \text{Signature Generation}(\text{pp}, \text{msg}, sk_{\text{ID}}, pk_{\text{ID}})$ : Given  $sk_{\text{ID}}$ , pp, and  $pk_{\text{ID}}$  as input, the signer with identity ID outputs the signature  $\chi$  on a message msg by employing Signature Generation.
- 0 or  $1 \leftarrow \text{Signature Verification}(\text{pp}, pk_{\text{ID}}, \text{msg}, \text{ID}, \chi)$ : On input pp,  $pk_{\text{ID}}$ , and ID, a verifier checks the validity of a message-signature pair (msg,  $\chi$ ) using Signature Verification. It produces 1 as output if the signature is correct; otherwise, discards and outputs 0.

## 2.5. Security Model for CLS

In a generic setting, security model of CLS= (Setup, Partial Private Key Extract, Set Secret Value, Set Secret Key, Set Public Key, Signature Generation, and Signature Verification) should consider two types of adversaries: **Type I** and **Type II**.

DEFINITION 2.2 (Type I). Type I adversary captures an attacker who doesn't have access to the master secret key msk, but is granted the power to replace the public key of any signer with a randomly chosen value of his choice. In other words, it models an outside attacker who is not in possession of msk of the KGC.

DEFINITION 2.3 (Type II). A Type II adversary models KGC who is in possession of msk but doesn't have the power to replace the public key of a signer.

Type I and Type II adversary can access the following oracles:

- Create User: Given the identity ID as input, nothing is returned if the ID has been created before. Otherwise, it will perform Partial Private Key Extract, Set Secret Value, and Set Public Key for ID to get the partial private key  $\mathbf{s}_{\text{ID}}$ , the secret value  $\mathbf{w}_{\text{ID}}$ , and the public key  $pk_{\text{ID}}$ . Finally, it adds  $\langle \text{ID}, \mathbf{s}_{\text{ID}}, \mathbf{w}_{\text{ID}}, pk_{\text{ID}} \rangle$  to list  $\mathcal{J}$ , which is a list of tuples ( $\text{ID}_i, \mathbf{s}_{\text{ID}_i}, \mathbf{w}_{\text{ID}_i}, pk_{\text{ID}_i}$ ) that is empty in the beginning, and returns  $pk_{\text{ID}}$ .
- Public Key Replace: Given as input a query  $(ID, pk_{ID})$ , this oracle replaces user ID's public key with a randomly chosen  $pk'_{ID}$  and updates the corresponding information in the list  $\mathcal{J}$  where ID denotes the identity which has been created and  $pk_{ID}$  is a public key value in the public key space.

Secret Value Extract: Given as input a query ID, it browses the list  $\mathcal{J}$ , and returns the secret value  $\mathbf{w}_{\text{ID}}$ where ID is the identity which has been created. Note that the secret value outputted by this oracle is the one which is used to generate ID's original public key  $pk_{\text{ID}}$ .

These adversaries are further divided in three classes: Normal, Strong, and Super (ordered by their attacking powers). Using sign query, a Normal adversary can only obtain a legitimate signature if the ID's public key has never been replaced. A Strong Type adversary has more power than Normal Type adversary. If the public key has been replaced, a Strong adversary can still obtain the valid signature by providing the corresponding secret value. On the other hand, a Super Type adversary can get a valid signature no matter whether the public key has been replaced or not. Thus, security against Super Type I/II adversary implies security against Normal and Strong Type I/II adversaries

## 2.5.1. Security against Super Type I adversary

Existential unforgeability against a Super Type I chosen message and chosen identity adversary can be defined by the following game between a challenger CH and a Super Type I forger  $FG_1$ .

- Setup: The CH runs  $Setup(1^{\kappa})$  to generate public parameter pp and master secret key msk. CH sends pp to FG<sub>1</sub> and keeps msk with itself.
- Query:  $FG_1$  is allowed to make query to CH for the oracles (Create User, Public Key Replace, Secret Value Extract) as defined in Section 2.5 polynomial number of times. Moreover, it can also make polynomial times query to CH for the Partial Private Key Extract and Super Sign oracles as described:
  - Partial Private Key Extract: Given as input a query ID, the oracle goes through the list  $\mathcal{J}$  and returns back the partial private key  $s_{ID}$ . Here ID denotes the identity which has been created before.
  - Super Sign: Given as input a query (ID, msg), this oracle outputs a signature  $\chi$  with  $1 \leftarrow$ Signature Verification(pp,  $\mathcal{PK}_{\text{ID}}$ , msg, ID,  $\chi$ ), where  $\mathcal{PK}_{\text{ID}}$  represents the user ID's current public key in the list  $\mathcal{J}$ . If this user's public key has not been replaced,  $\mathcal{PK}_{\text{ID}} = pk_{\text{ID}}$ , where  $pk_{\text{ID}}$  is the public key returned from the oracle Create User. Otherwise,  $\mathcal{PK}_{\text{ID}} = pk'_{\text{ID}}$ , where  $pk'_{\text{ID}}$  is the latest public key value generated during the oracle Public Key Replace.
- Forgery: After all the queries,  $\mathsf{FG}_1$  outputs a forge message-signature pair  $(\mathsf{msg}^*, \chi^*, \mathsf{ID}^*)$ . Let  $pk_{\mathsf{ID}^*}$ be the current public key of the user  $\mathsf{ID}^*$  in the list

 $\mathcal{J}$ . We say that the Super Type I adversary  $\mathsf{FG}_1$  wins the game if the forgery satisfies the following requirements:

- $\begin{array}{ll} 1. & \mathsf{FG}_1 \mbox{ has not queried } (\mathsf{ID}^*,\mathsf{msg}^*) \mbox{ to } \mathsf{Super Sign} \\ & \mbox{ oracle before.} \end{array}$
- 2.  $FG_1$  has not queried ID\* to Partial Private Key Extract oracle before.
- 3. 1  $\leftarrow$  Signature Verification(pp,  $pk_{\mathsf{ID}^*}, \mathsf{msg}^*, \mathsf{ID}^*, \chi)$

We denote the advantage or the success probability of FG<sub>1</sub> by  $\mathsf{Adv}_{\mathsf{FG}_1}^{\mathcal{EXP}^{\mathrm{cma-cida-super}}_{CLS(1^{\kappa})}}$  which is defined as  $\mathsf{Adv}_{\mathsf{FG}_1}^{\mathcal{EXP}^{\mathrm{cma-cida-super}}_{CLS(1^{\kappa})}} = \mathsf{Prob}[\mathcal{EXP}^{\mathrm{cma-cida-super}}_{CLS(1^{\kappa})} = 1]$ =  $\mathsf{Prob}[\mathsf{FG}_1 \text{ wins the game}].$ 

DEFINITION 2.4. A CLS is said to be secure against a chosen message and chosen identity Super Type I adversary FG<sub>1</sub> if  $\operatorname{Adv}_{FG_1}^{\mathcal{EXP}_{CLS(1^{\kappa})}^{cma-cida-super}}$  is negligible in security parameter  $\kappa$  for any probabilistic polynomial time (PPT) Type I forger FG<sub>1</sub> who is allowed to make at most  $Q_{cu}$  (polynomial time) Create User,  $Q_{ppk}$  (polynomial time) Partial Private Key Extract,  $Q_{pkr}$  (polynomial time) Public Key Replace,  $Q_{sve}$  (polynomial time) Secret Value Extract and  $Q_s$  (polynomial time) Super Sign queries.

2.5.2. Security against Super Type II adversary

Existential unforgeability against a Super Type II chosen message and chosen identity adversary is an attack game between a challenger CH and a Super Type II forger  $FG_2$ . This game is depicted below.

- Setup: The CH generates public parameter pp and master secret key msk by running  $Setup(1^{\kappa})$ , and sends pp, msk to  $FG_2$ .
- Query:  $FG_2$  is allowed to do query to CH for the oracles (Create User, Public Key Replace, Secret Value Extract) as defined in Section 2.5. In addition, it is allowed to make query to CH for Super Sign oracle of the following form.
  - Super Sign: This oracle takes as input a query (ID, msg) (where ID denotes the identity which has been created and msg denotes the message to be signed). As output, it produces a signature  $\chi$  such that  $1 \leftarrow$  Signature Verification(pp,  $\mathcal{PK}_{\text{ID}}$ , msg, ID,  $\chi$ ). Here  $\mathcal{PK}_{\text{ID}}$  denotes the user ID's current public key in the list  $\mathcal{J}$ . If this user's public key has not been replaced,  $\mathcal{PK}_{\text{ID}} = pk_{\text{ID}}$  where  $pk_{\text{ID}}$  is the public key returned from the oracle Create User. Otherwise,  $\mathcal{PK}_{\text{ID}} = pk'_{\text{ID}}$ , where  $pk'_{\text{ID}}$  is the latest public key value submitted to the oracle Public Key Replace.

5

- Forgery: On completion of all the queries,  $FG_2$  outputs a message-signature pair ( $msg^*, \chi^*, ID^*$ ). One can state that a Super Type II adversary  $FG_2$  wins the game if the following conditions are satisfied by the forgery:
  - 1.  $FG_2$  has not queried  $(ID^*, msg^*)$  to the Super-Sign oracle before.
  - 2.  $FG_1$  has not queried  $ID^*$  to the Secret-Value-Extract oracle before.
  - 1 ← Signature Verification(pp, pk<sub>ID\*</sub>, msg\*, ID\*, χ). Here pk<sub>ID\*</sub> is the original public key returned from the oracle Create-User.

The advantage or the success probability of  $\mathsf{FG}_2$ is denoted by  $\mathsf{Adv}_{\mathsf{FG}_2}^{\mathcal{EXP}_{CLS(1^{\kappa})}^{\operatorname{cma-cida-super}}}$  and defined by  $\mathsf{Adv}_{\mathsf{FG}_2}^{\mathcal{EXP}_{CLS(1^{\kappa})}^{\operatorname{cma-cida-super}}} = \mathsf{Prob}[\mathcal{EXP}_{CLS(1^{\kappa})}^{\operatorname{cma-cida-super}}] = 1]$  $= \mathsf{Prob}[\mathsf{FG}_2 \text{ wins the game}].$ 

DEFINITION 2.5. A CLS is said to be secure against a chosen message and chosen identity Super Type II adversary FG<sub>2</sub> if  $Adv_{FG_2}^{\mathcal{EXP}_{CLS(1^{\kappa})}^{cma-cida-super}}$  is negligible in security parameter  $\kappa$  for any probabilistic polynomial time (PPT) Type II forger FG<sub>2</sub> who is allowed to make at most  $Q_{cu}$  (polynomial time) Create User,  $Q_{pkr}$  (polynomial time) Public Key Replace,  $Q_{sve}$  (polynomial time) Secret Value Extract and  $Q_s$  (polynomial time) Super Sign queries.

## 3. PROPOSED MULTIVARIATE CERTIFI-CATELESS SIGNATURE (MUL-CLS)

high level overview: The Mul-CLS consists  $\mathbf{A}$ of seven algorithms, namely (i) Mul-CLS.Setup, Mul-CLS.Partial Private Key Extract, (ii) (iii) Mul-CLS.Set Secret Value, (iv)Mul-CLS.Set Secret Key, (v) Mul-CLS.Set Public Key, (vi)Mul-CLS.Signature Generation, and (vii) Mul-CLS.Signature Verification. In CLS, there is a semi-trusted third party called key generation center (KGC) who generates the master secret key (msk) and master public key (mpk) using Mul-CLS.Setup. It generates the partial private key  $\mathbf{s}_{\text{ID}}$  for a signer with identity ID by running Mul-CLS.Partial Private Key Extract on (pp, msk, ID), pp being the public parameter. In the following, the signer runs Mul-CLS.Set Secret Value on input pp to produce a secret information  $\mathbf{w}_{\mathsf{ID}}.$  Then the signer determines its full private key  $sk_{\rm ID}$  by combining the secret information  $\mathbf{w}_{\mathsf{ID}}$ , and its partial private key  $s_{ID}$  during Mul-CLS.Set Secret Key. Given pp, and  $sk_{ID}$ , the signer with identity ID obtains the corresponding public key  $pk_{ID}$  by running Mul-CLS.Set Public Key. The algorithm Mul-CLS.Signature Generation is run by the signer on input  $(pp, sk_{ID}, pk_{ID})$ , and a message msg to produce a signature  $\chi$ . In the following, a message-signature pair  $(msg, \chi)$  is verified by a verifier by running Mul-CLS.Signature Verification on  $pk_{\rm ID}$ , pp, and ID. For illustration purpose, a workflow diagram depicting communication flow of the proposed CLS is given in Figure 2 and 3. We make use of a secure multivariate-based signature and identification protocol of [20] as the underlying building blocks of our construction. The reason for employing [20], instead of other state of the art multivariate based identification schemes [22, 20, 23, 24, 25, 26], is due to the fact that 5-pass scheme of [20] is most efficient among others and offers least round complexity.

We now give an explicit explanation of our proposed construction technique. The proposed design gives a generic method to extend any secure multivariate based signature to CLS by using an identification scheme. The KGC produces the MPKC private key for the user U corresponding to the U's unique identity ID in a different manner as follows. The goal of our design is to generate the different parts of a user's private key through its ID. As a consequence its public key can also be computed through its ID. In order to generate the partial private key, KGC first computes the hash of the identity ID as  $\mathbf{h}_{\mathsf{ID}} \in \mathbb{F}_q^m$ . It then uses master public key to compute the partial private key by simply evaluating  $\mathcal{P}^{-1}(\mathbf{h}_{\mathsf{ID}}) = \mathbf{s}_{\mathsf{ID}}$ . Note that KGC only generates the partial private key for a user. Thus, our construction solves the problem of key-escrow. For generating the full secret key, a user first randomly chooses  $\mathbf{w}_{\mathsf{ID}}$  from  $\mathbb{F}_q^n$  and then sets  $(\mathbf{s}_{\mathsf{ID}}, \mathbf{w}_{\mathsf{ID}})$  as the full private key. As we mentioned before, our proposed design allows a user to compute its public key using its unique identity ID. In the first step, a user U having identity ID runs the key generation algorithm of secure MQ-based signature to produce a system of multivariate polynomials  $\mathcal{R}_{\mathsf{ID}} = S_{\mathsf{ID}} \circ F_{\mathsf{ID}} \circ T_{\mathsf{ID}}$ . In the following, the user U takes its full private key  $(\mathbf{s}_{\mathsf{ID}}, \mathbf{w}_{\mathsf{ID}})$  and evaluates the the master public key  $\mathcal{P}$  at the first component  $\mathbf{s}_{\mathsf{ID}}$  to get  $\mathbf{h}_{\mathsf{ID}}$ . In addition, it evaluates  $\mathcal{R}_{\mathsf{ID}}$  at the second component  $\mathbf{w}_{\mathsf{ID}}$  to get  $\mathbf{r}_{\mathsf{ID}}$ . The final public key is set as  $pk_{\mathsf{ID}} = (\mathcal{R}_{\mathsf{ID}}, \mathbf{h}_{\mathsf{ID}}, \mathbf{r}_{\mathsf{ID}})$ . For generating the signature we modify the identification protocol [20] into signature by producing a transcript of the interactive identification protocol over  $\delta$  rounds. We append the value  $\mathcal{R}_{\rm ID}^{-1}(\phi) = \mu$  in the final signature to ensure that signature can't not be forged and it gets verified only under the correct public key.

PROTOCOL 1. Mul-CLS

 $(\mathsf{pp},\mathsf{msk}) \leftarrow \mathsf{Setup}(1^{\kappa})$ . On input security parameter  $1^{\kappa}$ , the key generation center KGC runs the Key Gen algorithm of the underlying MQ based signature scheme for generating master public key  $\mathsf{mpk} = \mathcal{P} = S \circ F \circ T : \mathbb{F}_q^n \to \mathbb{F}_q^m$  and master secret key  $\mathsf{msk} = \{S, F, T\}$ . It then chooses a computationally binding and perfectly hiding commitment scheme Comm, and publishes  $\mathsf{pp} = (\mathsf{mpk}, \mathbb{F}_q, n, m, \mathsf{Ha}_1, \mathsf{Ha}_2, \mathsf{Ha}_3, \mathsf{Comm})$  as the public parameter, where  $\mathsf{Ha}_1 : \{0, 1\}^* \to \mathbb{F}_q^m$ ,  $\mathsf{Ha}_2 : \{0, 1\}^* \to \mathbb{F}_q^\delta$  and  $\mathsf{Ha}_3 : \{0, 1\}^* \to \{0, 1\}^\delta$  are cryptographically secure collision resistant hash

functions and  $\delta$  is the number of rounds of the underlying identification scheme.

 $\mathbf{s}_{\mathsf{ID}} \leftarrow \mathsf{Partial}\;\mathsf{Private}\;\mathsf{Key}\;\mathsf{Extract}(\mathsf{pp},\mathsf{msk},\mathsf{ID}).$  The KGC, on input msk and an identity  $\mathsf{ID} \in \{0,1\}^*$  of an user, computes  $\mathbf{h}_{\mathsf{ID}} = \mathsf{Ha}_1(\mathsf{ID}) \in \mathbb{F}_q^m$  and evaluates  $\mathcal{P}^{-1}(\mathbf{h}_{\mathsf{ID}}) = \mathbf{s}_{\mathsf{ID}} \in \mathbb{F}_q^n$ . It then sends  $\mathbf{s}_{\mathsf{ID}}$  to the user with identity ID as partial private key.

# Algorithm 1 Partial Private Key Extract Input: pp, msk, ID Output: s<sub>ID</sub>

- 1: computes  $\mathbf{h}_{\mathsf{ID}} = \mathsf{Ha}_1(\mathsf{ID}) \in \mathbb{F}_a^m$
- 2: evaluates  $\mathcal{P}^{-1}(\mathbf{h}_{\mathsf{ID}}) = \mathbf{s}_{\mathsf{ID}} \in \mathbb{F}_q^n$ .
- 3: return  $s_{ID}$
- $\mathbf{w}_{\mathsf{ID}} \leftarrow \mathsf{Set} \mathsf{Secret} \mathsf{Value}(\mathsf{pp}).$  Given  $\mathsf{pp}$ , the user with identity  $\mathsf{ID}$  randomly chooses  $\mathbf{w}_{\mathsf{ID}} \in \mathbb{F}_q^n$  and sets  $\mathbf{w}_{\mathsf{ID}}$  as secret value.

lgorithm 2 Set Secret Value		
Input: pp Output: w <sub>ID</sub>		
1: $\mathbf{w}_{ID} \in_R \mathbb{F}_q^n$		

- 2: return  $\mathbf{w}_{\text{ID}}$
- $sk_{\text{ID}} \leftarrow$  Set Secret Key( $\mathbf{s}_{\text{ID}}, \mathbf{w}_{\text{ID}}$ ). Given  $\mathbf{s}_{\text{ID}}, \mathbf{w}_{\text{ID}}$ , the user with identity ID sets  $sk_{\text{ID}} = (\mathbf{s}_{\text{ID}}, \mathbf{w}_{\text{ID}})$  as its secret key.

Algorithm 3 Set Secret Key	
Input: $\mathbf{s}_{ID}, \mathbf{w}_{ID}$	
<b>Output:</b> $sk_{ID}$	

1: return  $sk_{\mathsf{ID}} = (\mathbf{s}_{\mathsf{ID}}, \mathbf{w}_{\mathsf{ID}})$ 

- $pk_{\mathsf{ID}} \leftarrow \mathsf{Set} \mathsf{Public} \mathsf{Key}(\mathsf{pp}, sk_{\mathsf{ID}}).$  Given  $\mathsf{pp}$  and  $sk_{\mathsf{ID}} = (\mathbf{s}_{\mathsf{ID}}, \mathbf{w}_{\mathsf{ID}})$ , the user with identity  $\mathsf{ID}$  executes the following:
  - 1. runs the Key Gen algorithm of the underlying MQ based signature scheme to generate public key  $\mathcal{R}_{\mathsf{ID}} = S_{\mathsf{ID}} \circ F_{\mathsf{ID}} \circ T_{\mathsf{ID}} : \mathbb{F}_q^n \to \mathbb{F}_q^m$  and secret key  $\{S_{\mathsf{ID}}, F_{\mathsf{ID}}, T_{\mathsf{ID}}\},\$
  - 2. computes  $\mathcal{P}(\mathbf{s}_{\mathsf{ID}}) = \mathbf{h}_{\mathsf{ID}} \in \mathbb{F}_q^m, \ \mathcal{R}_{\mathsf{ID}}(\mathbf{w}_{\mathsf{ID}}) = \mathbf{r}_{\mathsf{ID}} \in \mathbb{F}_q^m, \ \mathcal{R}_q$
  - 3. publishes  $pk_{\text{ID}} = (\mathcal{R}_{\text{ID}}, \mathbf{h}_{\text{ID}}, \mathbf{r}_{\text{ID}})$  as its public key.
- $\chi \leftarrow \text{Signature Generation}(\text{pp}, \text{msg}, sk_{\text{ID}}, pk_{\text{ID}}).$  Given pp, a message msg  $\in \{0, 1\}^*$ ,  $sk_{\text{ID}} = (\mathbf{s}_{\text{ID}}, \mathbf{w}_{\text{ID}})$  and  $pk_{\text{ID}} = (\mathcal{R}_{\text{ID}}, \mathbf{h}_{\text{ID}}, \mathbf{r}_{\text{ID}})$ , the user with identity ID runs the  $\delta$ round of the underlying identification scheme for the system  $\mathcal{P}_{\text{ID}}(\mathbf{z}) = \mathcal{P}(\mathbf{x}) + \mathcal{R}_{\text{ID}}(\mathbf{y}) = h_{\text{ID}} + r_{\text{ID}} = k_{\text{ID}}$  of m multivariate polynomials in 2n variables  $\mathbf{z} = \mathbf{x} || \mathbf{y}$ in the following manner to generate the signature  $\chi$ , where  $\mathbf{v}_{\text{ID}} = \mathbf{s}_{\text{ID}} || \mathbf{w}_{\text{ID}} \in \mathbb{F}_q^{2n}$  is the secret solution of that system.
  - 1. chooses  $\mathbf{a}_{0,1}, \ldots, \mathbf{a}_{0,j}, \mathbf{b}_{0,1}, \ldots, \mathbf{b}_{0,j}, \in_R$  $\mathbb{F}_q^{2n}, \mathbf{c}_{0,1}, \ldots, \mathbf{c}_{0,j} \in_R \mathbb{F}_q^m$  and for  $j = 1, \ldots, \delta$ ,

#### Algorithm 4 Set Public Key

Input:  $pp, sk_{ID}$ Output:  $pk_{ID}$ 

1: runs the Key Gen algorithm of the underlying MQ based signature scheme to generate

7

public key  $\mathcal{R}_{\mathsf{ID}} = S_{\mathsf{ID}} \circ F_{\mathsf{ID}} \circ T_{\mathsf{ID}} : \mathbb{F}_q^n \to \mathbb{F}_q^m$  and secret key  $\{S_{\mathsf{ID}}, F_{\mathsf{ID}}, T_{\mathsf{ID}}\}$ 2: computes  $\mathcal{P}(\mathbf{s}_{\mathsf{ID}}) = \mathbf{h}_{\mathsf{ID}} \in \mathbb{F}_q^m, \ \mathcal{R}_{\mathsf{ID}}(\mathbf{w}_{\mathsf{ID}}) = \mathbf{r}_{\mathsf{ID}} \in \mathbb{F}_q^m$ 

3: **return**  $pk_{\mathsf{ID}} = (\mathcal{R}_{\mathsf{ID}}, \mathbf{h}_{\mathsf{ID}}, \mathbf{r}_{\mathsf{ID}})$ 

- (a) writes  $\mathbf{a}_{1,j} = \mathbf{v}_{\mathsf{ID}} \mathbf{a}_{0,j}$ ,
- (b) evaluates  $e_{0,j} = \mathsf{Comm}(\mathbf{a}_{0,j}, \mathbf{b}_{0,j}, \mathbf{c}_{0,j}), e_{1,j} = \mathsf{Comm}(\mathbf{a}_{1,j}, \mathcal{G}(\mathbf{b}_{0,j}, \mathbf{a}_{1,j}) + \mathbf{c}_{0,j}).$
- 2. sets  $COM = (e_{0,1}, e_{1,1}, \dots, e_{0,\delta}, e_{1,\delta})$
- 3. evaluates challenges  $\mathsf{Ha}_2(\mathcal{P}||\mathcal{R}_{\mathsf{ID}}||\mathsf{msg}||\mathsf{COM}) = (\alpha_1, \ldots, \alpha_{\delta}) \in \mathbb{F}_q^{\delta}.$
- 4. computes  $\mathbf{b}_{1,j} = \alpha_j \mathbf{a}_{0,j} \mathbf{b}_{0,j}$  and  $\mathbf{c}_{1,j} = \alpha_j \mathcal{P}_{\mathsf{ID}}(\mathbf{a}_{0,j}) \mathbf{c}_{0,j}$  for  $j = 1, \dots, \delta$ .
- 5. sets  $\mathsf{RE}_1 = (\mathbf{b}_{1,1}, \mathbf{c}_{1,1} \dots, \mathbf{b}_{1,\delta}, \mathbf{c}_{1,\delta}).$
- 6. derives challenges  $\mathsf{Ha}_{3}(\mathcal{P}||\mathcal{R}_{\mathsf{ID}}||\mathsf{msg}||\mathsf{COM}||\mathsf{RE}_{1}) = (t_{1},\ldots,t_{\delta}) \in \{0,1\}^{\delta}.$
- 7. writes  $\mathsf{RE}_2 = (\mathbf{a}_{t_1,1} \dots, \mathbf{a}_{t_{\delta},\delta}).$
- 8. computes  $\operatorname{Ha}_{3}(\mathcal{P}||\mathcal{R}_{\operatorname{ID}}||\operatorname{\mathsf{msg}}||\operatorname{COM}||\operatorname{RE}_{1}||\operatorname{RE}_{2}) = \phi \in \mathbb{F}_{q}^{m}$
- 9. evaluates  $\mathcal{R}_{\mathsf{ID}}^{-1}(\phi) = \mu$
- 10. outputs the signature as  $\chi = Sign(msg) = (COM, RE_1, RE_2, \mu).$

Length of the signature is  $2\delta \cdot |\mathsf{Comm}| + \delta \cdot (m + 4n) \log_2 q + n \log_2 q$  bit.

- 0 or  $1 \leftarrow \text{Signature Verification}(pp, pk_{\text{ID}}, \text{msg}, \text{ID}, \chi)$ . The verifier checks the validity of the message-signature pair (msg,  $\chi = Sign(\text{msg})$  with respect to the user with identity ID by executing the following steps:
  - 1. evaluates  $\mathbf{k}_{\text{ID}} = \mathbf{h}_{\text{ID}} + \mathbf{r}_{\text{ID}}$  if  $\text{Ha}_1(\text{ID}) = \mathbf{h}_{ID}$  appears in  $pk_{\text{ID}}$ , else discards and outputs 0;
  - 2. computes  $\phi$  =  $Ha_1(\mathcal{P}||\mathcal{R}_{\mathsf{ID}}||\mathsf{msg}||\mathsf{COM}||\mathsf{RE}_1||\mathsf{RE}_2) \in \mathbb{F}_q^m;$
  - 3. if the equality  $\mathcal{R}_{\text{ID}}(\mu) = \phi$  holds then it proceeds further, otherwise discards and outputs 0;
  - 4. computes challenges  $(\alpha_1, \dots, \alpha_{\delta}) =$   $\mathsf{Ha}_2(\mathcal{P}||\mathcal{R}_{\mathsf{ID}}||\mathsf{msg}||\mathsf{COM}) \in \mathbb{F}_q^{\delta} \text{ and } (t_1, \dots, t_{\delta}) =$  $\mathsf{Ha}_3(\mathcal{P}||\mathcal{R}_{\mathsf{ID}}||\mathsf{msg}||\mathsf{COM}||\mathsf{RE}_1) \in \{0,1\}^{\delta},$
  - 5. breaks COM into  $(e_{0,1}, e_{1,1}, \dots, e_{0,\delta}, e_{1,\delta})$ , RE<sub>1</sub> into  $((\mathbf{b}_{1,1}, \mathbf{c}_{1,1}, \dots, \mathbf{b}_{1,\delta}, \mathbf{c}_{1,\delta})$  and RE<sub>2</sub> into  $(\mathbf{a}_{t_1,1}, \dots, \mathbf{a}_{t_{\delta},\delta})$ .
  - 6. checks the validity of the following equalities

(a) for each  $j = 1, ..., \delta, t_j = 0$  implies

$$e_{0,j} \stackrel{?}{=} \mathsf{Comm}(\mathbf{a}_{t_j,j}, \alpha_j \mathbf{a}_{t_j,j} - \mathbf{b}_{1,j}, \alpha_j \mathcal{P}_{\mathsf{ID}}(\mathbf{a}_{t_i,j}) - \mathbf{c}_{1,j})$$

(b) for each 
$$j = 1, \ldots, \delta, t_j = 1$$
 implies

#### Algorithm 5 Signature Generation

Input: pp, msg,  $sk_{ID}$ ,  $pk_{ID}$ ) Output:  $\chi$ 

1: chooses  $\mathbf{a}_{0,1},\ldots,\mathbf{a}_{0,j},\mathbf{b}_{0,1},\ldots,\mathbf{b}_{0,j},\in_R$  $\mathbb{F}_q^{2n}, \mathbf{c}_{0,1}, \ldots, \mathbf{c}_{0,j} \in_R \mathbb{F}_q^m$ 2: for  $j = 1, ..., \delta$  do writes  $\mathbf{a}_{1,j} = \mathbf{v}_{\mathsf{ID}} - \mathbf{a}_{0,j}$ , evaluates  $e_{0,j} = \text{Comm}(\mathbf{a}_{0,j}, \mathbf{b}_{0,j}, \mathbf{c}_{0,j}), e_{1,j} =$  $\operatorname{Comm}(\mathbf{a}_{1,j}, \mathcal{G}(\mathbf{b}_{0,j}, \mathbf{a}_{1,j}) + \mathbf{c}_{0,j}).$ 2: sets  $COM = (e_{0,1}, e_{1,1}, \dots, e_{0,\delta}, e_{1,\delta})$ 3: evaluates challenges  $Ha_2(\mathcal{P}||\mathcal{R}_{ID}||msg||COM) =$  $(\alpha_1,\ldots,\alpha_\delta)\in\mathbb{F}_q^\delta.$ 4: for  $j = 1, ..., \delta$  do computes  $\mathbf{b}_{1,j} = \alpha_j \mathbf{a}_{0,j} - \mathbf{b}_{0,j}$  and  $\mathbf{c}_{1,j} =$  $\alpha_i \mathcal{P}_{\mathsf{ID}}(\mathbf{a}_{0,i}) - \mathbf{c}_{0,i}$ 5: sets  $\mathsf{RE}_1 = (\mathbf{b}_{1,1}, \mathbf{c}_{1,1}, \dots, \mathbf{b}_{1,\delta}, \mathbf{c}_{1,\delta}).$ 6: derives challenges  $Ha_3(\mathcal{P}||\mathcal{R}_{ID}||msg||COM||RE_1) =$  $(t_1,\ldots,t_{\delta}) \in \{0,1\}^{\delta}.$ 7: writes  $\mathsf{RE}_2 = (\mathbf{a}_{t_1,1} \dots, \mathbf{a}_{t_{\delta},\delta}).$ 8: computes  $Ha_3(\mathcal{P}||\mathcal{R}_{ID}||msg||COM||RE_1||RE_2) =$  $\phi \in \mathbb{F}_q^m$ 9: evaluates  $\mathcal{R}_{\mathsf{ID}}^{-1}(\phi) = \mu$ 10: return  $\chi = (COM, RE_1, RE_2, \mu)$ .

$$e_{1,j} \stackrel{?}{=} \mathsf{Comm}(\mathbf{a}_{t_j,j}, \alpha_j(\mathbf{k}_{\mathsf{ID}} - \mathcal{P}_{\mathsf{ID}}(\mathbf{a}_{t_j,j}) + \mathcal{P}_{\mathsf{ID}}(\mathbf{0})) - \mathcal{G}(\mathbf{b}_{1,j}, \mathbf{a}_{t_j,j}) - \mathbf{c}_{1,j})$$

- (c)  $\mathsf{Ha}_3(\mathcal{P}||\mathcal{R}_{\mathsf{ID}}||\mathsf{msg}||\mathsf{COM}||\mathsf{RE}_1||\mathsf{RE}_2) \stackrel{?}{=} \mathcal{R}_{\mathsf{ID}}(\mu)$
- 7. if all the aforementioned equalities hold then the pair  $(msg, \chi)$  as a valid one and outputs 1; otherwise, outputs 0 to denote the pair  $(msg, \chi)$ as an invalid one.

**Correctness:** The correctness of our proposed scheme can be achieved by showing the existence of the following equalities in the step 6 of Signature Verification:

$$\begin{aligned} &\text{if } t_j = 0 \text{ then} \\ &e_{0,j} = \text{Comm}(\mathbf{a}_{t_j,j}, \alpha_j \mathbf{a}_{t_j,j} - \mathbf{b}_{1,j}, \alpha_j \mathcal{P}_{\mathsf{ID}}(\mathbf{a}_{t_j,j}) - \mathbf{c}_{1,j}) \\ & (2) \\ &\text{if } t_j = 1 \text{ then} \\ &e_{1,j} = \text{Comm}(\mathbf{a}_{t_j,j}, \alpha_j(\mathbf{k}_{\mathsf{ID}} - \mathcal{P}_{\mathsf{ID}}(\mathbf{a}_{t_j,j}) + \mathcal{P}_{\mathsf{ID}}(\mathbf{0})) - \\ & \mathcal{G}(\mathbf{b}_{1,j}, \mathbf{a}_{t_j,j}) - \mathbf{c}_{1,j}) \end{aligned}$$

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

• **Case I**  $(t_j = 0)$ : Here  $\mathbf{a}_{t_j,j} = \mathbf{a}_{0,j}, \alpha_j \mathbf{a}_{t_j,j} - \mathbf{b}_{1,j} = \alpha_j \mathbf{a}_{0,j} - \mathbf{b}_{1,j} = \mathbf{b}_{0,j}$  and  $\alpha_j \mathcal{P}_{\mathsf{ID}}(\mathbf{a}_{t_j,j}) - \mathbf{c}_{1,j} = \alpha_j \mathcal{P}_{\mathsf{ID}}(\mathbf{a}_{0,j}) - \mathbf{c}_{1,j} = \mathbf{c}_{0,j}$ . Thus the equation 2 holds for each  $j = 1, \dots, \alpha$ .

Algorithm 6 Signature Verification		
<b>Input:</b> pp, $pk_{\text{ID}}$ , msg, ID, $\chi$	-	
Output: 0 or 1		
1: if $Ha_1(ID) = h_{ID}$ appears in $pk_{ID}$ then		
evaluates $\mathbf{k}_{ID} = \mathbf{h}_{ID} + \mathbf{r}_{ID}$		
computes $\phi$ =	=	
$Ha_1(\mathcal{P}  \mathcal{R}_{ID}  msg  COM  RE_1  RE_2) \in \mathbb{F}_q^m$		
$\mathbf{if} \ \mathcal{R}_{ID}(\mu) = \phi \ \mathbf{then}$		
computes challenges $(\alpha_1, \ldots, \alpha_{\delta}) =$	=	
$Ha_2(\mathcal{P}  \mathcal{R}_{ID}  msg  COM) \in \mathbb{F}_a^\delta \text{ and }$		
$(t_1,\ldots,t_\delta)$ =	=	
$Ha_3(\mathcal{P}  \mathcal{R}_{ID}  msg  COM  RE_1) \in \{0,1\}^\delta$		
breaks COM into $(e_{0,1}, e_{1,1}, \dots, e_{0,\delta}, e_{1,\delta})$	,	
$RE_1$ into $((\mathbf{b}_{1,1}, \mathbf{c}_{1,1}, \dots, \mathbf{b}_{1,\delta}, \mathbf{c}_{1,\delta})$ and		
$RE_2$ into $(\mathbf{a}_{t_1,1},\ldots,\mathbf{a}_{t_{\delta},\delta})$ .		
for $j = 1, \ldots, \delta$ and $t_j = 0$ do		
$\mathbf{if}$ $e_{0,j}$ $\stackrel{?}{=}$ $Comm(\mathbf{a}_{t_j,j}, lpha_j \mathbf{a}_{t_j,j}$ –	-	
$\mathbf{b}_{1,j}, lpha_j \mathcal{P}_{ID}(\mathbf{a}_{t_j,j}) - \mathbf{c}_{1,j})  ext{ and } e_{1,j} \stackrel{?}{=}$		
$Comm(\mathbf{a}_{t_j,j}, \alpha_j(\mathbf{k}_{ID} - \mathcal{P}_{ID}(\mathbf{a}_{t_j,j}) +$	-	
$\mathcal{P}_{ID}(0)) - \mathcal{G}(\mathbf{b}_{1,j},\mathbf{a}_{t_j,j}) - \mathbf{c}_{1,j})  ext{ then }$		
return 1		
else		
return 0		
else		
$\mathbf{return} \ 0$		
2: else		
return 0		

• Case II  $(t_j = 1)$ : Here  $\mathbf{a}_{t_j,j} = \mathbf{a}_{1,j}$  and

$$\begin{aligned} \alpha_{j}(\mathbf{k}_{\mathsf{ID}} - \mathcal{P}_{\mathsf{ID}}(\mathbf{a}_{t_{j},j}) + \mathcal{P}_{\mathsf{ID}}(\mathbf{0})) &- \mathcal{G}(\mathbf{b}_{1,j}, \mathbf{a}_{t_{j},j}) - \mathbf{c}_{1,j} \\ &= \alpha_{j}(\mathcal{P}_{\mathsf{ID}}(\mathbf{v}_{\mathsf{ID}}) - \mathcal{P}_{\mathsf{ID}}(\mathbf{a}_{1,j}) + \mathcal{P}_{\mathsf{ID}}(\mathbf{0})) - \\ \mathcal{G}(\mathbf{b}_{1,j}, \mathbf{a}_{1,j}) - \mathbf{c}_{1,j} \\ &= \alpha_{j}(\mathcal{P}_{\mathsf{ID}}(\mathbf{a}_{0,j} + \mathbf{a}_{1,j}) - \mathcal{P}_{\mathsf{ID}}(\mathbf{a}_{1,j}) + \mathcal{P}_{\mathsf{ID}}(\mathbf{0})) - \\ \mathcal{G}(\mathbf{b}_{1,j}, \mathbf{a}_{1,j}) - \mathbf{c}_{1,j} \text{ since } \mathbf{v}_{\mathsf{ID}} = \mathbf{a}_{0,j} + \mathbf{a}_{1,j} \\ &= \alpha_{j}(\mathcal{P}_{\mathsf{ID}}(\mathbf{a}_{0,j}) + \mathcal{G}(\mathbf{a}_{0,j}, \mathbf{a}_{1,j})) - \mathcal{G}(\mathbf{b}_{1,j}, \mathbf{a}_{1,j}) - \mathbf{c}_{1,j} \\ &= \mathcal{G}(\alpha_{j}\mathbf{a}_{0,j} - \mathbf{b}_{1,j}, \mathbf{a}_{1,j}) + \alpha_{j}\mathcal{P}(\mathbf{a}_{0,j}) - \mathbf{c}_{1,j} \\ &= \mathcal{G}(\mathbf{b}_{0,j}, \mathbf{a}_{1,j}) + \mathbf{c}_{0,j} \end{aligned}$$

Hence the equation 3 holds for each  $j = 1, \ldots, \alpha$ .

#### 4. SECURITY

(3)

THEOREM 4.1. The proposed scheme Mul-CLS is existentially unforgeable against a chosen message and chosen identity Super Type I adversary under the hardness of MQ problem, if

- (i) the underlying commitment scheme Comm is computationally binding and perfectly hiding,
- ii) the hash functions Ha<sub>1</sub>, Ha<sub>2</sub> and Ha<sub>3</sub> are designed as random oracles.

**Proof:** We prove the security of Mul-CLS against a chosen message and chosen identity Super Type I adversary by the method of contradiction where the MQ problem is assumed to be hard. Consider an adversary  $\mathcal{AD}_1$  whose success probability is assumed to be non-negligible in the game defined in the Section 2.5.1 for Mul-CLS. Then we will play a series of games  $\mathbf{Ga}_0, \ldots, \mathbf{Ga}_8$  to show that an oracle machine  $\mathcal{O}^{\mathcal{AD}}$  can be constructed to solve the MQ problem with the help of  $\mathcal{AD}_1$  and managing outputs of the random oracles  $\mathbf{Ha}_1, \mathbf{Ha}_2$  and  $\mathbf{Ha}_3$ . Note that for each  $i = 1, \ldots, 8$ ,  $\mathbf{Ga}_i$ is obtained by slight modification of  $\mathbf{Ga}_{i-1}$ . Consider  $\Pr[\mathbf{Ga}_i]$  as  $\mathcal{AD}_1$ 's success probability in  $\mathbf{Ga}_i$ .

- $\mathbf{Ga}_1$ : It is identical to  $\mathbf{Ga}_0$  except that during Create User query, the oracle machine  $\mathcal{O}^{\mathcal{AD}}$ 
  - 1. randomly chooses  $\mathbf{s}_{\mathsf{ID}} \in \mathbb{F}_q^n$ , and substitutes Ha<sub>1</sub>'s output on ID by  $\mathbf{h}_{\mathsf{ID}} = \mathcal{P}(\mathbf{s}_{\mathsf{ID}})$ ,
  - 2. randomly selects  $\mathbf{w}_{\mathsf{ID}} \in \mathbb{F}_q^n$ ,
  - 3. randomly chooses a system of quadratic multivariate polynomials  $\mathcal{R}_{\mathsf{ID}} : \mathbb{F}_q^n \to \mathbb{F}_q^m$  and computes  $\mathcal{R}_{\mathsf{ID}}(\mathbf{w}_{\mathsf{ID}}) = \mathbf{r}_{\mathsf{ID}}$ ,
  - 4. substitutes the output of Create User by  $\langle ID, \mathbf{s}_{ID}, \mathbf{w}_{ID}, (\mathcal{R}_{ID}, \mathbf{h}_{ID}, \mathbf{r}_{ID}) \rangle$ .

If  $|\Pr[\mathbf{Ga}_1] - \Pr[\mathbf{Ga}_0]|$  is non-negligible then one may use  $\mathcal{AD}_1$  for distinguishing  $\mathsf{Ha}_1$ 's distributions. This is impossible.  $\mathsf{Ha}_1$  is designed as random oracle. Consequently,  $|\Pr[\mathbf{Ga}_1] - \Pr[\mathbf{Ga}_0]| = \varepsilon_1(\kappa)$ , where  $\varepsilon_1(\kappa)$  is a negligible function.

- $\mathbf{Ga}_2$ : This game is analogues to  $\mathbf{Ga}_1$ , apart from the fact that  $\mathcal{O}^{\mathcal{AD}}$  randomly chooses  $\mathbf{s}_{\mathsf{ID}} \in \mathbb{F}_q^n$ , and substitutes  $\mathsf{Ha}_1$ 's output on  $\mathsf{ID}$  by  $\mathbf{h}_{\mathsf{ID}} = \mathcal{P}(\mathbf{s}_{\mathsf{ID}})$  and the respective partial private key by  $\mathbf{s}_{\mathsf{ID}}$  during Partial Private Key Extract query. Now  $|\mathsf{Pr}[\mathbf{Ga}_2] \mathsf{Pr}[\mathbf{Ga}_1]|$  non-negligible implies  $\mathcal{AD}_1$  can be used for distinguishing  $\mathsf{Ha}_1$ 's output distributions, which is impossible. Thereby,  $|\mathsf{Pr}[\mathbf{Ga}_2] \mathsf{Pr}[\mathbf{Ga}_1]| = \varepsilon_2(\kappa)$ , a negligible function.
- $\mathbf{Ga}_3$ : It is identical to  $\mathbf{Ga}_2$  except that during Public Key Replace query, the oracle machine  $\mathcal{O}^{\mathcal{AD}}$ 
  - $\begin{array}{ll} \text{1.} & \text{randomly chooses } \mathbf{s}_{\mathsf{ID}}' \in \mathbb{F}_q^n, \text{ and substitutes} \\ & \mathsf{Ha}_1\text{'s output on } \mathsf{ID} \text{ by } \mathbf{h}_{\mathsf{ID}}' = \mathcal{P}(\mathbf{s}_{\mathsf{ID}}'), \end{array}$
  - 2. randomly chooses a system of quadratic multivariate polynomials  $\mathcal{R}'_{\mathsf{ID}} : \mathbb{F}_q^n \to \mathbb{F}_q^m$  and computes  $\mathcal{R}'_{\mathsf{ID}}(\mathbf{w}'_{\mathsf{ID}}) = \mathbf{r}'_{\mathsf{ID}}$ ,
  - 3. replaces the public key  $pk_{\text{ID}}$  with  $pk'_{\text{ID}} = (\mathcal{R}'_{\text{ID}}, \mathbf{h}'_{\text{ID}}, \mathbf{r}'_{\text{ID}}).$

If  $|\Pr[\mathbf{Ga}_3] - \Pr[\mathbf{Ga}_2]|$  is non-negligible then one may use  $\mathcal{AD}$  for distinguishing Ha<sub>1</sub>'s distributions.

This is impossible. Consequently,  $|\Pr[\mathbf{Ga}_3] - \Pr[\mathbf{Ga}_2]| = \varepsilon_3(\kappa)$ , a negligible function.

- $\mathbf{Ga}_4$ : This game is analogues to  $\mathbf{Ga}_3$ , apart from the fact that  $\mathcal{O}^{\mathcal{AD}}$  randomly chooses  $\mathbf{w'}_{\mathsf{ID}} \in$  $\mathbb{F}_q^n$  and substitutes the secret value with  $\mathbf{w'}_{\mathsf{ID}}$ during Set Secret Value query. If  $|\mathsf{Pr}[\mathsf{Ga}_4] \mathsf{Pr}[\mathsf{Ga}_3]|$  is non-negligible then one may use  $\mathcal{AD}_1$ for distinguishing  $\mathcal{O}^{\mathcal{AD}}$ 's output sequence from a random sequence which is not possible. Hence, there exists a negligible function  $\varepsilon_4(\kappa)$  such that  $|\mathsf{Pr}[\mathsf{Ga}_4] - \mathsf{Pr}[\mathsf{Ga}_3]| = \varepsilon_4(\kappa)$ .
- $\mathbf{Ga}_5$ : It is identical to  $\mathbf{Ga}_4$  except that during Super Sign query, the oracle machine  $\mathcal{O}^{\mathcal{AD}}$ 
  - 1. randomly selects  $\mathbf{s}_{\mathsf{ID}}, \mathbf{w}_{\mathsf{ID}} \in \mathbb{F}_{a}^{n}$ ,
  - 2. chooses a system of quadratic multivariate polynomials  $\mathcal{R}_{\mathsf{ID}} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ , and computes  $\mathcal{R}_{\mathsf{ID}}(\mathbf{w}_{\mathsf{ID}}) = \mathbf{r}_{\mathsf{ID}}$ ,
  - 3. replaces the output of  $Ha_1$  on ID by  $h_{ID} = \mathcal{P}(\mathbf{s}_{ID})$ ,
  - 4. substitutes the signature by  $\chi$  which is produced by using secret key  $\mathbf{s}_{\text{ID}} || \mathbf{w}_{\text{ID}}$  for the system  $\mathcal{P}_{\text{ID}}(\mathbf{z}) = \mathcal{P}(\mathbf{x}) + \mathcal{R}_{\text{ID}}(\mathbf{y}) = \mathbf{h}_{\text{ID}} + \mathbf{r}_{\text{ID}} = \mathbf{k}_{\text{ID}}.$

If  $|\Pr[\mathbf{Ga}_5] - \Pr[\mathbf{Ga}_4]|$  is non-negligible then it is possible to utilize  $\mathcal{AD}_1$  for distinguishing Ha<sub>1</sub>'s distributions which is impossible. Therefore,  $|\Pr[\mathbf{Ga}_5] - \Pr[\mathbf{Ga}_4]| = \varepsilon_5(\kappa)$ , where  $\varepsilon_5(\kappa)$  is a negligible function.

- $\mathbf{Ga}_6$ : This game is similar to  $\mathbf{Ga}_5$  excepting  $\mathcal{O}^{\mathcal{AD}}$  replaces  $\mathbf{Ha}_2$ 's output by a random element chosen from  $\mathbb{F}_q^{\delta}$ . It is possible to use  $\mathcal{AD}_1$  for distinguishing  $\mathbf{Ha}_2$ 's distributions if  $|\Pr[\mathbf{Ga}_6] \Pr[\mathbf{Ga}_5]|$  is non-negligible, which is not possible. Thereby,  $|\Pr[\mathbf{Ga}_6] \Pr[\mathbf{Ga}_5]| = \varepsilon_6(\kappa)$ , a negligible function.
- $\mathbf{Ga}_7$ : It is analogues to  $\mathbf{Ga}_6$  apart from the fact that  $\mathcal{O}^{\mathcal{AD}}$  replaces  $\mathsf{Ha}_3$ 's output by randomly selected bit-string of length  $\delta$ . Note that one can utilize  $\mathcal{AD}_1$  in order to distinguish  $\mathsf{Ha}_3$ 's distributions if  $|\mathsf{Pr}[\mathbf{Ga}_7] \mathsf{Pr}[\mathbf{Ga}_6]|$  is non-negligible. This is not possible. As a consequence, there exists some non-negligible function  $\varepsilon_7(\kappa)$  such that  $|\mathsf{Pr}[\mathbf{Ga}_7] \mathsf{Pr}[\mathbf{Ga}_6]| = \varepsilon_7(\kappa)$ .
- $\mathbf{Ga}_8$ : This is identical to  $\mathbf{Ga}_7$  excepting  $\mathcal{O}^{\mathcal{AD}}$ substitutes  $\mathbf{Ha}_1$  query on  $\mathbf{ID}^*$  using randomly selected  $\mathbf{h}^* \in \mathbb{F}_q^m$ , replaces the outputs of  $\mathbf{Ha}_2$  and  $\mathbf{Ha}_3$  by a random element of  $\mathbb{F}_q^{\delta}$  and a randomly chosen  $\delta$ -length bit-string respectively. One may argue that  $|\Pr[\mathbf{Ga}_8] - \Pr[\mathbf{Ga}_7]| = \varepsilon_8(\kappa)$  (negligible function) by using the arguments of  $\mathbf{Ga}_1, \mathbf{Ga}_2$ , and  $\mathbf{Ga}_3, \mathbf{Ga}_5, \mathbf{Ga}_6$ , and  $\mathbf{Ga}_7$ .

Therefore,

$$\begin{split} |\Pr[\mathbf{Ga}_8] - \Pr[\mathcal{EXP}_{\mathsf{Mul-CLS}(1^{\kappa})}^{\operatorname{cma-cida-super}} = 1]| \\ &= |\Pr[\mathbf{Ga}_8] - \Pr[\mathbf{Ga}_0]| \\ &\leq |\Pr[\mathbf{Ga}_8] - \Pr[\mathbf{Ga}_7]| + |\Pr[\mathbf{Ga}_7] - \Pr[\mathbf{Ga}_6]| \\ &+ |\Pr[\mathbf{Ga}_6] - \Pr[\mathbf{Ga}_5]| + |\Pr[\mathbf{Ga}_5] - \Pr[\mathbf{Ga}_4]| \\ &+ |\Pr[\mathbf{Ga}_4] - \Pr[\mathbf{Ga}_3]| + |\Pr[\mathbf{Ga}_3] - \Pr[\mathbf{Ga}_2]| \\ &+ |\Pr[\mathbf{Ga}_2] - \Pr[\mathbf{Ga}_1]| + |\Pr[\mathbf{Ga}_1] - \Pr[\mathbf{Ga}_0]| \\ &= \varepsilon_8(\kappa) + \varepsilon_7(\kappa) + \varepsilon_6(\kappa) + \varepsilon_5(\kappa) + \varepsilon_4(\kappa) + \varepsilon_3(\kappa) \\ &+ \varepsilon_2(\kappa) + \varepsilon_1(\kappa) = \epsilon(\kappa) (\text{negligible function}). \end{split}$$

 $\begin{array}{l} \mathrm{Therefore,} \ \mathsf{Adv}_{\mathcal{AD}_{1}}^{\mathcal{EXP}_{\mathsf{Mul}^{\mathsf{cma-cida-super}}}^{\mathrm{cma-cida-super}}} = \mathsf{Pr}[\mathcal{EXP}_{\mathsf{Mul}^{\mathsf{cma-cida-super}}}^{\mathrm{cma-cida-super}} = 1 \\ 1 ] \ \mathrm{is \ same \ as \ } \mathsf{Pr}[\mathbf{Ga}_{8}]. \ \ \mathrm{Hence,} \ \mathsf{Adv}_{\mathcal{AD}_{1}}^{\mathcal{EXP}_{\mathsf{Mul}^{\mathsf{cma-cida-super}}}} \\ \mathrm{non-negligible \ implies \ } \mathsf{Pr}[\mathbf{Ga}_{8}] \ \ \mathrm{non-negligible.} \end{array}$ 

If possible, let  $\Pr[\mathbf{Ga}_8]$  be non-negligible. Then it can be shown that  $\mathcal{O}^{\mathcal{AD}}$  would be able to solve the MQ problem by finding a solution  $\mathbf{v}^*$  of the system  $\mathbf{k}^* = \mathcal{P}_{\mathsf{ID}^*}(\mathbf{z})$  using  $\mathcal{AD}_1$ .

1. The oracle machine  $\mathcal{O}^{\mathcal{AD}}$  generates four valid transcripts  $(\mathsf{COM}, \Omega^{(i)}, \mathsf{RE}_1^{(i)}, \Upsilon^{(j)}, \mathsf{RE}_2^{(i,j)})_{\{i,j=0,1\}}$ with the help of  $\mathcal{AD}_1$  and controlling the output of random oracles Ha<sub>2</sub> and Ha<sub>3</sub>, where

$$\begin{split} \mathsf{COM} &= (e_{0,1}, e_{1,1}, \dots, e_{0,\delta}, e_{1,\delta}) \\ \Omega^{(i)} &= (\alpha_1^{(i)}, \dots, \alpha_{\delta}^{(i)}) \text{ with } \alpha_l^{(0)} \neq \alpha_{\delta}^{(1)} \\ \text{for } l &= 1, \dots, \delta \\ \mathsf{RE}_1^{(i)} &= (\mathbf{b}_{1,1}^{(i)}, \mathbf{c}_{1,1}^{(i)}, \dots, \mathbf{b}_{1,\delta}^{(i)}, \mathbf{c}_{1,\delta}^{(i)} \\ \Upsilon^{(j)} &= (t_1^{(j)}, \dots, t_{\delta}^{(j)}) \text{ with } t_l^{(j)} = j \in \{0,1\} \\ \text{for } l &= 1, \dots, \delta \\ \mathsf{RE}_2^{(i,j)} &= (\mathbf{a}_{j,1}^{(i)}, \dots, \mathbf{a}_{j,\delta}^{(i)}) \end{split}$$

2. For each 
$$l = 1, \ldots, \alpha$$
,

$$\begin{aligned} e_{1,l} &= \mathsf{Comm}(\mathbf{a}_{1,l}^{(0)}, \ \alpha_{l}^{(0)}(\mathbf{k}^{*} - \mathcal{P}_{\mathsf{ID}^{*}}(\mathbf{a}_{1,l}^{(0)}) + \\ \mathcal{P}_{\mathsf{ID}^{*}}(\mathbf{0})) &- \mathcal{G}(\mathbf{b}_{1,l}^{(0)}, \mathbf{a}_{1,l}^{(0)}) - \mathbf{c}_{1,l}^{(0)}) \\ &= \mathsf{Comm}(\mathbf{a}_{1,l}^{(1)}, \ \alpha_{l}^{(1)}(\mathbf{k}^{*} - \mathcal{P}_{\mathsf{ID}^{*}}(\mathbf{a}_{1,l}^{(1)}) \\ &+ \mathcal{P}_{\mathsf{ID}^{*}}(\mathbf{0})) - \mathcal{G}(\mathbf{b}_{1,l}^{(1)}, \mathbf{a}_{1,l}^{(1)}) - \mathbf{c}_{1,l}^{(1)}) \end{aligned}$$
(5)

3. The computationally binding property of the commitment scheme Comm ensures that the arguments of Comm for  $e_{0,l}$  are equal in 4 and for  $e_{1,l}$  are equal in 5. Thus, we have

$$\mathbf{a}_{0,l}^{(0)} = \mathbf{a}_{0,l}^{(1)} \tag{6}$$

$$\alpha_l^{(0)} \mathbf{a}_{0,l}^{(0)} - \mathbf{b}_{1,l}^{(0)} = \alpha_l^{(1)} \mathbf{a}_{0,l}^{(1)} - \mathbf{b}_{1,l}^{(1)}$$
(7)

$$\alpha_l^{(0)} \mathcal{P}_{\mathsf{ID}^*}(\mathbf{a}_{0,l}^{(0)}) - \mathbf{c}_{1,l}^{(0)} = \alpha_l^{(1)} \mathcal{P}_{\mathsf{ID}^*}(\mathbf{a}_{0,l}^{(1)}) - \mathbf{c}_{1,l}^{(1)} \quad (8)$$

$$\mathbf{a}_{1,l}^{(0)} = \mathbf{a}_{1,l}^{(1)} \tag{9}$$

$$\begin{aligned} \alpha_{l}^{(0)}(\mathbf{k}^{*} - \mathcal{P}_{\mathsf{ID}^{*}}(\mathbf{a}_{1,l}^{(0)}) + \mathcal{P}_{\mathsf{ID}^{*}}(\mathbf{0})) &- \mathcal{G}(\mathbf{b}_{1,l}^{(0)}, \mathbf{a}_{1,l}^{(0)}) - \mathbf{c}_{1,l}^{(0)} \\ &= \alpha_{l}^{(1)}(\mathbf{k}^{*} - \mathcal{P}_{\mathsf{ID}^{*}}(\mathbf{a}_{1,l}^{(1)}) + \mathcal{P}_{\mathsf{ID}^{*}}(\mathbf{0})) - \mathcal{G}(\mathbf{b}_{1,l}^{(1)}, \\ &\mathbf{a}_{1,l}^{(1)}) - \mathbf{c}_{1,l}^{(1)} \end{aligned}$$
(10)

4. From the equations 9 and 10,

$$\begin{aligned} & (\alpha_{l}^{(0)} - \alpha_{l}^{(1)})(\mathbf{k}^{*} - \mathcal{P}_{\mathsf{ID}^{*}}(\mathbf{a}_{1,l}^{(0)}) + \mathcal{P}_{\mathsf{ID}^{*}}(\mathbf{0})) = \\ & \mathcal{G}(\mathbf{b}_{1,l}^{(0)}, \mathbf{a}_{1,l}^{(0)}) - \mathcal{G}(\mathbf{b}_{1,l}^{(1)}, \mathbf{a}_{1,l}^{(1)}) + \mathbf{c}_{1,l}^{(0)} - \mathbf{c}_{1,l}^{(1)} \\ & \Rightarrow (\alpha_{l}^{(0)} - \alpha_{l}^{(1)})(\mathbf{k}^{*} - \mathcal{P}_{\mathsf{ID}^{*}}(\mathbf{a}_{1,\rho}^{(0)}) + \mathcal{P}_{\mathsf{ID}^{*}}(\mathbf{0})) = \mathcal{G}(\mathbf{b}_{1,l}^{(0)}) \\ & - \mathbf{b}_{1,l}^{(1)}, \mathbf{a}_{1,l}^{(0)}) + \mathbf{c}_{1,l}^{(0)} - \mathbf{c}_{1,l}^{(1)} \end{aligned}$$
(11)

5. From 6, 7, 8 and 11

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

6. Thus, the oracle machine  $\mathcal{O}^{\mathcal{AD}}$  extracts a solution  $\mathbf{a}_{0,l}^{(0)} + \mathbf{a}_{1,l}^{(0)}$  of  $\mathbf{k}^* = \mathcal{P}_{\mathsf{ID}^*}(\mathbf{z})$  i.e.,  $\mathbf{k}^* = \mathcal{P}_{\mathsf{ID}^*}(\mathbf{a}_{0,l}^{(0)} + \mathbf{a}_{1,l}^{(0)})$ .

Thus,  $\Pr[\mathbf{Ga}_8]$  is non-negligible implies  $\mathcal{O}^{\mathcal{AD}}$  is able to determine a solution of the MQ problem  $\mathbf{k}^* = \mathcal{P}_{\mathsf{ID}^*}(\mathbf{z})$ . It contradicts the assumption that MQ problem is NP-hard. Consequently,  $\Pr[\mathbf{Ga}_8]$  is negligible which ensures that  $\mathsf{Adv}_{\mathcal{AD}_1}^{\mathsf{Cma-cida-super}} =$  $\Pr[\mathcal{EXP}_{Mul^-CLS(1^\kappa)}^{\mathsf{cma-cida-super}} = 1]$  is negligible. Therefore, we may conclude that the proposed Mul-CLS attains existential unforgeability against a chosen message and chosen identity Super Type I adversary.  $\Box$ 

THEOREM 4.2. The proposed scheme Mul-CLS is existentially unforgeable against chosen message and chosen identity Super Type II adversary under the hardness of MQ problem, if

- (i) the underlying commitment scheme Comm is computationally binding and perfectly hiding.
- ii) the hash functions Ha<sub>1</sub>, Ha<sub>2</sub>, and Ha<sub>3</sub> are designed as random oracles.

We use the method of contradiction to prove **Proof:** the security of Mul-CLS against a chosen message and chosen identity Super Type II adversary. Consider an adversary  $\mathcal{AD}_2$  with non-negligible success probability in the game defined in the Section 2.5.2 for Mul-CLS. We now play a series of games  $Ga_0, \ldots, Ga_7$  to construct an oracle machine  $\mathcal{O}^{\mathcal{A}\mathcal{D}}$  for solving the MQ problem with the help of  $\mathcal{AD}_2$  and managing outputs of the random oracles  $Ha_1$ ,  $Ha_2$ , and  $Ha_3$ . Note  $Ga_i$  is obtained by slight modification of  $\mathbf{Ga}_{i-1}$  for  $i = 1, \ldots, 7$ . Let the success probability of  $\mathcal{AD}_2$  in  $\mathbf{Ga}_i$  be  $\mathsf{Pr}[\mathbf{Ga}_i]$ .

- $Ga_0$ :  $Ga_0$  is nothing but the game defined in the Section 2.5.2 for Mul-CLS. As a consequence,  $\mathsf{Adv}_{\mathcal{AD}_2}^{\mathsf{EXP}_{\mathsf{Mul-CLS}(1^\kappa)}^{\mathrm{cma-cida-super}}}$  $= \Pr[\mathcal{EXP}_{\mathsf{Mul-Cl}\,\mathsf{S}(1^{\kappa})}^{\text{cma-cida-super}}]$ = 1] =  $\Pr[\mathbf{Ga}_0].$
- $Ga_1$ : It is similar to  $Ga_0$  except that during Create User query, the oracle machine  $\mathcal{O}^{\mathcal{AD}}$ 
  - randomly selects  $\mathbf{s}_{\mathsf{ID}} \in \mathbb{F}_q^n$ , and substitutes 1. Ha<sub>1</sub>'s output on ID by  $\mathbf{h}_{\text{ID}} = \mathcal{P}(\mathbf{s}_{\text{ID}})$ ,
  - 2. randomly picks  $\mathbf{w}_{\mathsf{ID}} \in \mathbb{F}_q^n$ ,
  - randomly chooses a system of quadratic 3. multivariate polynomials  $\mathcal{R}_{\mathsf{ID}}: \mathbb{F}_q^n \to \mathbb{F}_q^m$  and computes  $\mathcal{R}_{\mathsf{ID}}(\mathbf{w}_{\mathsf{ID}}) = \mathbf{r}_{\mathsf{ID}}$ ,
  - replaces Create User queries output by 4.  $\langle \mathsf{ID}, \mathbf{s}_{\mathsf{ID}}, \mathbf{w}_{\mathsf{ID}}, (\mathcal{R}_{\mathsf{ID}}, \mathbf{h}_{\mathsf{ID}}, \mathbf{r}_{\mathsf{ID}}) \rangle.$

 $|\Pr[\mathbf{Ga}_1] - \Pr[\mathbf{Ga}_0]|$  is non-negligible implies  $\mathcal{AD}_2$ can be used to distinguish Ha<sub>1</sub>'s distributions. This is impossible. Consequently,  $|\Pr[\mathbf{Ga}_1] - \Pr[\mathbf{Ga}_0]| =$  $\varepsilon_1(\kappa)$ , where  $\varepsilon_1(\kappa)$  is a negligible function.

- $\mathbf{Ga}_2$ : It is same as  $\mathbf{Ga}_1$  except that during Public Key Replace query, the oracle machine  $\mathcal{O}^{\mathcal{AD}}$ 
  - randomly selects  $\mathbf{s}'_{\mathsf{ID}} \in \mathbb{F}_q^n$ , and replaces  $\mathsf{Ha}_1$ 's 1. output on ID by  $\mathbf{h}'_{\text{ID}} = \mathcal{P}(\mathbf{s}'_{\text{ID}}),$
  - randomly chooses a system of quadratic 2.multivariate polynomials  $\mathcal{R}'_{\mathsf{ID}}$  :  $\mathbb{F}_q^n \to \mathbb{F}_q^m$ , and computes  $\mathcal{R}'_{\mathsf{ID}}(\mathbf{w}'_{\mathsf{ID}}) = \mathbf{r}'_{\mathsf{ID}}$ ,
  - 3. substitutes the public key  $pk_{\rm ID}$  with  $pk'_{\rm ID} =$  $(\mathcal{R}'_{\mathsf{ID}}, \mathbf{h}'_{\mathsf{ID}}, \mathbf{r}'_{\mathsf{ID}}).$

If  $|\Pr[\mathbf{Ga}_2] - \Pr[\mathbf{Ga}_1]|$  is non-negligible then one may use  $\mathcal{AD}_2$  in order to distinguish with Ha<sub>1</sub>'s distributions which is impossible. Hence, there exists a negligible function  $\varepsilon_2(\kappa)$  such that  $|\mathsf{Pr}[\mathbf{Ga}_2] - \mathsf{Pr}[\mathbf{Ga}_1]| = \varepsilon_2(\kappa).$ 

- $Ga_3$ : This game is analogues to  $Ga_2$ , apart from the fact that  $\mathcal{O}^{\mathcal{AD}}$  randomly selects  $\mathbf{w}'_{\mathsf{ID}} \in \mathbb{F}_{q}^{n}$ and replaces the secret value with  $\mathbf{w'}_{\mathsf{ID}}$  during Set Secret Value query.  $|\Pr[\mathbf{Ga}_4] - \Pr[\mathbf{Ga}_3]|$  is nonnegligible implies  $\mathcal{AD}_2$  can be utilized for distinguishing  $\mathcal{O}^{\mathcal{A}\mathcal{D}}$ 's output sequence from a random sequence which is not possible. Consequently,  $|\Pr[\mathbf{Ga}_4] - \Pr[\mathbf{Ga}_3]| = \varepsilon_3(\kappa)$ , where  $\varepsilon_3(\kappa)$  is a negligible function.
- $Ga_4$ : It is identical to  $Ga_3$  except that during Super Sign query, the oracle machine  $\mathcal{O}^{\mathcal{AD}}$ 
  - 1.
  - randomly chooses  $\mathbf{s}_{\mathsf{ID}} \in \mathbb{F}_q^n$ , randomly selects  $\mathbf{w}_{\mathsf{ID}} \in \mathbb{F}_q^n$  by accessing the 2. oracle Secret Value Extract,
  - 3. computes  $\mathcal{R}_{ID}(\mathbf{w}_{ID}) = \mathbf{r}_{ID}$  where system of quadratic multivariate polynomials  $\mathcal{R}_{ID}$  is received through oracle Create-user,
  - 4. replaces the output of  $Ha_1$  on ID by  $h_{ID}$  =  $\mathcal{P}(\mathbf{s}_{\mathsf{ID}}),$
  - substitutes the signature by  $\chi$  which is 5.produced by using secret key  $\mathbf{s}_{\mathsf{ID}} || \mathbf{w}_{\mathsf{ID}}$  for the system  $\mathcal{P}_{\mathsf{ID}}(\mathbf{z}) = \mathcal{P}(\mathbf{x}) + \mathcal{R}_{\mathsf{ID}}(\mathbf{y}) = \mathbf{h}_{\mathsf{ID}} + \mathbf{r}_{\mathsf{ID}} =$ kin.

If  $|\Pr[\mathbf{Ga}_4] - \Pr[\mathbf{Ga}_3]|$  is non-negligible then  $\mathcal{AD}_2$ can be used for distinguishing Ha<sub>1</sub>'s distributions. This is impossible. As a consequence,  $|\Pr[\mathbf{Ga}_4] \Pr[\mathbf{Ga}_3] = \varepsilon_4(\kappa)$ , a negligible function.

- $Ga_5$ : This game is similar to  $Ga_4$  excepting  $\mathcal{O}^{\mathcal{AD}}$  replaces Ha<sub>2</sub>'s output by a randomly chosen element from  $\mathbb{F}_q^{\delta}$ . It is possible to use  $\mathcal{AD}_2$  for distinguishing  $Ha_2$ 's distributions if  $|Pr[Ga_5] \Pr[\mathbf{Ga}_4]$  is non-negligible, which is not possible. Thereby, a negligible function  $\varepsilon_5(\kappa)$  exists such that  $|\Pr[\mathbf{Ga}_5] - \Pr[\mathbf{Ga}_4]| = \varepsilon_5(\kappa)$ .
- $\mathbf{Ga}_6$ : It is identical to  $\mathbf{Ga}_5$  apart from the fact that  $\mathcal{O}^{\mathcal{AD}}$  replaces  $Ha_3$ 's output by a randomly chosen bit-string of length  $\delta$ . Note that one can use  $\mathcal{AD}_2$  in order to distinguish Ha<sub>3</sub>'s distributions if  $|\Pr[\mathbf{Ga}_6] - \Pr[\mathbf{Ga}_5]|$  is non-negligible. This impossible. As a consequence, there exists some non-negligible function  $\varepsilon_6(\kappa)$  such that  $|\Pr[\mathbf{Ga}_6] -$  $\Pr[\mathbf{Ga}_5]| = \varepsilon_6(\kappa).$
- $\mathbf{Ga}_7$ : This is identical to  $\mathbf{Ga}_6$  excepting  $\mathcal{O}^{\mathcal{AD}}$ substitutes  $Ha_1$  query on  $ID^*$  using randomly selected  $\mathbf{h}^* \in \mathbb{F}_q^m$ , replaces the outputs of Ha<sub>2</sub> and  $Ha_3$  by a random element of  $\mathbb{F}_q^{\delta}$  and a randomly selected  $\delta$ -length bit-string respectively. We can argue that  $|\Pr[\mathbf{Ga}_7] - \Pr[\mathbf{Ga}_6]| = \varepsilon_7(\kappa)$  (negligible function) by utilizing the similar arguments as mentioned  $\mathbf{Ga}_1$ ,  $\mathbf{Ga}_2$ ,  $\mathbf{Ga}_4$ ,  $\mathbf{Ga}_5$ , and  $\mathbf{Ga}_6$ .

Therefore,

$$\begin{split} |\Pr[\mathbf{Ga}_{7}] - \Pr[\mathcal{EXP}_{\mathsf{Mul-CLS}(1^{\kappa})}^{cma-cida-super} = 1]| \\ &= |\Pr[\mathbf{Ga}_{7}] - \Pr[\mathbf{Ga}_{0}]| \\ &\leq |\Pr[\mathbf{Ga}_{7}] - \Pr[\mathbf{Ga}_{6}]| + |\Pr[\mathbf{Ga}_{6}] - \Pr[\mathbf{Ga}_{5}]| \\ &+ |\Pr[\mathbf{Ga}_{7}] - \Pr[\mathbf{Ga}_{4}]| + |\Pr[\mathbf{Ga}_{4}] - \Pr[\mathbf{Ga}_{3}]| \\ &+ |\Pr[\mathbf{Ga}_{3}] - \Pr[\mathbf{Ga}_{2}]| + |\Pr[\mathbf{Ga}_{2}] - \Pr[\mathbf{Ga}_{1}]| \\ &+ |\Pr[\mathbf{Ga}_{1}] - \Pr[\mathbf{Ga}_{0}]| \\ &= \varepsilon_{7}(\kappa) + \varepsilon_{6}(\kappa) + \varepsilon_{5}(\kappa) + \varepsilon_{4}(\kappa) + \\ &\varepsilon_{3}(\kappa) + \varepsilon_{2}(\kappa) + \varepsilon_{1}(\kappa) = \epsilon(\kappa) (\text{negligible function}). \end{split}$$

Thereby, 
$$\operatorname{\mathsf{Adv}}_{\mathcal{AD}_2}^{\mathcal{EXP}_{\operatorname{\mathsf{Mul-CLS}}(1^{\kappa})}^{\operatorname{cma-cida-super}}} = \Pr[\mathcal{EXP}_{\operatorname{\mathsf{Mul-CLS}}(1^{\kappa})}^{\operatorname{cma-cida-super}} = 1]$$
  
is same as  $\Pr[\mathbf{Ga}_7]$ . Thus,  $\operatorname{\mathsf{Adv}}_{\mathcal{AD}_2}^{\mathcal{EXP}_{\operatorname{\mathsf{Mul-CLS}}(1^{\kappa})}^{\operatorname{cma-cida-super}}}$  is non-negligible implies  $\Pr[\mathbf{Ga}_7]$  non-negligible.

If possible let  $\Pr[\mathbf{Ga}_7]$  be non-negligible. Then it is possible to show that  $\mathcal{O}^{\mathcal{AD}}$  can break the MQ problem by finding a solution  $\mathbf{v}^*$  of the system  $\mathbf{k}^* - \mathcal{P}(\mathbf{x}^*) = \mathcal{R}_{\mathsf{ID}^*}(\mathbf{y})$  using  $\mathcal{AD}_2$ .

1. The oracle machine  $\mathcal{O}^{\mathcal{AD}}$  generates four valid transcripts (COM,  $\Omega^{(i)}$ ,  $\mathsf{RE}_1^{(i)}$ ,  $\Upsilon^{(j)}$ ,  $\mathsf{RE}_2^{(i,j)}$ )<sub>{i,j=0,1}</sub> with the help of  $\mathcal{AD}_2$  and controlling the output of random oracles Ha<sub>2</sub> and Ha<sub>3</sub>, where

$$\begin{split} \mathsf{COM} &= (e_{0,1}, e_{1,1}, \dots, e_{0,\delta}, e_{1,\delta}) \\ \Omega^{(i)} &= (\alpha_1^{(i)}, \dots, \alpha_{\delta}^{(i)}) \text{ with } \alpha_l^{(0)} \neq \alpha_{\delta}^{(1)} \\ \text{for } l &= 1, \dots, \delta \\ \mathsf{RE}_1^{(i)} &= (\mathbf{b}_{1,1}^{(i)}, \mathbf{c}_{1,1}^{(i)}, \dots, \mathbf{b}_{1,\delta}^{(i)}, \mathbf{c}_{1,\delta}^{(i)} \\ \Upsilon^{(j)} &= (t_1^{(j)}, \dots, t_{\delta}^{(j)}) \text{ with } t_l^{(j)} = j \in \{0, 1\} \\ \text{for } l = 1, \dots, \delta \\ \mathsf{RE}_2^{(i,j)} &= (\mathbf{a}_{j,1}^{(i)}, \dots, \mathbf{a}_{j,\delta}^{(i)}) \end{split}$$

2. For each  $l = 1, \ldots, \alpha$ ,

$$e_{0,l} = \mathsf{Comm}(\mathbf{a}_{0,l}^{(0)}, \ \alpha_l^{(0)} \mathbf{a}_{0,l}^{(0)} - \mathbf{b}_{1,l}^{(0)}, \ \alpha_l^{(0)} \mathcal{P}_{\mathsf{ID}^*}(\mathbf{a}_{0,l}^{(0)}) - \mathbf{c}_{1,l}^{(0)})$$

$$= \operatorname{Comm} \left( \mathbf{a}_{0,l}^{(1)}, \ \alpha_l^{(1)} \mathbf{a}_{0,l}^{(1)} - \mathbf{b}_{1,l}^{(1)}, \ \alpha_l^{(1)} \mathcal{P}_{\mathsf{ID}^*}(\mathbf{a}_{0,l}^{(1)}) - \mathbf{c}_{1,l}^{(1)} \right)$$
(12)

$$\begin{split} e_{1,l} &= \mathsf{Comm}(\mathbf{a}_{1,l}^{(0)}, \ \alpha_l^{(0)}(\mathbf{k}^* - \mathcal{P}_{\mathsf{ID}^*}(\mathbf{a}_{1,l}^{(0)}) + \mathcal{P}_{\mathsf{ID}^*}(\mathbf{0})) \\ &- \mathcal{G}(\mathbf{b}_{1,l}^{(0)}, \mathbf{a}_{1,l}^{(0)}) - \mathbf{c}_{1,l}^{(0)}) \end{split}$$

$$= \operatorname{Comm}(\mathbf{a}_{1,l}^{(1)}, \ \alpha_l^{(1)}(\mathbf{k}^* - \mathcal{P}_{\mathsf{ID}^*}(\mathbf{a}_{1,l}^{(1)}) + \mathcal{P}_{\mathsf{ID}^*}(\mathbf{0})) \\ -\mathcal{G}(\mathbf{b}_{1,l}^{(1)}, \mathbf{a}_{1,l}^{(1)}) - \mathbf{c}_{1,l}^{(1)})$$
(13)

3. The computationally binding property of the commitment scheme Comm ensures that the arguments of Comm for  $e_{0,l}$  are equal in 12 and for  $e_{1,l}$  are equal in 13. Thus, we have

$$\mathbf{a}_{0,l}^{(0)} = \mathbf{a}_{0,l}^{(1)} \tag{14}$$

$$\alpha_l^{(0)} \mathbf{a}_{0,l}^{(0)} - \mathbf{b}_{1,l}^{(0)} = \alpha_l^{(1)} \mathbf{a}_{0,l}^{(1)} - \mathbf{b}_{1,l}^{(1)}$$
(15)

$$\alpha_l^{(0)} \mathcal{P}_{\mathsf{ID}^*}(\mathbf{a}_{0,l}^{(0)}) - \mathbf{c}_{1,l}^{(0)} = \alpha_l^{(1)} \mathcal{P}_{\mathsf{ID}^*}(\mathbf{a}_{0,l}^{(1)}) - \mathbf{c}_{1,l}^{(1)}$$
(16)

$$\mathbf{a}_{1,l}^{(0)} = \mathbf{a}_{1,l}^{(1)} \tag{17}$$

$$\alpha_l^{(0)}(\mathbf{k}^* - \mathcal{P}_{\mathsf{ID}^*}(\mathbf{a}_{1,l}^{(0)}) + \mathcal{P}_{\mathsf{ID}^*}(\mathbf{0})) - \mathcal{G}(\mathbf{b}_{1,l}^{(0)}, \mathbf{a}_{1,l}^{(0)}) - \mathbf{c}_{1,l}^{(0)}$$

$$= \alpha_{l}^{(1)}(\mathbf{k}^{*} - \mathcal{P}_{\mathsf{ID}^{*}}(\mathbf{a}_{1,l}^{(1)}) + \mathcal{P}_{\mathsf{ID}^{*}}(\mathbf{0})) - \mathcal{G}(\mathbf{b}_{1,l}^{(1)}, \mathbf{a}_{1,l}^{(1)}) - \mathbf{c}_{1,l}^{(1)}$$

$$(18)$$

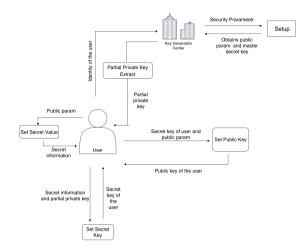
4. From the equations 17 and 18,

$$\begin{aligned} &(\alpha_{l}^{(0)} - \alpha_{l}^{(1)})(\mathbf{k}^{*} - \mathcal{P}_{\mathsf{ID}^{*}}(\mathbf{a}_{1,l}^{(0)}) + \mathcal{P}_{\mathsf{ID}^{*}}(\mathbf{0})) = \mathcal{G}(\mathbf{b}_{1,l}^{(0)}, \\ &\mathbf{a}_{1,l}^{(0)}) - \mathcal{G}(\mathbf{b}_{1,l}^{(1)}, \mathbf{a}_{1,l}^{(1)}) + \mathbf{c}_{1,l}^{(0)} - \mathbf{c}_{1,l}^{(1)} \\ &\Rightarrow (\alpha_{l}^{(0)} - \alpha_{l}^{(1)})(\mathbf{k}^{*} - \mathcal{P}_{\mathsf{ID}^{*}}(\mathbf{a}_{1,\rho}^{(0)}) + \mathcal{P}_{\mathsf{ID}^{*}}(\mathbf{0})) = \\ &\mathcal{G}(\mathbf{b}_{1,l}^{(0)} - \mathbf{b}_{1,l}^{(1)}, \mathbf{a}_{1,l}^{(0)}) + \mathbf{c}_{1,l}^{(0)} - \mathbf{c}_{1,l}^{(1)} \end{aligned}$$
(19)

5. From 14, 15, 16 and 19

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

- 6. Hence, the oracle machine  $\mathcal{O}^{\mathcal{AD}}$  is able to extract a solution  $\mathbf{a}_{0,l}^{(0)} + \mathbf{a}_{1,l}^{(0)}$  of  $\mathbf{k}^* = \mathcal{P}_{\mathsf{ID}^*}(\mathbf{z})$  i.e.,  $\mathbf{k}^* = \mathcal{P}_{\mathsf{ID}^*}(\mathbf{a}_{0,l}^{(0)} + \mathbf{a}_{1,l}^{(0)})$ .
- 7. From the Step 6, we have  $\mathbf{k}^* = \mathcal{P}_{\mathsf{ID}^*}(\mathbf{a}_{0,l}^{(0)} + \mathbf{a}_{1,l}^{(0)}) = \mathcal{P}(\mathbf{x}^*) + \mathcal{R}_{\mathsf{ID}^*}(\mathbf{y}^*)$ . Therefore, we have  $\mathcal{R}_{\mathsf{ID}^*}(\mathbf{y}^*) = \mathbf{k}^* \mathcal{P}(\mathbf{x}^*)$ . Thus the oracle machine  $\mathcal{O}^{\mathcal{AD}}$  extracts a solution  $\mathbf{y}^*$  of  $\mathbf{k}^* \mathcal{P}(\mathbf{x}^*) = \mathcal{R}_{\mathsf{ID}^*}(\mathbf{y})$



**FIGURE 2.** A workflow diagram depicting the communication flow of the proposed Mul-CLS: Part I



**FIGURE 3.** A workflow diagram depicting the communication flow of the proposed Mul-CLS: Part II

Therefore,  $\Pr[\mathbf{Ga}_7]$  is non-negligible implies  $\mathcal{O}^{\mathcal{AD}}$ is able to find a solution of the MQ problem  $\mathbf{k}^*$  =  $\mathcal{R}_{\mathsf{ID}^*}(\mathbf{y})$  without knowing  $\mathcal{R}_{\mathsf{ID}^*}^{-1}$ . It contradicts the assumption that MQ problem is NP-hard. As a consequence,  $\Pr[\mathbf{Ga}_7]$  is negligible which makes sure  $\mathcal{EXP}_{\mathsf{Mul-CLS}(1^{\kappa})}^{\mathrm{cma-cida-super}}$ that  $\mathsf{Adv}_{\mathcal{AD}_2}$  $= \mathsf{Pr}[\mathcal{EXP}^{\scriptscriptstyle{\mathrm{cma-cida-super}}}_{\mathsf{Mul-CLS}(1^{\kappa})}$ 1] is negligible. Thus, we can conclude that the proposed Mul-CLS is existentially unforgeable against chosen message and chosen identity Super Type II adversary.

# 5. EFFICIENCY

In this section, we discuss the communication and storage complexity of our proposed Mul-CLS. In particular, sizes of master public key mpk, master secret key msk, secret key of user, and signature are respectively  $\frac{m(n+2)(n+1)}{2}$  field ( $\mathbb{F}_q$ ) elements,  $n^2 + m^2 + c$  field ( $\mathbb{F}_q$ ) elements, 2n field ( $\mathbb{F}_q$ ) elements, and  $2\delta \cdot |\mathsf{Comm}| + \delta \cdot (m + 4n)\log_2 q + n\log_2 q$  bits. Here  $n, m, c, \delta$ ,  $|\mathsf{Comm}|$ , and q denote respectively the number of variables, number of equations, size of the central map, number of rounds of the underlying identification scheme, size of the commitment scheme, and the cardinality of the underlying field. We summarize the data in Table 1.

We now discuss the findings of our comparative analysis. The security of [10, 27, 9, 8, 4, 28, 5, 29, 30] relies on number-theoretic hardness assumptions.

TABLE 1. Communication and storage costs of Mul-CLS

 <b>TABLE 1.</b> Communication and storage costs of Mul-CE.					
mpk size	$\frac{m(n+2)(n+1)}{2}$ field ( $\mathbb{F}_q$ ) elements				
msk size	$n^2 + m^2 + c$ field ( $\mathbb{F}_q$ ) elements				
User's secret key size	$2n$ field $(\mathbb{F}_q)$ elements				
User's public key size	$\frac{m(n+2)(n+1)}{2} + 2m$ field ( $\mathbb{F}_q$ ) elements				
Signature size	$2\delta \cdot  Comm  + \delta \cdot (m+4n)\log_2 q + n\log_2 q$ bits				

**TABLE 2.** Running time complexity of Mul-CLS for 80 bit security level over GF(31)

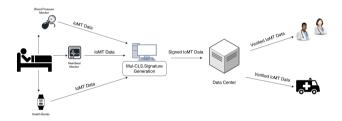
	Time (in seconds)
Setup Phase	1.45
Partial Private Key Extract	0.062
Set Secret Value	0.001
Set Secret Key	$7 \times 10^{-6}$
Set Public Key	1.32
Signature	0.089
Verification	0.029

Therefore, as soon as an adversary get access to large scale quantum computers, it can very easily mount an attack on these schemes, and make them obsolete, insecure and useless. We point out that although the size of signature is large in our scheme, MPKCbased schemes are very fast, and can efficiently work on memory-constraint devices. This is because the core operations required in MPKC are only binary modular field multiplications and additions. Research has shown that MPKC schemes can be efficiently implemented on low cost devices like smart cards and RFID chips, and they outperform most of their competitors with regard to performance [31, 32, 33, 34, 35]. This makes MPKC schemes a promising candidate for the security of the IoMT systems. In addition, unlike classical schemes, our proposed Mul-CLS provides security against the threat of quantum computers. Thus, Mul-CLS has compensatory advantages which gives it an upper hand over existing classical CLS.

# 6. APPLICATION TO INTERNET OF MED-ICAL THINGS

Ensuring the integrity and authenticity of sensitive data in an computationally-limited IoMT network is of utmost importance. Large number of devices are connected to an IoMT network, and if the digital identity (example IP address) of a device is not securely authenticated, it can jeopardize the system. Thus. authenticating the identity of machines connected in IoMT systems is also one of the major tasks. Given the context of the situation, a signature scheme appears to be an efficient cryptographic primitive that helps to address security issues. Unfortunately, conventional signature schemes in the current state of the art, either it is PKI-based or IBC-based primitives, can not work efficiently within IoMT systems. This is due to the fact that devices connected in an IoMT systems, for example blood pressure monitor etc, are very tiny and autonomous which places down constraints on power and storage capabilities. The problem with PKI-based signature primitives is that it requires certificate management. This results in large amount of computational-overhead and communication-cost, making it unsuitable for IoMT networks. The IBCbased signature primitives circumvents the need of certificates, but the inherent problem of key escrow makes it unsuitable for deployment in large-scale IoMT networks. In view of the circumstances, our proposed certificateless signature scheme Mul-CLS is an efficient and resilient cryptographic primitive that can be employed to build robust IoMT systems.

The proposed design Mul-CLS is a viable cryptographic primitive that addresses all the security issue mentioned above at one go. Mul-CLS provides advanced security features like undeniability and unforgeability. In addition, by using Mul-CLS, a verifier can check whether the message was altered during the transmission or not to ensure the integrity of transmitted data. It not only circumvents the heavy cost of certificate management, but also addresses the issue of key escrow of IBC-based cryptosystem.



**FIGURE 4.** Application of Mul-CLS in IoMT: Health Data collected by IoMT devices like Heartbeat monitor and Blood pressure monitor are signed before transmitted. After receiving the data from the connected and authorized devices, Data center (DC) verify the validity of the signature to assess the authenticity and integrity of the received data.

IoMT devices like wearable biosensor have very restricted computing bandwidth and processing power. Therefore, it is very important to ensure that computation time and bandwidth required for generating signatures in an IoMT setting should be as least as possible. Our proposed design is based on MPKC. Research [31, 32, 33, 34, 35] demonstrate that multivariate-based schemes can be implemented very efficiently, and outperform most of their competitors with regard to performance. Hence, cryptographic-primitives built using MPKC are ideally suited for low-end IoMT devices. Implementation of the proposed scheme only requires modest computational resources; basically doing finite field multiplication and additions. Thus, Mul-CLS being a scheme based on a MPKC, is by and large fast, and requires only inexpensive computing resources that makes it ideal for use on economical and budget devices which forms a part of an IoMT network. In short, Mul-CLS provides strong security guarantees like authenticity, integrity, and undeniability, in a cost-effective manner (re-

**TABLE 3.** List of notations and symbols used in the article

KGC	Key generation center	
CLS	Certificateless signature	
MQ	MQ Multivariate Quadratic	
MPKC	C Multivariate public key cryptography	
IoMT	T Internet of Medical Things	
PKI	KI Public key infrastructure	
IBC	IBC Identity based cryptography	
msk	msk master secret key	
mpk	mpk master public key	
SID	s <sub>ID</sub> partial private key	
pp	pp public parameter	
WID	secret information	
$\mathbb{F}_q$	Finite field of order $q$	
n	number of equations	
m	m number of variables	
Ha1, Ha2, Ha3	Cryptographically secure hash functions	
Comm	Commitment scheme	
ID	Identity of the user	
pk <sub>ID</sub>	public key corresponding to the user with identity ID	
skid	secret key corresponding to the user with identity ID	
1 <sup>κ</sup>	security parameter	
msg	message	
χ	signature	
δ	number of rounds of the underlying identification scheme	

fer to Figure 4). IoMT systems deals with very delicate and sensitive health related data, and thus, ensuring the security of such system is of critical importance. Currently used solutions are based on the number-theoretic hardness assumptions, but advent of quantum computers in near future will completely break these IoMT systems. Our proposed design Mul-CLS addresses this issue as well. It is built on the top of the intractability of MQ problem which is assumed to be NP-hard [19]. Hence, Mul-CLS can resist attacks by quantum computers. As a consequence, by employing Mul-CLS, we can build efficient and robust IoMT system with future security guarantees.

# 7. CONCLUSION

This work presented the design and analysis of provably secure multivariate-based certificateless signature scheme Mul-CLS. The scheme is constructed by putting to use a secure MPKC-based signature in company with Sakumoto et al. [20]'s identification protocol as the fundamental building blocks. Our proposed design is existentially unforgeable against chosen message and chosen identity Super Type I and Super Type II adversaries in ROM. To the best of our knowledge, the Mul-CLS is the *first* multivariate based CLS. Our scheme is ideally suited for IoMT where ensuring the integrity and authenticity of the transmitted data is of utmost importance. Mul-CLS is fast, inexpensive, efficient, and requires only modest computational resources for working owing to the fact that it is a MPKC based scheme. Being a certificateless based cryptographic primitive, Mul-CLS avoids the computationally heavy task of certificate management and key escrow problem. Thus, it can be employed to build secure large-scale IoMT networks. In other words, by making use of Mul-CLS as a cryptographic building block, we can build robust, computationally-inexpensive, and post quantum-secure IoMT networks while logically addressing the security challenges up front.

**Data Availability Statement:** Data sharing not applicable to this article as no new data were generated or analysed in support of this research.

## ACKNOWLEDGEMENTS

This research work was supported by Graduate Assistantships in Developing Countries(GRAID) Program by International Mathematical Union (IMU).

#### REFERENCES

- [1] Adams, C. and Lloyd, S. Understanding public-key infrastructure: concepts, standards, and deployment considerations. Sams Publishing.
- [2] Shamir, A. Identity-based cryptosystems and signature schemes. In Blakley, G. R. and Chaum, D. (eds.), *Advances in Cryptology*, Santa Barbara California USA, pp. 47–53. Springer Berlin Heidelberg.
- [3] Al-Riyami, S. S. and Paterson, K. G. Certificateless public key cryptography. In Laih, C.-S. (ed.), Advances in Cryptology - ASIACRYPT 2003, Taipei, Taiwan, November 30 – December 4, 2003, pp. 452–473. Springer Berlin Heidelberg.
- [4] Wang, W., Xu, H., Alazab, M., Gadekallu, T. R., Han, Z., and Su, C. Blockchain-based reliable and efficient certificateless signature for iiot devices. *IEEE Transactions on Industrial Informatics*, Early Access.
- [5] Du, H., Wen, Q., Zhang, S., and Gao, M. A new provably secure certificateless signature scheme for internet of things. *Ad Hoc Networks*, **100**, 102074.
- [6] Mei, Q., Zhao, Y., and Xiong, H. A new provably secure certificateless signature with revocation in the standard model. *Informatica*, **30**, 711–728.
- [7] Hussain, S., Ullah, S. S., Gumaei, A., Al-Rakhami, M., Ahmad, I., and Arif, S. M. A novel efficient certificateless signature scheme for the prevention of content poisoning attack in named data networkingbased internet of things. *IEEE Access*, 9, 40198–40215.
- [8] Thumbur, G., Rao, G. S., Reddy, P. V., Gayathri, N., and Reddy, D. R. K. Efficient pairing-free certificateless signature scheme for secure communication in resourceconstrained devices. *IEEE Communications Letters*, 24, 1641–1645.
- [9] Xu, Z., He, D., Kumar, N., and Choo, K.-K. R. Efficient certificateless aggregate signature scheme for performing secure routing in vanets. *Security and Communication Networks*, 2020.
- [10] Yang, X., Pei, X., Chen, G., Li, T., Wang, M., and Wang, C. A strongly unforgeable certificateless signature scheme and its application in iot environments. *Sensors*, **19**, 2692.
- [11] Yang, W., Wang, S., and Mu, Y. An enhanced certificateless aggregate signature without pairings for e-healthcare system. *IEEE Internet of Things Journal*, 8, 5000–5008.
- [12] Zhang, Y., Deng, R. H., Zheng, D., Li, J., Wu, P., and Cao, J. Efficient and robust certificateless signature

for data crowdsensing in cloud-assisted industrial iot. *IEEE Transactions on Industrial Informatics*, **15**, 5099–5108.

- [13] Zhao, Y., Hou, Y., Wang, L., Kumari, S., Khan, M. K., and Xiong, H. An efficient certificateless aggregate signature scheme for the internet of vehicles. *Transactions on Emerging Telecommunications Technologies*, **31**, e3708.
- [14] Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, **41**, 303–332.
- [15] Rivest, R. L., Shamir, A., and Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, **21**, 120– 126.
- [16] Koblitz, N. Elliptic curve cryptosystems. Mathematics of computation, 48, 203–209.
- [17] Kravitz, D. W. Digital signature algorithm. US Patent 5,231,668.
- [18] Bernstein, D. J. Introduction to post-quantum cryptography. In Bernstein, D. J., Buchmann, J., and Dahmen, E. (eds.), *Post-Quantum Cryptography*, pp. 1–14. Springer Berlin Heidelberg.
- [19] Garey, M. R. and Johnson, D. S. Computers and intractability. Freeman San Francisco.
- [20] Sakumoto, K., Shirai, T., and Hiwatari, H. Public-key identification schemes based on multivariate quadratic polynomials. In Rogaway, P. (ed.), Advances in Cryptology – CRYPTO 2011, Santa Barbara, CA, USA, August 14-18, 2011, pp. 706–723. Springer Berlin Heidelberg.
- [21] Huang, X., Mu, Y., Susilo, W., Wong, D. S., and Wu, W. Certificateless signature revisited. In Pieprzyk, J., Ghodosi, H., and Dawson, E. (eds.), *Information Security and Privacy*, Townsville, Australia, July 2-4, 2007, pp. 308–322. Springer Berlin Heidelberg.
- [22] Sakumoto, K. Public-key identification schemes based on multivariate cubic polynomials. In Fischlin, M., Buchmann, J., and Manulis, M. (eds.), *Public Key Cryptography – PKC 2012*, Darmstadt, Germany, May 21-23, 2012, pp. 172–189. Springer Berlin Heidelberg.
- [23] Nachef, V., Patarin, J., and Volte, E. Zero-knowledge for multivariate polynomials. In Hevia, A. and Neven, G. (eds.), *Progress in Cryptology – LATINCRYPT* 2012, Santiago, Chile, October 7-10, 2012, pp. 194–213. Springer Berlin Heidelberg.
- [24] Monteiro, F. S., Goya, D. H., and Terada, R. Improved identification protocol based on the mq problem. *IEICE Transactions on Fundamentals of Electronics*, *Communications and Computer Sciences*, 98, 1255– 1265.
- [25] Akleylek, S. and Soysaldi, M. A novel 3-pass identification scheme and signature scheme based on multivariate quadratic polynomials. *Turkish Journal* of Mathematics, 43, 241–257.
- [26] Wolf, C. and Preneel, B. Mq-ip: An identitybased identification scheme without number-theoretic assumptions. *Cryptology ePrint Archive*, **2010:087**.
- [27] Xiang, D., Li, X., Gao, J., and Zhang, X. A secure and efficient certificateless signature scheme for internet of things. Ad Hoc Networks, 124, 102702.

- [28] Hung, Y.-H., Huang, S.-S., Tseng, Y.-M., and Tsai, T.-T. Certificateless signature with strong unforgeability in the standard model. *Informatica*, 26, 663–684.
- [29] Yang, W., Weng, J., Luo, W., and Yang, A. Strongly unforgeable certificateless signature resisting attacks from malicious-but-passive kgc. *Security and Communication Networks*, **2017**, 1–8.
- [30] Yan, F., Xing, L., and Zhang, Z. An improved certificateless signature scheme for iot-based mobile payment. *International Journal of Network Security*, 23, 904–913.
- [31] Shim, K.-A., Park, C.-M., Koo, N., and Seo, H. A high-speed public-key signature scheme for 8-b iotconstrained devices. *IEEE Internet of Things Journal*, 7, 3663–3677.
- [32] Yang, B.-Y., Cheng, C.-M., Chen, B.-R., and Chen, J.-M. Implementing minimized multivariate pkc on lowresource embedded systems. In Clark, J. A., Paige, R. F., Polack, F. A. C., and Brooke, P. J. (eds.), *Security in Pervasive Computing*, York, UK, April 18-21, 2006, pp. 73–88. Springer Berlin Heidelberg.
- [33] Bogdanov, A., Eisenbarth, T., Rupp, A., and Wolf, C. Time-area optimized public-key engines: Mqcryptosystems as replacement for elliptic curves? In Oswald, E. and Rohatgi, P. (eds.), *Cryptographic Hardware and Embedded Systems – CHES 2008*, Washington, D.C., USA, August 10-13, 2008, pp. 45– 61. Springer Berlin Heidelberg.
- [34] Chen, A. I.-T., Chen, M.-S., Chen, T.-R., Cheng, C.-M., Ding, J., Kuo, E. L.-H., Lee, F. Y.-S., and Yang, B.-Y. Sse implementation of multivariate pkcs on modern x86 cpus. In Clavier, C. and Gaj, K. (eds.), *Cryptographic Hardware and Embedded Systems* - *CHES 2009*, Lausanne, Switzerland, September 6-9, 2009, pp. 33–48. Springer Berlin Heidelberg.
- [35] Yang, B.-Y., Chen, J.-M., and Chen, Y.-H. Tts: Highspeed signatures on a low-cost smart card. In Joye, M. and Quisquater, J.-J. (eds.), *Cryptographic Hardware* and *Embedded Systems - CHES 2004*, Cambridge, MA, USA, August 11-13, pp. 371–385. Springer Berlin Heidelberg.