International Journal of Networking and Computing – www.ijnc.org, ISSN 2185-2847
Volume 10, Number 2, pages 308–324, July 2020

An Efficient $\mathcal{MQ}$-based Signature with Tight Security Proof

Hiroki Furue
Department of Mathematical Informatics
Graduate School of Information Science and Technology
The University of Tokyo
7-3-1, Hongo, Bunkyo-Ku, Tokyo, 113-8656, Japan

Dung Hoang Duong
Institute of Cybersecurity and Cryptology
School of Computing and Information Technology
University of Wollongong
Northfields Avenue, Wollongong, NSW 2522, Australia

Tsuyoshi Takagi
Department of Mathematical Informatics
Graduate School of Information Science and Technology
The University of Tokyo
7-3-1, Hongo, Bunkyo-Ku, Tokyo, 113-8656, Japan

Received: February 14, 2020
Revised: May 3, 2020
Accepted: June 11, 2020
Communicated by Yasuyuki Nogami

Abstract

At PKC 2018, Chen et al. proposed SOFIA, the first $\mathcal{MQ}$-based digital signature scheme having tight security in the quantum random oracle model (QROM). SOFIA is constructed by applying an extended version of the Unruh transform (EUROCRYPT 2015) to the $\mathcal{MQ}$-based 5-pass identification scheme (IDS) proposed by Sakumoto et al. (CRYPTO 2011). In this paper, we propose an $\mathcal{MQ}$-based 3-pass IDS with impersonation probability of $\frac{1}{2}$ and apply the original version of the Unruh transform to it to obtain a more efficient $\mathcal{MQ}$-based digital signature scheme tightly secure in the QROM. The signature size of our digital signature scheme decreases by about 35% compared with SOFIA in the level I of NIST PQC security category, and is supposed to be the shortest among that of $\mathcal{MQ}$-based signatures tightly secure in the QROM.

Keywords: Post-quantum cryptography, Multivariate public key cryptography, Identification scheme, QROM, Unruh transform

1 Introduction

The $\mathcal{MQ}$-problem asks to solve a system of multivariate quadratic equations over a finite field and is known to be NP-complete [11]. Even though the $\mathcal{MQ}$-problem is basic for multivariate public

[0]This is an abstract footnote

key cryptography (MPKC), almost all current schemes [6, 18] are not based on the $\mathcal{MQ}$-problem but related to problems such as the Isomorphism of Polynomial (IP) problem [17] or the MinRank problem [5, 9]. At AsiaCrypt 2016, Chen et al. proposed MQDSS [2], the first multivariate signature scheme whose security is based solely on the $\mathcal{MQ}$-problem. This scheme is obtained by applying an extended version of the Fiat-Shamir transform [10] to the $\mathcal{MQ}$-based 5-pass identification scheme (IDS) proposed by Sakumoto et al. [19]. MQDSS is a $\mathcal{MQ}$-based digital signature scheme (DSS) that has passed into the second round of NIST call for post-quantum proposals [16]. In 2019, the security of DSSs constructed from the original version of the Fiat-Shamir transform is proven in the quantum random oracle model (QROM) under some natural settings [8, 14], where QROM means that a quantum adversary can access the random oracle in superposition. Moreover, in 2020, Don et al. [7] prove the security of MQDSS in the QROM. However, the security reduction of MQDSS in the QROM is not tight. In this paper, we define a tight security reduction as follows: for any attackers on the target security (e.g. EU-CMA security) with a success probability ϵ, there is an attacker on the underlying mathematical problem (e.g. $\mathcal{MQ}$-problem) with a success probability ϵ' satisfying $\epsilon' \geq \epsilon - \mathsf{negl}(k)$, where $\mathsf{negl}(k)$ is a negligible function for the security parameter k.

At PKC 2018, Chen et al. [3] proposed a DSS called SOFIA obtained by applying the Unruh transform [20] to the $\mathcal{MQ}$-based 5-pass IDS proposed by Sakumoto et al. [19]. This DSS is proven secure in the QROM, and the security reduction is tight. However, one problem with SOFIA is that it loses its effectiveness: its signature is about three times larger than that of MQDSS.

In both MQDSS and SOFIA, the authors chose Sakumoto et al.'s 5-pass IDS since it has small impersonation probability of $\frac{1}{2} + \frac{1}{2q}$ (q is the order of the finite field) and small "response" size, and this choice is appropriate with the Fiat-Shamir transform. However, in the Unruh transform, several "challenges" are iterated per one "commitment". This means that the impersonation probability depends on the number of "challenges" per one "commitment" t. In SOFIA, one sets $t = 3$ to make the signature smallest, but this changes the impersonation probability to $\frac{2}{3}$. The number of rounds will increase if the impersonation probability becomes larger. Therefore, this makes the signature size larger.

Our contribution. In this paper, we propose a more efficient MQ-based DSS with tight security proof in the QROM. Our approach is to propose a novel 3-pass IDS with impersonation probability of $\frac{1}{2}$ which is more optimal with the Unruh transform. We also apply the Unruh transform to other 3-pass IDSs by Sakumoto et al. [19] and Monteiro et al. [15] to obtain two other $\mathcal{MQ}$-based DSSs, and compare these DSSs with SOFIA at the security level I of NIST PQC (see Table 1). As a result, our DSS is the most efficient among all other DSSs from the Unruh transform. In particular, the signature size of our DSS is decreased by about 35% compared with SOFIA.

Table 1: Size of signature obtained by applying the Unruh transform to $\mathcal{MQ}$-based identification schemes in level I of NIST PQC security category. (r: number of rounds, t: number of challenges per round, 1KB=1024B)

$\mathcal{MQ}$-based signature secure in the QROM	r	t	signature (KB)
SOFIA [3]	219	3	46.8
DSS from Sakumoto et al.'s IDS [19]	219	3	34.8
DSS from Monteiro et al.'s IDS [15]	128	4	33.3
DSS from our proposed 3-pass IDS	128	4	**29.6**

Our technique in designing a new 3-pass IDS combines both IDSs of Sakumoto et al. [19] and Monteiro et al. [15]. As a result, it has impersonation probability of $\frac{1}{2}$, which is the same as that of Monteiro et al.'s, whereas that of the 3-pass IDS of Sakumoto et al. is $\frac{2}{3}$. One drawback of our IDS is that the response size is larger than that of Sakumoto et al.'s and comparable with that of Monteiro et al.'s (see Table 6). However, if we construct an $\mathcal{MQ}$-based DSS by applying the Unruh transform to our IDS, then the signature of our DSS is smaller than those of DSSs using the previous 3-pass IDSs. We stress that the signature size of our proposed DSS is not shorter than that of MQDSS. We can also construct a DSS by applying the Fiat-Shamir transform to our proposed IDS, but this DSS

from the Fiat-Shamir transform is not effective than MQDSS and not tightly secure. Therefore, in this paper, we consider only our DSS from the Unruh transform.

Related work. Recently, Beullens [1] proposed a $\mathcal{MQ}$-based DSS constructed from the Fiat-Shamir transform, called MUDFISH, which is proven to be EU-CMA secure in the QROM and has shorter signature than MQDSS. However, the tightness of the security reduction in [8,14] depends on the construction of IDS, and the proof of MUDFISH in the QROM is not tight. Furthermore, it is unknown whether there exists a tight security proof of MQDSS in the QROM. On the other hand, our proposed DSS, constructed by applying the Unruh transform, has a tight security reduction. Therefore, we can say that our proposed DSS has the shortest signature among the $\mathcal{MQ}$-based DSSs with the tight security in the QROM.

Organization. Our paper is organized as follows. In Section 2, we give the definitions of IDS and DSS, and explain the Fiat-Shamir transform and the Unruh transform. In Section 3, we recall the $\mathcal{MQ}$-problem and explain several $\mathcal{MQ}$-based IDSs and DSSs. In Section 4, we give details of the proposed IDS with its security proof. In Section 5, we discuss applying the Unruh transform to the proposed IDS and a comparison of the obtained DSS with other DSSs from other $\mathcal{MQ}$-based IDSs. The security proof of our DSS is proven in the appendix. We conclude the paper in Section 6.

2 Preliminaries

In this section, we provide notions about the security of IDS and DSS following Chen et al.'s study [3]. We then explain the Fiat-Shamir transform and the Unruh transform.

2.1 Identification Scheme (IDS)

A 3-pass IDS with security parameter k, denoted as $\mathsf{IDS}(1^k)$, is a triplet of probabilistic polynomial time (PPT) algorithms $\mathsf{IDS} = (\mathsf{KGen}, P, V)$ such that a key generator algorithm KGen is a probabilistic algorithm that outputs a key pair $(\mathsf{sk}, \mathsf{pk})$, and P and V are interactive prover and verifier algorithms. The P takes as input a secret key sk and V takes as input a public key pk. At the conclusion of the protocol, V outputs a bit b with $b = 1$ indicating "accept" or $b = 0$ indicating "reject".

A 3-pass IDS with $P = (P_0, P_1)$ and $V = (\mathsf{ChS}, \mathsf{Vf})$ works as follows: $P_0(\mathsf{sk})$ computes the initial commitment com sent as the first message and a state st fed forward to P_1. After obtaining the com from P_0, ChS computes the challenge message $\mathsf{ch} \xleftarrow{R} \mathsf{Ch}$, sampling at random from the challenge space Ch and sends to P. Now P uses $P_1(\mathsf{st}, \mathsf{ch})$ to computes the response resp, which is sent back to V. The V computes $\mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}, \mathsf{resp})$ to yield the final decision whether to accept or reject.

In P_0, we use a commitment scheme $\mathsf{Com} : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^{2k}$ for the security parameter k, that takes as input k uniformly random bits and a message, and outputs a $2k$-bit commitment.

In this paper, we assume that Com is computational binding and computational hiding.

Definition 1 (Computational binding)**.** *Let* Com *be a commitment scheme with a security parameter* k*. We say that* Com *is computational binding, if, after publishing* $\mathsf{Com}(x)$*, any adversary cannot find* $y \neq x$ *such that* $\mathsf{Com}(y) = \mathsf{Com}(x)$ *with non-negligible probability for* k*.*

Definition 2 (Computational hiding)**.** *Let* Com *be a commitment scheme with a security parameter* k*. We say that* Com *is computational hiding, if, given* $\mathsf{Com}(x)$*, any adversary cannot find* x *with non-negligible probability for* k*.*

In order to be computationally hiding, the commitment scheme needs a random k bit string as the input [13].

For the correctness of an IDS, we require that for all $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^k)$, a verifier given pk outputs "accept" interacting with an honest prover given sk. In addition, we give some definitions for IDS. Let $\mathsf{negl}(k)$ be the negligible function for the security parameter k.

Definition 3 (Key relation)**.** *Let* $\mathsf{IDS}(1^k)$ *be a 3-pass IDS with a security parameter* k *and* R *be a relation. We say that* IDS *has key relation* R *if and only if* R *is the minimal relation such that*

$$\forall(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^k) : (\mathsf{pk}, \mathsf{sk}) \in R.$$

Definition 4 (KOW). *Let* $\mathsf{IDS}(1^k)$ *be a 3-pass IDS with a security parameter* k *and key relation* R*. We call* IDS *key-one-way (KOW) if for any quantum polynomial time algorithm* A*,*

$$\mathsf{Pr}[(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{KGen}(1^k), \mathsf{sk}' \leftarrow A(\mathsf{pk}) : (\mathsf{pk},\mathsf{sk}') \in R] = \mathsf{negl}(k).$$

We denote the transcript of messages exchanged in the IDS as $\mathsf{trans}(\langle P(\mathsf{sk}), V(\mathsf{pk})\rangle)$.

Definition 5 ((computational) HVZK). *Let* $\mathsf{IDS}(1^k)$ *be a 3-pass IDS with a security parameter* k*. We say that* IDS *is computational honest-verifier zero-knowledge (HVZK) if there exists a PPT algorithm* S*, called the simulator, such that for any quantum polynomial time algorithm* A *and* $(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{KGen}(1^k)$*:*

$$|\mathsf{Pr}\left[1 \leftarrow A(\mathsf{sk},\mathsf{pk},\mathsf{trans}(\langle P(\mathsf{sk}), V(\mathsf{pk})\rangle))\right] - \mathsf{Pr}\left[1 \leftarrow A(\mathsf{sk},\mathsf{pk},S(\mathsf{pk}))\right]| = \mathsf{negl}(k).$$

Definition 6 (α-extractor). *Let* $\mathsf{IDS}(1^k)$ *be a 3-pass IDS with a security parameter* k *and key relation* R*. We say that* IDS *has an* α*-extractor if* $|\mathsf{Ch}| \geq \alpha$*, where* Ch *denotes the challenge space, and there exists a polynomial time algorithm* K*, the extractor, that given a public key* pk *and* α *valid transcripts for pk:*

$$\begin{aligned}
\mathsf{trans}^{(1)} &= (\mathsf{com},\mathsf{ch}^{(1)},\mathsf{resp}^{(1)}),\\
\mathsf{trans}^{(2)} &= (\mathsf{com},\mathsf{ch}^{(2)},\mathsf{resp}^{(2)}),\\
&\vdots\\
\mathsf{trans}^{(\alpha)} &= (\mathsf{com},\mathsf{ch}^{(\alpha)},\mathsf{resp}^{(\alpha)}),
\end{aligned}$$

where $\mathsf{ch}^{(1)},\mathsf{ch}^{(2)},\ldots,\mathsf{ch}^{(\alpha)}$ *are different, outputs a secret key* sk *such that* $(\mathsf{pk},\mathsf{sk}) \in R$ *with success probability* $1 - \mathsf{negl}(k)$*.*

2.2 Digital Signature Scheme (DSS)

A DSS with a security parameter k, denoted as $\mathsf{DSS}(1^k)$, is a triplet of PPT algorithms $\mathsf{DSS} = (\mathsf{KGen},\mathsf{Sign},\mathsf{Vf})$ such that key generator algorithm KGen is a probabilistic algorithm that outputs a key pair $(\mathsf{sk},\mathsf{pk})$, signing algorithm Sign is a possibly probabilistic algorithm that on input of a secret key sk and a message M outputs a signature σ, and verification algorithm Vf is a deterministic algorithm that on input of a pk, M, and σ outputs a bit b with $b = 1$ indicating "accept" or $b = 0$ indicating "reject". For the correctness of a DSS, we require that for all $(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{KGen}(1^k)$ and message M, $\mathsf{Vf}(\mathsf{pk},M,\mathsf{Sign}(\mathsf{sk},M)) = 1$.

Definition 7 (EU-CMA). *Let* $\mathsf{DSS}(1^k)$ *be a DSS with a security parameter* k*. We call such a* DSS *EU-CMA secure if for any quantum polynomial time algorithm* A *making queries to a classical signing oracle* Sig*,*

$$\mathsf{Pr}\left[\mathsf{Vf}(\mathsf{pk},M',\sigma') = 1 \wedge M' \notin Q : (\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{KGen}(1^k), (M',\sigma') \leftarrow A^{\mathsf{Sig}}(\mathsf{pk})\right] = \mathsf{negl}(k),$$

where Q *is the list of all queried messages made to* Sig*.*

2.3 Fiat-Shamir Transform

The Fiat-Shamir transform [10] is one of the most basic ways that transform a 3-pass IDS into a DSS. The prover generates a signature by replacing the challenge chosen by the verifier in a 3-pass IDS with an output of a hash function computed by the prover. This is iterated for several rounds in order to achieve the required security level.

Table 2: Signature generation of the Fiat-Shamir transform.

$\mathsf{Sign}(\mathsf{sk}, M)$
For $j \in \{1, \ldots, r\}$ **do**
$\quad (\mathsf{st}^{(j)}, \mathsf{com}^{(j)}) \leftarrow P_0(\mathsf{sk})$
$\mathsf{md} \leftarrow H(\mathsf{pk}, M, \{\mathsf{com}^{(j)}\}_{j=1}^{r})$
Read md **as vector** $(\mathsf{ch}^{(1)}, \ldots, \mathsf{ch}^{(r)})$
For $j \in \{1, \ldots, r\}$ **do**
$\quad (\mathsf{resp}^{(j)}) \leftarrow P_1(\mathsf{st}^{(j)}, \mathsf{ch}^{(j)})$
$\sigma := (\mathsf{md}, \{\mathsf{com}^{(j)}, \mathsf{resp}^{(j)}\}_{j=1}^{r})$

Table 3: Verification of the Fiat-Shamir transform.

$\mathsf{Vf}(\mathsf{pk}, M, \sigma)$
Read md **as vector** $(\mathsf{ch}^{(1)}, \ldots, \mathsf{ch}^{(r)})$
$\mathsf{md}' \leftarrow H(\mathsf{pk}, M, \{\mathsf{com}^{(j)}\}_{j=1}^{r})$
Check that $\mathsf{md}' \stackrel{?}{=} \mathsf{md}$
For $j \in \{1, \ldots, r\}$ **do**
$\quad$ Check $1 \stackrel{?}{=} b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}^{(j)}, \mathsf{ch}^{(j)}, \mathsf{resp}^{(j)})$
If all checks succeed, output success.

See Tables 2 and 3 for the construction of the Fiat-Shamir transformation. First, P_0 is iterated for r times, and generates $\mathsf{com}^{(1)}, \ldots, \mathsf{com}^{(r)}$. Then, the signer determines the challenge as an output of the hash function H. Finally, the signer executes P_1 on the input of $\mathsf{st}^{(j)}$ and $\mathsf{ch}^{(j)}$ in each round, and sends the output of H, commitments and responses of each round as a signature.

2.4 Unruh Transform

The Unruh transform [20] also converts an IDS into a DSS. The basic idea is to let the signer generate several transcripts for one com. Tables 4 and 5 show the details of the transformation.

Table 4: Signature generation of the Unruh transform.

$\mathsf{Sign}(\mathsf{sk}, M)$
For $j \in \{1, \ldots, r\}$ **do**
$\quad (\mathsf{st}^{(j)}, \mathsf{com}^{(j)}) \leftarrow P_0(\mathsf{sk})$
$\quad$ **For** $i \in \{1, \ldots, t\}$ **do**
$\quad\quad \mathsf{ch}^{(i,j)} \stackrel{R}{\leftarrow} \mathsf{Ch} \setminus \{\mathsf{ch}^{(1,j)}, \ldots, \mathsf{ch}^{(i-1,j)}\}$
$\quad\quad (\mathsf{resp}^{(i,j)}) \leftarrow P_1(\mathsf{st}^{(j)}, \mathsf{ch}^{(i,j)})$
$\quad\quad \mathsf{cr}^{(i,j)} \leftarrow G(\mathsf{resp}^{(i,j)})$
$\quad \mathsf{trans}_{\mathsf{full}}(j) := \mathsf{com}^{(j)}, \{\mathsf{ch}^{(i,j)}, \mathsf{cr}^{(i,j)}\}_{i=1}^{t}$
$\mathsf{md} \leftarrow H(\mathsf{pk}, M, \{\mathsf{trans}_{\mathsf{full}}(j)\}_{j=1}^{r})$
Read md **as vector** $(I_1, \ldots, I_r)$
$\mathsf{trans}_{\mathsf{red}}(j) := \mathsf{com}^{(j)}, \{\mathsf{ch}^{(i,j)}, \mathsf{cr}^{(i,j)}\}_{i \neq I_j, i=1}^{t}$
$\sigma := (\mathsf{md}, \{\mathsf{trans}_{\mathsf{red}}(j), \mathsf{ch}^{(I_j,j)}, \mathsf{resp}^{(I_j,j)}\}_{j=1}^{r})$

Table 5: Verification of the Unruh transform.

$\mathsf{Vf}(\mathsf{pk}, M, \sigma)$
Read md **as vector** $(I_1, \ldots, I_r)$
For $j \in \{1, \ldots, r\}$ **do**
$\quad \mathsf{cr}^{(I_j,j)} \leftarrow G(\mathsf{resp}^{I_j,j})$
$\mathsf{md}' \leftarrow H(\mathsf{pk}, M, \{\mathsf{trans}_{\mathsf{full}}(j)\}_{j=1}^{r})$
Check that $\mathsf{md}' \stackrel{?}{=} \mathsf{md}$
For $j \in \{1, \ldots, r\}$ **do**
$\quad$ Check that $\mathsf{ch}^{(1,j)}, \ldots, \mathsf{ch}^{(t,j)}$ are all distinct
$\quad$ Check $1 \stackrel{?}{=} b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}^{(j)}, \mathsf{ch}^{(I_j,j)}, \mathsf{resp}^{(I_j,j)})$
If all checks succeed, output success.

First, P_0 generates several commitments $\mathsf{com}^{(1)}, \ldots, \mathsf{com}^{(r)}$, and the signer chooses challenges $\mathsf{ch}^{(1,j)}, \ldots, \mathsf{ch}^{(t,j)}$ in each round j. Then, P_1 outputs responses for every challenge in each round, and these responses are blinded by using a length-preserving hash function G. The output of the hash function H computed by the signer determines which challenges are verified by the verifier. If i is selected by H, the open response $\mathsf{resp}^{(i,j)}$ is included in the signature, otherwise the blinded response $\mathsf{cr}^{(i,j)}$ is included.

3 $\mathcal{MQ}$-based Schemes

In this section, we recall the $\mathcal{MQ}$-problem and introduce several $\mathcal{MQ}$-based identification schemes and signatures.

3.1 $\mathcal{MQ}$-problem

Let $\mathbf{F} = (f_1, \ldots, f_m)$ be a system of quadratic polynomials with n variables $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$. The problem to find $\mathbf{x} \in \mathbb{F}_q^n$ such that $\mathbf{F}(\mathbf{x}) = \mathbf{y}$ is called the $\mathcal{MQ}$-problem, where $\mathbf{y} \in \mathbb{F}_q^m$, and denoted by $\mathcal{MQ}(q, n, m)$. Garey and Johnson [11] showed that this problem is NP-complete. In addition, there is no quantum algorithm to solve this problem in polynomial time. Therefore, this problem is known to be resistant to quantum adversaries.

3.2 $\mathcal{MQ}$-based Identification Schemes

Suppose that $\mathbf{F}$ denotes the $\mathcal{MQ}$ function without a constant term. In $\mathcal{MQ}$-based IDSs, we use the polar system $\mathbf{G}$ defined by $\mathbf{G}(\mathbf{a}, \mathbf{b}) := \mathbf{F}(\mathbf{a} + \mathbf{b}) - \mathbf{F}(\mathbf{a}) - \mathbf{F}(\mathbf{b})$. Then $\mathbf{G}$ has bilinearity: for $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{F}_q^n$, $\alpha \in \mathbb{F}_q$,

$$\begin{aligned}
\mathbf{G}(\mathbf{a} + \mathbf{b}, \mathbf{c}) &= \mathbf{G}(\mathbf{a}, \mathbf{c}) + \mathbf{G}(\mathbf{b}, \mathbf{c}), \\
\mathbf{G}(\mathbf{a}, \mathbf{b} + \mathbf{c}) &= \mathbf{G}(\mathbf{a}, \mathbf{b}) + \mathbf{G}(\mathbf{a}, \mathbf{c}), \\
\alpha\mathbf{G}(\mathbf{a}, \mathbf{b}) &= \mathbf{G}(\alpha\mathbf{a}, \mathbf{b}) = \mathbf{G}(\mathbf{a}, \alpha\mathbf{b}).
\end{aligned}$$

Now, suppose that $\mathbf{F}(\mathbf{s}) = \mathbf{v}$, which means that a secret key is $\mathbf{s}$ and public key is $(\mathbf{F}, \mathbf{v})$.

Let us first look at the $\mathcal{MQ}$-based 3-pass IDS proposed by Sakumoto et al. [19], which is one of the most basic $\mathcal{MQ}$-based IDSs. In the 3-pass IDS proposed by Sakumoto et al., this $\mathbf{s}$ is split as follows:

$$\mathbf{s} \begin{cases} \mathbf{r}_0 \begin{cases} \mathbf{t}_0 \\ \mathbf{t}_1 \end{cases}, & \mathbf{F}(\mathbf{r}_0) \begin{cases} \mathbf{e}_0 \\ \mathbf{e}_1 \end{cases}. \\ \mathbf{r}_1 \end{cases}$$

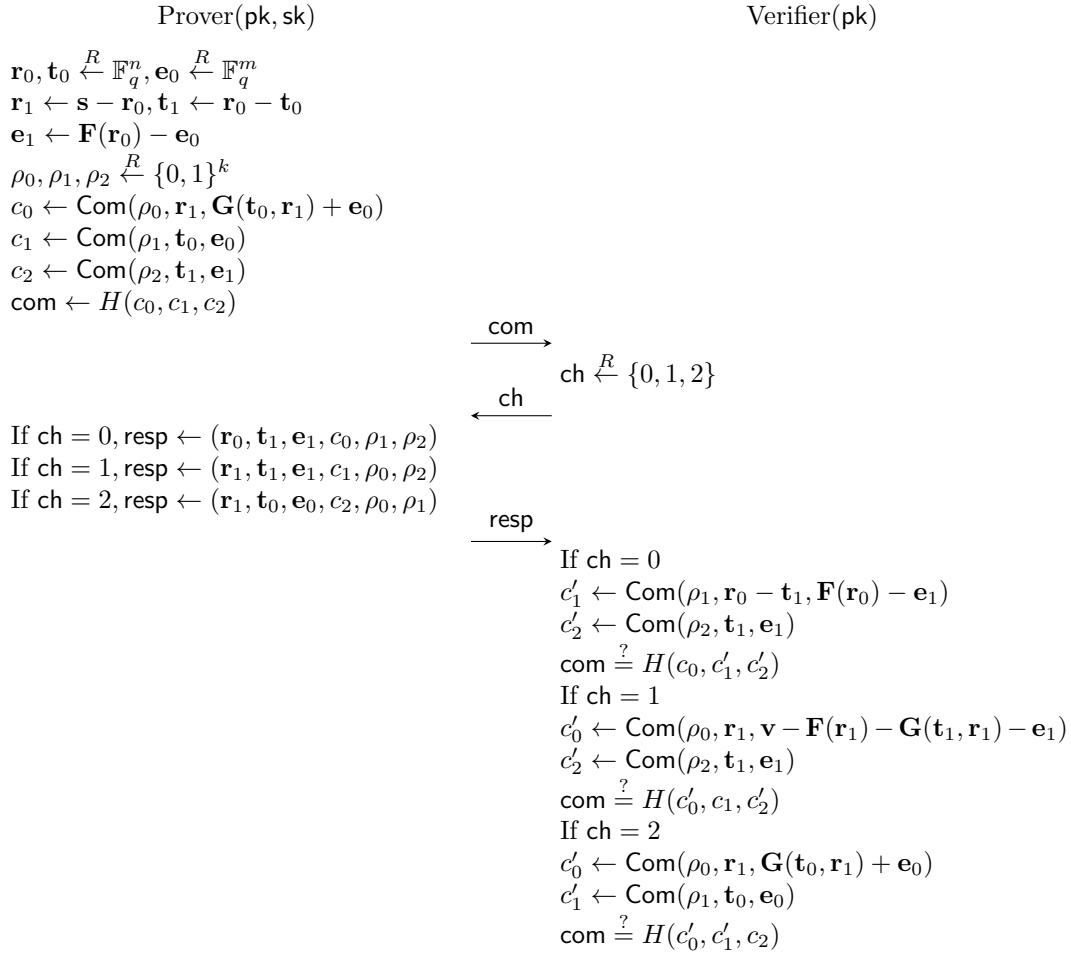

Figure 1: $\mathcal{MQ}$-based 3-pass identification scheme (IDS) proposed by Sakumoto et al.

Then we obtain the following:

$$\begin{aligned} \mathbf{v} &= \mathbf{F}(\mathbf{s}) \\ &= \mathbf{G}(\mathbf{r}_0, \mathbf{r}_1) + \mathbf{F}(\mathbf{r}_0) + \mathbf{F}(\mathbf{r}_1) \\ &= \mathbf{G}(\mathbf{t}_0, \mathbf{r}_1) + \mathbf{G}(\mathbf{t}_1, \mathbf{r}_1) + \mathbf{e}_0 + \mathbf{e}_1 + \mathbf{F}(\mathbf{r}_1). \end{aligned}$$

The prover can prove that he has the secret key without giving any information to the verifier, since this equation can be seen as the function of $\mathbf{r}_1$, not $\mathbf{r}_0$. Figure 1 shows the details of this scheme. In Figure 1, ρ_0, ρ_1, ρ_2 are random k-bit strings for the computationally hiding of the commitment scheme Com. Sakumoto et al.'s 3-pass IDS has an impersonation probability of $\frac{2}{3}$; hence, to reach the desired security level, one needs to repeat the protocol a number of rounds.

Sakumoto et al. [19] also introduced a 5-pass IDS with impersonation probability of $\frac{1}{2} + \frac{1}{2q}$ with q denoting the order of the underlying finite field, which is used in MQDSS and SOFIA. In this 5-pass scheme, they use the splitting way like the following:

$$\mathbf{s} \begin{cases} \mathbf{r}_0 & \alpha\mathbf{r}_0 \begin{cases} \mathbf{t}_0 \\ \mathbf{t}_1, \end{cases} & \alpha\mathbf{F}(\mathbf{r}_0) \begin{cases} \mathbf{e}_0 \\ \mathbf{e}_1, \end{cases} \\ \mathbf{r}_1 \end{cases}$$

where α is randomly chosen from $\mathbb{F}_q$ as the first challenge by the verifier.

In 2015, Monteiro et al. [15] proposed an $\mathcal{MQ}$-based 3-pass IDS. Their idea is to also further split $\mathbf{r}_1$ and $\mathbf{F}(\mathbf{r_1})$ as follows:

$$\mathbf{s}\begin{cases}\mathbf{r}_0\begin{cases}\mathbf{t}_0 & \mathbf{F}(\mathbf{r}_0)\begin{cases}\mathbf{e}_0\\ \mathbf{e}_1\end{cases}\\ \mathbf{t}_1\end{cases}\\ \mathbf{r}_1\begin{cases}\mathbf{d}_0 & \mathbf{F}(\mathbf{r}_1)\begin{cases}\mathbf{u}_0\\ \mathbf{u}_1\end{cases}\\ \mathbf{d}_1\end{cases}\end{cases}.$$

They also changed the challenge space to $\{0,1,2,3\}$; as a result, their protocol has impersonation probability of $\frac{1}{2}$.

These IDSs are honest-verifier zero-knowledge (HVZK) when the commitment is computationally binding.

3.3 MQDSS and Attack on the Scheme

MQDSS proposed by Chen et al. [2] is a $\mathcal{MQ}$-based signature constructed by applying the extended Fiat-Shamir transform [10] to the $\mathcal{MQ}$-based 5-pass IDS proposed by Sakumoto et al. [19] and one of the candidates of the second round of NIST post-quantum standardization project [16]. Suppose that exchanged message in 5-pass IDS is denoted by $\{\mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2\}$. In MQDSS, ch_1 is determined as $H_1(\mathsf{pk}, M, \mathsf{com})$, and ch_2 is determined as $H_2(\mathsf{pk}, M, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1)$, where M is a message and H_1 and H_2 are hash functions. In [2], they prove that MQDSS is EU-CMA secure in the ROM, but this security reduction is not tight.

In [12], Kales and Zaverucha proposed an attack on MQDSS with the parameters in [4]. This attack exploits that the original IDS used in MQDSS is a 5-pass scheme. In the 5-pass IDS, the attacker can impersonate the honest prover, if the attacker succeeds guessing either ch_1 or ch_2 chosen randomly by the verifier. The detail of this attack is to split the attacker's work between two phases. First, the attacker guesses ch_1 for N_1 rounds ($N_1 < r$, where r is the number of rounds), and iterates to input fake commitments until H_1 outputs the value corresponding to his guesses in the N_1 rounds. Second, the attacker guesses ch_2 for remaining $r - N_1$ rounds, and also iterates to input fake responses until H_2 outputs the value corresponding to his guesses in the remaining rounds. Then, this attack is successful since the attacker can impersonate by a correct guess for either ch_1 or ch_2. As a result, the complexity of this attack is smaller than that of the basic exhaustive search. We must increase the number of rounds of MQDSS by $30 \sim 40\%$ to repair its security against the attack proposed by Kales and Zaverucha.

3.4 MUDFISH

In [1], Beullens proposed another $\mathcal{MQ}$-based IDS constructed by transforming the identification protocol with a trusted third party called the "helper" in addition to the verifier and the prover. In his protocol with three parties, the helper randomly chooses $\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0$, and produces $\mathbf{r}_1$ and $\{\mathbf{t}_1^{(c)}, \mathbf{e}_1^{(c)}\}_{c\in\mathbb{F}_q}$ computed by the same way as the 5-pass IDS by Sakumoto et al., where this c indicates α in Subsection 3.2. After the prover outputs a commitment, the verifier randomly chooses a challenge $\alpha \in \mathbb{F}_q$, and then, the prover generates a response by using $\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0, \mathbf{r}_1, \{\mathbf{t}_1^{(\alpha)}, \mathbf{e}_1^{(\alpha)}\}$ made by the helper. This scheme with helper has a small impersonation probability under the assumption that the helper is honest. The signature scheme constructed by applying the Fiat-Shamir transform to the IDS constructed by removing the helper is called MUDFISH. The signature size of MUDFISH becomes relatively small by using the Merkle tree on commitments and fewer seeds with a binary tree. As a result, MUDFISH has a smaller size signature than MQDSS. Beullens proved that MUDFISH is EU-CMA secure in the QROM, but this reduction is not tight.

4 Proposed Identification Scheme

In this section, we first give details of the proposed $\mathcal{MQ}$-based 3-pass IDS. We also prove the security of this scheme, α-extractor, and honest-verifier zero-knowledge (HVZK). Furthermore, we compare our IDS with other $\mathcal{MQ}$-based IDSs.

4.1 Protocol of Proposed IDS

The proposed $\mathcal{MQ}$-based 3-pass IDS is based on the IDSs proposed by Sakumoto et al. [19] and Monteiro et al. [15]. In our IDS, we also use the polar system $\mathbf{G}$, as with these schemes, but we change the manner of splitting the information. We divide the secret key $\mathbf{s}$ into $\mathbf{r}_0$ and $\mathbf{r}_1$, $\mathbf{r}_0$ is divided into $\mathbf{t}_0$ and $\mathbf{t}_1$, and $\mathbf{r}_1$ is divided into $\mathbf{d}_0$ and $\mathbf{d}_1$. This is the same as that of Monteiro et al.'s. While Monteiro et al. splits both $\mathbf{F}(\mathbf{r}_0)$ and $\mathbf{F}(\mathbf{r}_1)$, we choose to split only $\mathbf{G}(\mathbf{r}_0, \mathbf{r}_1)$ into $\mathbf{e}_0$ and $\mathbf{e}_1$. This is described as follows:

$$\mathbf{s} \begin{cases} \mathbf{r}_0 \begin{cases} \mathbf{t}_0 \\ \mathbf{t}_1 \end{cases} \\ \mathbf{r}_1 \begin{cases} \mathbf{d}_0 \\ \mathbf{d}_1 \end{cases} \end{cases}, \quad \mathbf{G}(\mathbf{r}_0, \mathbf{r}_1) \begin{cases} \mathbf{e}_0 \\ \mathbf{e}_1 \end{cases}.$$

Then the equation

$$\mathbf{v} = \mathbf{G}(\mathbf{r}_0, \mathbf{r}_1) + \mathbf{F}(\mathbf{r}_0) + \mathbf{F}(\mathbf{r}_1)$$

can be seen as an equation having a function of $\mathbf{r}_0$ on one side and function of $\mathbf{r}_1$ on the other as follows:

$$\mathbf{v} - \mathbf{e}_0 - \mathbf{F}(\mathbf{r}_0) = \mathbf{e}_1 + \mathbf{F}(\mathbf{r}_1).$$

Figure 2 shows the details of the protocol of our IDS. Firstly, the prover determines $\mathbf{r}_0$, $\mathbf{r}_1$, $\mathbf{t}_0$, $\mathbf{t}_1$, $\mathbf{d}_0$, $\mathbf{d}_1$, $\mathbf{e}_0$, $\mathbf{e}_1$ and generates a commitment value com. Secondly, the verifier chooses a challenge ch from $\{0, 1, 2, 3\}$. Thirdly, the prover sends a response resp, and the verifier yields the final decision.

4.2 Security Proofs of Our IDS

We first prove that our IDS has a 3-extractor. Now we show there exists an adversary C that can cheat a verifier with probability $\frac{1}{2}$. Suppose that C chooses a false secret key $\mathbf{s}'$ randomly from $\mathbb{F}_q^n$ and executes other steps similar to an honest prover. If ch is 2 or 3, then C succeeds in impersonating since $\mathbf{F}(\mathbf{s}) = \mathbf{v}$ is not used in verifying. When ch is 0 or 1, C also succeeds by computing $c_2 \leftarrow \mathsf{Com}(\rho_2, \mathbf{t}_1, \mathbf{d}_0, \mathbf{v} - \mathbf{e}_0 - \mathbf{F}(\mathbf{r}_0))$ and $c_3 \leftarrow \mathsf{Com}(\rho_3, \mathbf{t}_0, \mathbf{d}_1, \mathbf{v} - \mathbf{e}_1 - \mathbf{F}(\mathbf{r}_0))$. By using prior or latter way randomly, these adversaries succeed in cheating with probability $\frac{1}{2}$.

Theorem 1. *Our IDS has a* 3*-extractor when the commitment scheme* Com *is computationally binding against any quantum polynomial time algorithm.*

Proof. Suppose that given a set of valid transcripts: $\{(\mathsf{com}, 1, \mathsf{resp}_1), (\mathsf{com}, 2, \mathsf{resp}_2), (\mathsf{com}, 3, \mathsf{resp}_3)\}$. Let $c_0, c_1, c_2, c_3, c_4, c_5$ be the commitment value and

$$\begin{aligned}
\mathsf{resp}_1 &= (\mathbf{r}_0^{(1)}, \mathbf{t}_1^{(1)}, \mathbf{d}_1^{(1)}, \mathbf{e}_1^{(1)}, c_1, c_2, c_4, \rho_0^{(1)}, \rho_3^{(1)}, \rho_5^{(1)}), \\
\mathsf{resp}_2 &= (\mathbf{r}_1^{(2)}, \mathbf{t}_0^{(2)}, \mathbf{d}_0^{(2)}, \mathbf{e}_0^{(2)}, c_0, c_2, c_5, \rho_1^{(2)}, \rho_3^{(2)}, \rho_4^{(2)}), \\
\mathsf{resp}_3 &= (\mathbf{r}_1^{(3)}, \mathbf{t}_1^{(3)}, \mathbf{d}_1^{(3)}, \mathbf{e}_1^{(3)}, c_0, c_3, c_4, \rho_1^{(3)}, \rho_2^{(3)}, \rho_5^{(3)}).
\end{aligned}$$

Then we have the following:

$$\begin{aligned}
c_1 &= \mathsf{Com}(\rho_1^{(2)}, \mathbf{r}_1^{(2)}, \mathbf{e}_0^{(2)} - \mathbf{G}(\mathbf{t}_0^{(2)}, \mathbf{r}_1^{(2)})) \\
&= \mathsf{Com}(\rho_1^{(3)}, \mathbf{r}_1^{(3)}, \mathbf{G}(\mathbf{t}_1^{(3)}, \mathbf{r}_1^{(3)}) - \mathbf{e}_1^{(3)}), \\
c_3 &= \mathsf{Com}(\rho_3^{(1)}, \mathbf{r}_0^{(1)} - \mathbf{t}_1^{(1)}, \mathbf{d}_1^{(1)}, \mathbf{v} - \mathbf{e}_1^{(1)} - \mathbf{F}(\mathbf{r}_0^{(1)})) \\
&= \mathsf{Com}(\rho_3^{(3)}, \mathbf{t}_0^{(2)}, \mathbf{r}_1^{(2)} - \mathbf{d}_0^{(2)}, \mathbf{e}_0^{(2)} + \mathbf{F}(\mathbf{r}_1^{(2)})), \\
c_5 &= \mathsf{Com}(\rho_5^{(1)}, \mathbf{t}_1^{(1)}, \mathbf{d}_1^{(1)}, \mathbf{e}_1^{(1)}) \\
&= \mathsf{Com}(\rho_5^{(2)}, \mathbf{t}_1^{(3)}, \mathbf{d}_1^{(3)}, \mathbf{e}_1^{(3)}).
\end{aligned}$$

Figure 2: Protocol of the proposed $\mathcal{MQ}$-based 3-pass identification scheme (IDS).

If any of the arguments of Com on the left-hand side is different from that on the right-hand side in any of the three equations, then we obtain two different arguments of Com, which contradicts its computationally binding property. If they are the same in the three equations, we obtain the following equalities: $\mathbf{r}_1^{(2)} = \mathbf{r}_1^{(3)}$, $\mathbf{r}_0^{(1)} - \mathbf{t}_1^{(1)} = \mathbf{t}_0^{(2)}$, $\mathbf{t}_1^{(1)} = \mathbf{t}_1^{(3)}$, $\mathbf{e}_1^{(1)} = \mathbf{e}_1^{(3)}$, $\mathbf{e}_0^{(2)} - \mathbf{G}(\mathbf{t}_0^{(2)}, \mathbf{r}_1^{(2)}) = \mathbf{G}(\mathbf{t}_1^{(3)}, \mathbf{r}_1^{(3)}) - \mathbf{e}_1^{(3)}$,

Table 6: Several $\mathcal{MQ}$-based identification schemes (IDSs).

	soundness	response size (bits)
Sakumoto et al.'s 5-pass IDS [19]	$1/2 + 1/2q$	$3k + 3n\lceil \log q \rceil$
Sakumoto et al.'s 3-pass IDS [19]	$2/3$	$4k + 3n\lceil \log q \rceil$
Monteiro et al.'s 3-pass IDS [15]	$1/2$	$8k + 5n\lceil \log q \rceil$
Proposed IDS	$1/2$	$9k + 4n\lceil \log q \rceil$

$\mathbf{v} - \mathbf{e}_1^{(1)} - \mathbf{F}(\mathbf{r}_0^{(1)}) = \mathbf{e}_0^{(2)} + \mathbf{F}(\mathbf{r}_1^{(2)})$. Combining these equalities, we obtain

$$\begin{aligned} \mathbf{v} &= \mathbf{e}_0^{(2)} + \mathbf{e}_1^{(1)} + \mathbf{F}(\mathbf{r}_0^{(1)}) + \mathbf{F}(\mathbf{r}_1^{(2)}) \\ &= \mathbf{G}(\mathbf{t}_0^{(2)} + \mathbf{t}_1^{(3)}, \mathbf{r}_1^{(2)}) + \mathbf{F}(\mathbf{r}_0^{(1)}) + \mathbf{F}(\mathbf{r}_1^{(2)}) \\ &= \mathbf{G}(\mathbf{r}_0^{(1)}, \mathbf{r}_1^{(2)}) + \mathbf{F}(\mathbf{r}_0^{(1)}) + \mathbf{F}(\mathbf{r}_1^{(2)}). \end{aligned}$$

Therefore, $\mathbf{r}_0^{(1)} + \mathbf{r}_1^{(2)}$ is a solution to the given $\mathcal{MQ}$-problem.

When three other valid transcripts are chosen, we can also obtain a solution to the given $\mathcal{MQ}$-problem in a similar way. □

Now we show that our IDS is computationally HVZK.

Theorem 2. *Our IDS is computationally HVZK when* Com *is computationally hiding.*

Proof. Let S be a simulator to impersonate an honest prover against the honest verifier without knowing the secret key. First, S chooses a $\mathbf{s}' \in \mathbb{F}_q^n$ randomly. If $\mathsf{ch} \in \{2, 3\}$, S executes the algorithm similar to an honest prover using $\mathbf{s}'$ as a true secret key $\mathbf{s}$. If $\mathsf{ch} \in \{0, 1\}$, S only changes the computation of c_2 and c_3 such as $c_2 \leftarrow \mathsf{Com}(\rho_2, \mathbf{t}_1, \mathbf{d}_0, \mathbf{v} - \mathbf{e}_0 - \mathbf{F}(\mathbf{r}_0))$ and $c_3 \leftarrow \mathsf{Com}(\rho_3, \mathbf{t}_0, \mathbf{d}_1, \mathbf{v} - \mathbf{e}_1 - \mathbf{F}(\mathbf{r}_0))$.

Then S can output a valid transcript, and the response holds randomness. Since Com is computationally hiding, our IDS is computationally HVZK. □

4.3 Comparison with Other $\mathcal{MQ}$-based IDSs

Table 6 compares our IDS with other $\mathcal{MQ}$-based IDSs in terms of impersonation probability (soundness) and response size. In this table, we suppose that the size of the random strings (ρ_i) of the commitment scheme (Com) is k bits and the size of the commitment (c_i) is $2k$ bits, where k is the security parameter. We also assume that n equals m in $\mathcal{MQ}(q, n, m)$ since it is the best choice in terms of the hardness of the $\mathcal{MQ}$-problem. Table 6 shows that our IDS is better in terms of soundness but not good in response size. Comparing our proposed IDS with the Monteiro et al.'s one, our scheme has the same soundness and a slightly shorter response since the security parameter k is generally smaller than $n\lceil \log q \rceil$.

5 Our New MQ-based Signature Scheme

We apply the Unruh transform to our $\mathcal{MQ}$-based 3-pass IDS to obtain a new $\mathcal{MQ}$-based DSS. In this section, we discuss the security, optimization, and parameters for our DSS.

5.1 Formal Statement of Security Proof

We prove that our DSS is EU-CMA secure in the QROM by the following theorem. This theorem is obtained from Lemma 3 and 4 in the Appendix.

Theorem 3. *Let k be the security parameter and $t, r \in \mathbb{N}$ be the parameters in Tables 4 and 5. Suppose the DSS applying the Unruh transform to the 3-pass IDS being HVZK and having an α-extractor. Let A be a quantum algorithm that breaks the EU-CMA security of the DSS with probability ϵ. Then, in the QROM there exists an algorithm M^A that breaks the KOW security of the IDS with success probability*

$$\epsilon' \geq \epsilon - \epsilon(4+\sqrt{2})q_{\mathsf{Sign}}\sqrt{q_H}2^{-\frac{rk}{4}} - 2(q_H+1)2^{-(r\log\frac{t}{\alpha-1})/2}, \tag{1}$$

where q_{Sign} and q_H denote the number of queries issued to the signing oracle and the random oracle, respectively.

This theorem is slightly changed from Theorem 23 in [20], since the IDS in the above theorem has an α-extractor and no "special soundness". The inequality (1) shows that our security reduction is tight if we choose the parameters appropriately.

5.2 Our Optimization

In this subsection, we optimize our DSS. This optimization is carried out without losing the tightness of our security reduction.

We execute our IDS for all four challenges per one commitment. This means that we do not need to include which challenges are selected in the signature. This reduces the signature size.

Then, we must include responses for all challenges, which means all blinded or opened values are included in the signature twice. For example, $\mathbf{r}_0$ is included in the response when $\mathsf{ch} = 0$ and $\mathsf{ch} = 1$. Therefore, we include each blinded or opened $\mathbf{r}_0$, $\mathbf{r}_1$, $\mathbf{t}_0$, $\mathbf{t}_1$, $\mathbf{d}_0$, $\mathbf{d}_1$, $\mathbf{e}_0$, $\mathbf{e}_1$ into the signature once. This also reduces the signature size.

When we compute $\mathsf{com} \leftarrow H(c_0, c_1, c_2, c_3, c_4, c_5)$ in each round, we can build a Merkle tree on $c_0, \ldots, c_5$ and add the root of this tree to the signature. By building a Merkle tree appropriately, we can reduce the number of commitments included in the signature for some challenges. Moreover, the signer can generate one hash value overall roots of the Merkle tree of each round and include it in the signature.

Finally, in our DSS, $\mathbf{r}_0, \mathbf{t}_0, \mathbf{d}_0 \in \mathbb{F}_q^n, \mathbf{e}_0 \in \mathbb{F}_q^m$ are chosen randomly in each round. Therefore, we can use a PRNG with a small seed to reduce the communication cost in the following. First, we choose a k-bit seed sd for PRNG randomly, where k is the security parameter and usually smaller than the bit size of elements of $\mathbb{F}_q^n, \mathbb{F}_q^m$. Next, from sd, we generate two additional seeds sd_{r_0} and $\mathsf{sd}_{t_0,d_0,e_0}$ by the PRNG, and we compute $\mathbf{r}_0$ and $\mathbf{t}_0, \mathbf{d}_0, \mathbf{e}_0$ by the PRNG with the seeds sd_{r_0} and $\mathsf{sd}_{t_0,d_0,e_0}$, respectively. On the other hand, in our DSS, $\mathbf{r}_1, \mathbf{t}_1, \mathbf{d}_1, \mathbf{e}_1$ are determined by $\mathbf{r}_0, \mathbf{t}_0, \mathbf{d}_0, \mathbf{e}_0$ and the secret key $\mathbf{s}$. Then, the signer sends sd opened for the verifier and $\mathbf{r}_1, \mathbf{t}_1, \mathbf{d}_1, \mathbf{e}_1$ blinded for the verifier using the length-preserving hash function when $\mathsf{ch} = 0$. Similarly, the signer sends opened $\mathsf{sd}_{r_0}, \mathbf{t}_1, \mathbf{d}_1, \mathbf{e}_1$ and blinded $\mathbf{r}_1, \mathsf{sd}_{t_0,d_0,e_0}$ when $\mathsf{ch} = 1$, opened $\mathbf{r}_1, \mathsf{sd}_{t_0,d_0,e_0}$ and blinded $\mathsf{sd}_{r_0}, \mathbf{t}_1, \mathbf{d}_1, \mathbf{e}_1$ when $\mathsf{ch} = 2$, and opened $\mathbf{r}_1, \mathbf{t}_1, \mathbf{d}_1, \mathbf{e}_1$ and blinded $\mathsf{sd}_{r_0}, \mathsf{sd}_{t_0,d_0,e_0}$ when $\mathsf{ch} = 3$.

As a result, the signature is composed of $2k$-bit random string computed by the hash function H for the EU-CMA security, md in Table 5, the hash value overall roots of the Merkle tree on $c_0, \ldots, c_5$ of each round, two or three nodes of the Markle tree of each round required to reconstruct the root, opened or blinded responses and the random k-bit strings ρ_i.

5.3 Parameters

We estimate the size of the public key, secret key and signature of our DSS with the security parameter k in the following. For a quadratic system $\mathbf{F}(\mathbf{s}) = \mathbf{v}$, the public key $(\mathbf{F}, \mathbf{v})$ is expressed by $k + n\lceil\log_2 q\rceil$ bits and the secret key $\mathbf{s}$ is expressed by k bits, since the seed for the public and secret key is k bits and the bit size of elements of $\mathbb{F}_q^n$ for the public key is $n\lceil\log_2 q\rceil$. Next, the number of challenges per one round t holds $t \geq \alpha - 1 = 2$, and the number of rounds r is $r \approx 1.71k$ for $t = 3$, and $r = k$ for $t = 4$ due to $(\frac{\alpha-1}{t})^r \leq 2^{-k}$. Therefore, we choose $t = 4$ for achieving a smaller signature. When we apply the optimizations discussed in Subsection 5.2, the signature size becomes $4k + (9.25k + 4n\lceil\log_2 q\rceil + 2)r$ bits. This value is estimated by calculating the average, since the

Table 7: Applying the Unruh transform to several $\mathcal{MQ}$-based identification schemes (IDSs).

	t	signature size (bits)
Sakumoto et al.'s 5-pass IDS [19]	3	$6.84k^2 + 12.0kn\lceil \log q \rceil + 7.42k$
Sakumoto et al.'s 3-pass IDS [19]	3	$10.3k^2 + 5.13kn\lceil \log q \rceil + 7.42k$
Monteiro et al.'s 3-pass IDS [15]	4	$9.75k^2 + 5kn\lceil \log q \rceil + 6k$
Proposed IDS	4	$9.25k^2 + 4kn\lceil \log q \rceil + 6k$

Table 8: Parameter of our proposed signature.

Security category	k	q	$n = m$	r
I	128	4	88	128
III	192	4	128	192
V	256	4	160	256

Table 9: Comparing signature in each security level (1KB=1024B)

Security category	DSS	Public key size (B)	Secret key size (B)	Signature size (KB)	Security reduction
I	MQDSS	46	16	27.7	non-tight
	MUDFISH	38	16	14.4	non-tight
	Our scheme	38	16	29.6	tight
III	MQDSS	64	24	58.5	non-tight
	MUDFISH	56	24	32.9	non-tight
	Our scheme	56	24	65.8	tight
V	MQDSS	87	32	106.0	non-tight
	MUDFISH	72	32	55.6	non-tight
	Our scheme	72	32	114.2	tight

signature size of our optimized scheme is depending on the challenge in each round. (If we build a Merkle tree on commitment values such as $H(H(c_0, c_5), H(c_1, c_3), H(c_2, c_4))$ in each round, the sizes of opened and blinded response in each round are $8k + 4n\lceil \log_2 q \rceil$ bits for $\mathsf{ch} = 0$, $9k + 4n\lceil \log_2 q \rceil$ bits for $\mathsf{ch} = 1, 2$ and $11k + 4n\lceil \log_2 q \rceil$ bits for $\mathsf{ch} = 3$.)

In Table 7, we compare several signature schemes constructed by applying the Unruh transform to several $\mathcal{MQ}$-based IDSs in terms of signature size. We omit the signature scheme constructed from Beullens' IDS, since the structure of Beullens' IDS is very different from other $\mathcal{MQ}$-based IDSs as stated in Subsection 3.4. We leave the way of efficiently applying the Unruh transform to the Beullens' IDS as future work. For each scheme, we choose t so that the scheme has the shortest signature, and optimize them like our proposed scheme. This table shows that our proposed IDS has the shortest signature among the schemes constructed by applying the Unruh transform to $\mathcal{MQ}$-based IDSs. Compared to the signature size of SOFIA, that of our DSS decreases by up to about 35%.

In Table 8, we provide concrete parameters to make our DSS achieve NIST PQC security level I, III and V. We choose the parameter of $\mathcal{MQ}$-problem following the discussion by Chen et al. [4] about the $\mathcal{MQ}$-problem.

In Table 9, we show the key and signature size of our proposed signature scheme in NIST PQC security level I, III and V, and that of MQDSS and MUDFISH as reference values. The signature size of MQDSS is larger than the value in [4], since we increase the number of rounds by considering the attack on MQDSS [12]. Furthermore, MQDSS uses $2k$-bit random strings as an input on the commitment scheme, whereas MUDFISH and our scheme use k-bit random strings, which may affect the signature size in Table 9 slightly. Note that our scheme has tight security reduction and the reduction of the other two schemes are not tight.

6 Conclusion

We proposed a $\mathcal{MQ}$-based 3-pass IDS, which is obtained by changing the manner of dividing the secret key from the IDSs proposed by Sakumoto et al. and Monteiro et al. We showed that our DSS obtained by applying the Unruh transform to the proposed IDS is tightly EU-CMA secure in the QROM, and the signature size is smaller than all other DSSs, such as SOFIA, obtained by applying the Unruh transform to other $\mathcal{MQ}$-based IDSs.

By using the recent security results of the Fiat-Shamir transform in the QROM at CRYPTO 2019, the $\mathcal{MQ}$-based DSSs from the Fiat-Shamir transform such as MUDFISH is proven to be EU-CMA secure in the QROM. However, tight security proof for the $\mathcal{MQ}$-based DSS from the Fiat-Shamir transform has not been proposed. Therefore, our DSS currently has the shortest signature among all $\mathcal{MQ}$-based DSS with tight security proof.

We leave whether there is another $\mathcal{MQ}$-based DSS with tight security reduction having a smaller signature than our DSS or a tight proof for MQDSS or MUDFISH as future work.

Acknowledgment

This work was supported by JST CREST Grant Number JPMJCR14D6, Japan.

References

[1] W. Beullens. Sigma protocols for MQ, PKP and SIS, and fishy signature schemes. IACR Cryptology ePrint Archive 2019: 490, 2019.

[2] M. S. Chen, A. Hülsing, J. Rijneveld, S. Samardjiska, and P. Schwabe. From 5-pass MQ-based identification to MQ-based signatures. *ASIACRYPT 2016*, 10032 of LNCS:135–165, 2016.

[3] M. S. Chen, A. Hülsing, J. Rijneveld, S. Samardjiska, and P. Schwabe. SOFIA: MQ-based signature in the QROM. *PKC 2018*, 10770 of LNCS:3–33, 2018.

[4] M. S. Chen, A. Hülsing, J. Rijneveld, S. Samardjiska, and P. Schwabe. MQDSS specification version 2.0, 2019. Round 2 submission to the NIST post-quantum cryptography project.

[5] N. T. Courtois. Efficient zero-knowledge authentication based on a linear algebra problem MinRank. *ASIACRYPT 2001*, 2248 of LNCS:402–421, 2001.

[6] J. Ding and D. Schmidt. Rainbow, a new multivariate polynomial signature scheme. *ACNS 2005*, 3531 of LNCS:164–175, 2005.

[7] J. Don, S. Fehr, and C. Majenz. The measure-and-reprogram technique 2.0: multi-round Fiat-Shamir and more. IACR Cryptology ePrint Archive 2020: 282, 2020.

[8] J. Don, S. Fehr, C. Majenz, and C. Schaffner. Security of the Fiat-Shamir transformation in the quantum random-oracle model. *CRYPTO 2019*, 11693 of LNCS:356–383, 2019.

[9] J. C. Faugére, F. Levy dit Vehel, and L. Perret. Cryptanalysis of MinRank. *CRYPTO 2008*, 5157 of LNCS:280–296, 2008.

[10] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. *CRYPTO 1986*, 263 of LNCS:186–194, 1987.

[11] M. R. Garey and D. S. Johnson. *Computers and intractability: a guide to the theory of NP-completeness*. W. H. Freeman, 1979.

[12] D. Kales and G. Zaverucha. Forgery attacks on MQDSSv2.0. 2019.

[13] D. Leichtle. Post-quantum signatures from identification schemes. Master's thesis, Technicshe Universiteit Eindhoven, 2018.

[14] Q. Liu and M. Zhandry. Revisiting post-quantum Fiat-Shamir. *CRYPTO 2019*, 11693 of LNCS:326–355, 2019.

[15] F. S. Monteiro, D. H. Goya, and R. Terada. Improved identification protocol based on the MQ problem. *IEICE*, pages E98–A, 2015.

[16] NIST. Post-quantum Cryptography, Round 2 Submissions. `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions`, 2019. [Online; accessed 03-July-2019].

[17] J. Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. *EUROCRYPT 1996*, 1070 of LNCS:33–48, 1996.

[18] A. Petzoldt, M. S. Chen, B. Y. Yang, C. Tao, and J. Ding. Design principles for HFEv- based multivariate signature schemes. *ASIACRYPT 2015*, 9452 of LNCS:311–334, 2015.

[19] K. Sakumoto, T. Shirai, and H. Hiwatari. Public-key identification scheme based on multivariate quadratic polynomials. *CRYPTO 2011*, 6841 of LNCS:706–723, 2011.

[20] D. Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. *EUROCRYPT 2015*, 9057 of LNCS:755–784, 2015.

[21] M. Zhandry. Secure identity-based encryption in the quantum random oracle model. *CRYPTO 2012*, 7417 of LNCS:758–775, 2012.

A Signature from IDS Having α-extractor

We prove the security of our DSS obtained by applying the Unruh transform to our 3-pass IDS with α-extractor and computational HVZK. We prove that our DSS is EU-CMA secure in the ROM in Subsection A.1 and in the QROM in Subsection A.2.

A.1 EU-CMA Security in the ROM

We show that a quantum algorithm that breaks the EU-CMA security can be used to extract a valid secret key. Our proof is mainly based on the proof in the study by Chen et al. [3].

Lemma 1. *Let k be the security parameter and $t, r \in \mathbb{N}$ be the parameters in Tables 4 and 5. Suppose the DSS applying the Unruh transform to the 3-pass IDS having an α-extractor. Let A be a quantum algorithm that implements a key-only-attack (KOA) forger, which given only the public key pk outputs a valid message-signature with probability ϵ. Then, in the classical ROM there exists an algorithm M^A that given oracle access to any such A breaks the KOW security of the IDS in essentially the same running time as the given A and with success probability*

$$\epsilon' \geq \epsilon - (q_H + 1)2^{-r \log \frac{t}{\alpha - 1}},$$

where q_H denotes the number of queries issued to the random oracle. Moreover, M^A only manipulates the random oracle G and leaves random oracle H untouched.

Proof. This lemma is almost proved by the proof in Lemma 3.1 in the study by Chen et al. [3]. Therefore, we show only a sketch of the proof.

Let $\mathbf{E}_A$ be the event that A outputs a valid message-signature pair (M, σ). Note that M^A can open all blinded responses in the signature because M^A learns all of A's queries.

Let $T(j, i)$ be the following string: $(\mathsf{com}^{(j)}, \mathsf{ch}^{(i,j)}, \mathsf{resp}^{(i,j)})$, and $\mathbf{E}_{\neg\mathsf{ext}}$: $\forall j \in \{1, \ldots, r\}$, $T(j, i)$ is valid in at most $\alpha - 1$ elements of $\{1, \ldots, t\}$. We try to evaluate the probability of $\mathbf{E}_{\neg\mathsf{ext}}$, since the secret key can be recovered if α or more strings of $T(j, i)$ ($i \in \{1, \ldots, t\}$) are valid. In order for the signature to pass the verification, H must choose one of $i \in \{1, \ldots, t\}$ having a valid response. Thus, this probability is $\frac{(\alpha-1)^r}{t^r} = 2^{-r \log \frac{t}{\alpha-1}}$. Now let q_H be the number of queries to H. Then

$$\mathsf{Pr}[\mathbf{E}_A \wedge \mathbf{E}_{\neg\mathsf{ext}}] \leq (q_H + 1)2^{-r \log \frac{t}{\alpha-1}},$$

as A can try at most q_H tuples.

Consequently, we obtain the following:

$$\begin{aligned}\epsilon' &\geq \mathsf{Pr}[\mathbf{E}_A \wedge \neg \mathbf{E}_{\neg \mathsf{ext}}] \\ &= \mathsf{Pr}[\mathbf{E}_A] - \mathsf{Pr}[\mathbf{E}_A \wedge \mathbf{E}_{\neg \mathsf{ext}}] \\ &\geq \epsilon - (q_H+1)2^{-r\log\frac{t}{\alpha-1}}.\end{aligned}$$

□

Lemma 2. *Let k be the security parameter and $t, r \in \mathbb{N}$ be the parameters in Tables 4 and 5. Suppose the DSS applying the Unruh transform to the 3-pass IDS being HVZK. Let A be a quantum algorithm that breaks the EU-CMA security of the DSS with probability ϵ. Then, in the classical ROM there exists an algorithm M^A that breaks the KOA security of the DSS in essentially the same running time as the given A and with success probability*

$$\epsilon' \geq \epsilon(1 - q_{\mathsf{Sign}} q_H 2^{-rk}),$$

where q_{Sign} and q_H denote the number of queries issued to the signing oracle and the random oracle, respectively. Moreover, M^A only manipulates H and leaves G untouched.

This lemma is almost the same as Lemma 3.2 in the study by Chen et al. [3].

We obtain the following theorem from the two previous lemmas.

Theorem 4. *Let k be the security parameter and $t, r \in \mathbb{N}$ be the parameters in Tables 4 and 5. Suppose the DSS applying the Unruh transform to the 3-pass IDS being HVZK and having an α-extractor. Let A be a quantum algorithm that breaks the EU-CMA security of the signature scheme with probability ϵ. Then, in the classical ROM there exists an algorithm M^A that breaks the KOW security of the IDS in essentially the same running time as the given A and with success probability*

$$\epsilon' \geq \epsilon - \epsilon q_{\mathsf{Sign}} q_H 2^{-rk} - (q_H+1)2^{-r\log\frac{t}{\alpha-1}},$$

where q_{Sign} and q_H denote the number of queries issued to the signing oracle and the random oracle, respectively.

A.2 EU-CMA Security in the QROM

We show that a quantum algorithm that breaks the EU-CMA security can be used to extract a valid secret key in the QROM. Our proof is mainly based on the proofs in previous studies [3, 20].

Lemma 3. *Let k be the security parameter and $t, r \in \mathbb{N}$ be the parameters in Tables 4 and 5. Suppose the DSS applying the Unruh transform to the 3-pass IDS having an α-extractor. Let A be a quantum algorithm that implements a KOA forger, which given only the public key pk, outputs a valid message-signature with probability ϵ. Then, in the QROM there exists an algorithm M^A that given oracle access to any such A breaks the KOW security of the IDS with success probability*

$$\epsilon' \geq \epsilon - 2(q_H+1)2^{-(r\log\frac{t}{\alpha-1})/2},$$

where q_H denotes the number of queries issued to the random oracle. Moreover, M^A only manipulates G and leaves H untouched.

Proof. This lemma is mainly proved by the proof in Lemma 3.5 in the study by Chen et al. [3] and Theorem 18 in that by Unruh [20]. Therefore, we show only a sketch of the proof.

The changes in the proof from that in the classical ROM are as follows. First, M^A cannot learn A's random oracle queries to G. A previous study [21] showed that a random function is indistinguishable from a $2q$-wise independent function (where q is the number of oracle queries carried out), and random polynomials of degree $2q-1$ are $2q$-wise independent. Therefore, M^A can open the blinded responses in the signature by replacing G with a random polynomial of degree $2q-1$ and inverting the polynomial. (The preimage will not be unique, but the number of possible preimages will be small enough so that we can scan through all of them [20].) Second, the probability of $\mathbf{E}_A \wedge \mathbf{E}_{\neg \mathsf{ext}}$ changes to $2(q_H+1)2^{-(r\log\frac{t}{\alpha-1})/2}$ by Lemma 7 in the study by Unruh [20]. □

Lemma 4. *Let k be the security parameter and $t, r \in \mathbb{N}$ be the parameters in Tables 4 and 5. Suppose the DSS applying the Unruh transform to the 3-pass IDS being HVZK. Let A be a quantum algorithm that breaks the EU-CMA security of the DSS with probability ϵ. Then, in the QROM there exists an algorithm M^A that breaks the KOA security of the DSS with success probability*

$$\epsilon' \geq \epsilon\{1 - (4 + \sqrt{2})q_{\mathsf{Sign}}\sqrt{q_H}2^{-\frac{rk}{4}}\},$$

where q_{Sign} and q_H denote the number of queries issued to the signing oracle and the random oracle, respectively. Moreover, M^A only manipulates H and leaves G untouched.

This lemma is almost the same as Theorem 15 in the study by Unruh [20].
We obtained Theorem 3 in Subsection 5.1 from these two lemmas.