An Efficient $\mathcal{MQ}$-based Signature in the QROM

Hiroki Furue[1,a)] Dung Hoang Duong[2,b)] Tsuyoshi Takagi[1,c)]

Abstract: At PKC 2018, Chen et al. proposed SOFIA, the first $\mathcal{MQ}$-based digital signature scheme secure 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 secure in the QROM. The signature size with our digital signature scheme decreases by about 30% compared with SOFIA.

Keywords: Post-quantum cryptography, Multivariate 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-hard [8]. Even though the $\mathcal{MQ}$-problem is basic for multivariate public key cryptography (MPKC), almost all current schemes [4, 13] are not based on $\mathcal{MQ}$-problem but related to problems such as the Isomorphism of Polynomial (IP) problem [12] or the MinRank problem [3, 6]. At AsiaCrypt 2016, Chen et al. proposed MQDSS [1], 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 [7] to the $\mathcal{MQ}$-based 5-pass identification scheme (IDS) proposed by Sakumoto et al. [14]. The security of this IDS is proven in the random oracle model (ROM). MQDSS is a $\mathcal{MQ}$-based digital signature scheme (DSS) that have passed into the second round of NIST call for post-quantum proposals [11]. However, MQDSS is not proven to be secure in the quantum random oracle model (QROM), which means that a quantum adversary can access the random oracle in superposition, and the reduction in the security in the ROM is not tight.

At PKC 2018, Chen et al. [2] proposed a DSS called SOFIA obtained by applying the Unruh transform [15] to the $\mathcal{MQ}$-based 5-pass IDS proposed by Sakumoto et al. [14]. This DSS is proven secure not only in the ROM but also in the QROM, and the security reduction is tight in the ROM. 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 because 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 round will increase if the impersonation probability becomes larger. Therefore, this makes the signature size larger.

Table 1 Unruh transform applied to several $\mathcal{MQ}$-based identification schemes. (r: number of rounds, t: number of challenges per round)

$\mathcal{MQ}$-based signature secure in the QROM	r	t	signature (bytes)
SOFIA [2]	438	3	126, 176
DSS from Sakumoto et al.'s IDS [14]	438	3	98, 144
DSS from Monteiro et al.'s IDS [10]	257	4	98, 720
DSS from our proposed 3-pass IDS	257	4	**90, 496**

Our contribution. We first propose an $\mathcal{MQ}$-based 3-pass IDS with impersonation probability of $\frac{1}{2}$ to obtain a more efficient $\mathcal{MQ}$-based DSS that is proven to be secure in the QROM by applying the original version of the Unruh transform [15] to the proposed IDS. We also apply this transform to other 3-pass IDSs by Sakumoto et al. [14] and Monteiro et al. [10] to obtain two other $\mathcal{MQ}$-based DSSs. We then compared the three DSSs with SOFIA at the 128-bit quantum security level (see Table 1). Among others, our DSS is the most efficient among all others secure in the QROM. In particular, the signature size of our DSS decreased by about 30% compared with SOFIA.

[1] Graduate school of Information Science and Technology, The University of Tokyo
[2] Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong
[a)] hiroki_furue@mist.i.u-tokyo.ac.jp
[b)] hduong@uow.edu.au
[c)] takagi@mist.i.u-tokyo.ac.jp

Our technique in designing a new 3-pass IDS combines both IDSs of Sakumoto et al. [14] and Monteiro et al. [10]. However, our IDS is different in the manner of splitting information. As a result, it has impersonation probability of $\frac{1}{2}$, which is the same as that of Monteiro et al. ' s, whereas it is $\frac{2}{3}$ for the 3-pass IDS of Sakumoto et al. 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 5). However, if we construct an $\mathcal{MQ}$-based DSS by applying the Unruh transform to our IDS, then the signature of that DSS is smaller than the those of DSSs using the previous 3-pass IDSs.

Table 2 Fiat-Shamir transform applied to several $\mathcal{MQ}$-based identification schemes. (r: number of rounds)

$\mathcal{MQ}$-based signature secure in the ROM	r	signature (bytes)
MQDSS [1]	269	40952
DSS from Sakumoto et al. ' s 3-pass IDS [14]	438	56128
DSS from Monteiro et al. ' s 3-pass IDS [10]	257	57632
DSS from our 3-pass IDS	257	**57632**

Fiat-Shamir transform case. We also compared several $\mathcal{MQ}$-based DSSs that are secure in the classical ROM. It is possible to construct $\mathcal{MQ}$-based DSSs by applying the Fiat-Shamir transform to the 3-pass IDSs by Sakumoto et al. [14], Monteiro et al. [10], and ours. However, the obtained signatures in the ROM are larger than that of MQDSS (see Table 2).

Very recently, the security of DSSs constructed from the Fiat-Shamir transform in the QROM has been discussed [5,9]. It is a future work to investigate the security of $\mathcal{MQ}$-based DSSs using the Fiat-Shamir transform in the QROM by applying these new results.

Our paper is organized as follows. In Section 2, we give the definitions of IDS and DSS, and explain the Unruh transform. In Section 3, we recall the $\mathcal{MQ}$-problem and explain the $\mathcal{MQ}$-based 3-pass IDS proposed by Sakumoto et al. [14]. 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 [2]. We then explain the Unruh transform.

2.1 Identification Scheme (IDS)

2.1.1 3-pass IDS

A 3-pass IDS with security parameter k, denoted as IDS(1^k), is a triplet of probabilistic polynomial time (PPT) algorithms IDS = (KGen, P, V) such that key generator algorithm KGen is a probabilistic algorithm that outputs a key pair (sk, pk), and P and V are interactive prover and verifier algorithms executing a common protocol, respectively. 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 $V = (\mathrm{ChS}, \mathrm{Vf})$ works as follows: $P_0(sk)$ 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, V computes the challenge message $ch \xleftarrow{R} Ch$, sampling at random from the challenge space Ch and sends to P. Now P uses $P_1(st, ch)$ to computes the response $resp$, which is sent back to V. The V computes $\mathrm{Vf}(pk, com, ch, resp)$ to yield the final decision whether to accept or reject.

For correctness of an IDS, we require that for all $(pk, sk) \leftarrow \mathrm{KGen}()$ a verifier given pk outputs "accept" interacting with an honest prover given sk. We denote the transcript of messages exchanged during this execution as $\mathrm{trans}(\langle P(sk), V(pk)\rangle)$. Moreover, the probability that the com takes a given value is $\leq 2^{-k}$, where the probability is taken over the random choice of the input and the used randomness.

Definition 1 (Key relation)**.** *Let* IDS *be a 3-pass IDS and R be a relation. We say that* IDS *has key relation R if and only if R is the minimal relation such that*

$$\forall (pk, sk) \leftarrow \mathrm{KGen}() : (pk, sk) \in R.$$

Definition 2 (PQ-KOW)**.** *Let k be the security parameter and* IDS(1^k) *be a 3-pass IDS with key relation R. We call* IDS *post-quantum key-one-way (PQ-KOW) if for any quantum polynomial time algorithm A,*

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

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

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

Definition 4 (α-extractor)**.** *Let* IDS(1^k) *be a 3-pass IDS with R. We say that* IDS(1^k) *has an α-extractor if $|Ch| \geq \alpha$ and there exists a polynomial time algorithm K, the extractor, that, given a public key pk and α valid transcripts for pk:*

$$\begin{aligned} trans^{(1)} &= (com, ch^{(1)}, resp^{(1)}), \\ trans^{(2)} &= (com, ch^{(2)}, resp^{(2)}), \\ trans^{(3)} &= (com, ch^{(3)}, resp^{(3)}), \end{aligned}$$

where $ch^{(1)} \neq ch^{(2)}$, $ch^{(2)} \neq ch^{(3)}$, and $ch^{(3)} \neq ch^{(1)}$, output a secret key sk such that $(pk, sk) \in R$ with success probability $1 - negl(k)$.

Table 3 Signature generation.

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

Table 4 Verification.

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

2.2 Digital signature scheme (DSS)

2.2.1 Digital signature scheme

A DSS with k, denoted as $\mathrm{DSS}(1^k)$, is a triplet of PPT algorithms $\mathrm{DSS} = (\mathrm{KGen}, \mathrm{Sign}, \mathrm{Vf})$ such that key generator algorithm KGen is a probabilistic algorithm that outputs a key pair (sk, 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".

Definition 5 (PQ-EU-CMA)**.** *Let* $\mathrm{DSS}(1^k)$ *be a DSS with* k*. We call such a* DSS *post-quantum existential unforgeability under adaptive chosen message attacks (PQ-EU-CMA) secure if for any A making queries to a classical signing oracle* Sig*,*

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

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

2.3 Unruh Transform

The Unruh transform [15] converts an IDS into a DSS. The basic idea is to let the signer generate several transcripts for one *com*. This is iterated for several initial *com*s. Tables 3 and 4 list the details of the transformation.

3. $\mathcal{MQ}$-based Identification schemes

In this section, we recall the $\mathcal{MQ}$-problem and 3-pass IDS by Sakumoto et al. [14].

3.1 $\mathcal{MQ}$ problem

Let $\mathbf{F} = (f_1, \ldots, f_m)$ be a system of quadratic polynomials with n variables $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$. We denote the problem to find $\mathbf{x} \in \mathbb{F}_q^n$ such that $\mathbf{F}(\mathbf{x}) = \mathbf{y}$ as $\mathcal{MQ}(n, m, q)$, where $\mathbf{y} \in \mathbb{F}_q^m$. Garey and Johnson [8] showed that the $\mathcal{MQ}$-problem is NP-complete. In addition, there is no quantum algorithm to solve the problem in polynomial time. Therefore, this problem is known to be resistant to quantum adversaries.

3.2 Protocols

Let us first explain the $\mathcal{MQ}$-based 3-pass IDS proposed by Sakumoto et al. [14], which is the most basic among $\mathcal{MQ}$-based IDSs. Suppose that $\mathbf{F}$ denotes the $\mathcal{MQ}$ function. In this IDS, $\mathbf{G}$ denotes a polar system such that $\mathbf{G}(\mathbf{a}, \mathbf{b}) := \mathbf{F}(\mathbf{a} + \mathbf{b}) - \mathbf{F}(\mathbf{a}) - \mathbf{F}(\mathbf{b})$. Then $\mathbf{G}$ has bilinearity.

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

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

Then we obtain the following:

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

Because this equation can be seen as the function of $\mathbf{r}_1$ not $\mathbf{r}_0$, the prover can prove that he has the secret key without giving any information to the verifier. Figure 1 shows the details of this scheme.

Sakumoto et al.'s 3-pass IDS has impersonation probability of $\frac{2}{3}$; hence, to reach a desired security level, one needs to repeat the protocol a number of rounds. Sakumoto et al. 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 implies the most up-to-date efficient MQDSS.

In 2015, Monteiro et al. [10] 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:

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

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.

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. [14] and Monteiro et al. [10]. In our IDS, we also use the polar system $\mathbf{G}$, as with these schemes, but we change the manner of splitting the infor-

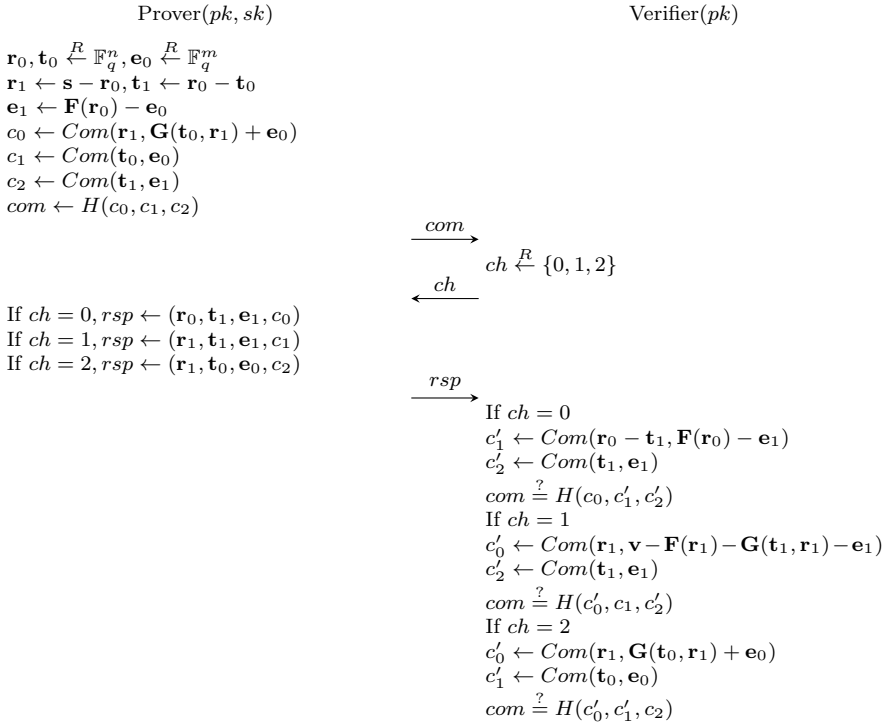

Fig. 1 $\mathcal{MQ}$-based 3-pass identification scheme (IDS) proposed by Sakumoto et al.

mation. We divide $\mathbf{s}$ 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. 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.

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 $\mathbf{s}'$ randomly from $\mathbb{F}_q^n$ and executes other steps similar to an honest prover. If ch is 2 or 3, then C succeeds. When ch is 0 or 1, C also succeeds by computing $c_2 \leftarrow Com(\mathbf{t}_1, \mathbf{d}_0, \mathbf{v} - \mathbf{e}_0 - \mathbf{F}(\mathbf{r}_0))$ and $c_3 \leftarrow Com(\mathbf{t}_0, \mathbf{d}_1, \mathbf{v} - \mathbf{e}_1 - \mathbf{F}(\mathbf{r}_0))$. These adversaries cheat 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 a given a set of valid transcriptions: $\{(com, 1, rsp_1), \quad (com, 2, rsp_2), \quad (com, 3, rsp_3)\}$. Let $c_0, c_1, c_2, c_3, c_4, c_5$ be the commitment value and

$$\begin{aligned} rsp_1 &= (\mathbf{r}_0^{(1)}, \mathbf{t}_1^{(1)}, \mathbf{d}_1^{(1)}, \mathbf{e}_1^{(1)}, c_1, c_2, c_4), \\ rsp_2 &= (\mathbf{r}_1^{(2)}, \mathbf{t}_0^{(2)}, \mathbf{d}_0^{(2)}, \mathbf{e}_0^{(2)}, c_0, c_2, c_5), \\ rsp_3 &= (\mathbf{r}_1^{(3)}, \mathbf{t}_1^{(3)}, \mathbf{d}_1^{(3)}, \mathbf{e}_1^{(3)}, c_0, c_3, c_4). \end{aligned}$$

Then we have the following:

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

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: $\mathbf{r}_1^{(2)} = \mathbf{r}_1^{(3)}$, $\mathbf{r}_0^{(1)} - \mathbf{t}_1^{(1)} = \mathbf{t}_0^{(2)}$, $\mathbf{t}_1^{(1)} = \mathbf{t}_1^{(3)}$, $\mathbf{e}_1^{(1)} = \mathbf{e}_1^{(3)}$, $\mathbf{e}_0^{(2)} - \mathbf{G}(\mathbf{t}_0^{(2)}, \mathbf{r}_1^{(2)}) = \mathbf{G}(\mathbf{t}_1^{(3)}, \mathbf{r}_1^{(3)}) - \mathbf{e}_1^{(3)}$, $\mathbf{v} - \mathbf{e}_1^{(1)} - \mathbf{F}(\mathbf{r}_0^{(1)}) = \mathbf{e}_0^{(2)} + \mathbf{F}(\mathbf{r}_1^{(2)})$. 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.

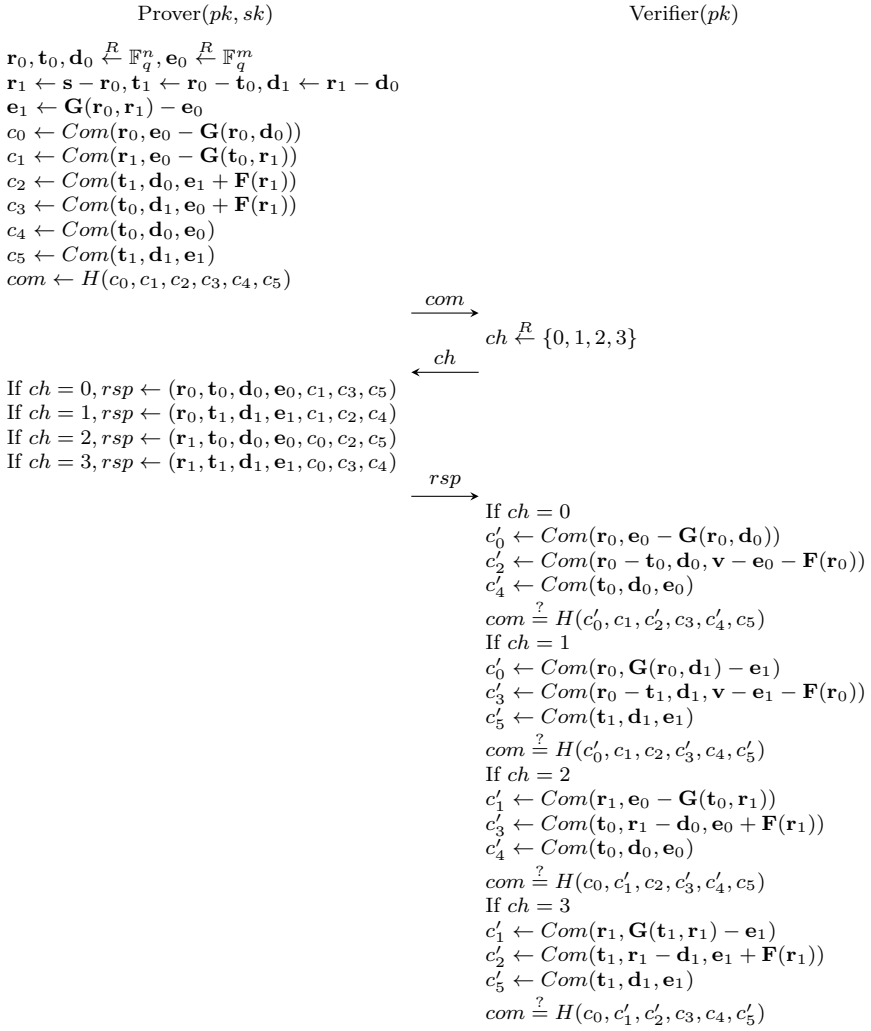

Fig. 2 Protocol of proposed $\mathcal{MQ}$-based 3-pass identification scheme (IDS).

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

Now we show that our IDS is computationally PQ-HVZK.

Theorem 2. *Our IDS is computationally PQ-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 $\mathbf{s}' \in \mathbb{F}_n^q$ randomly. If $ch \in \{2, 3\}$, S executes the algorithm similar to an honest prover using $\mathbf{s}'$ as $\mathbf{s}$. If $ch \in \{0, 1\}$, S only changes the computation of c_2 and c_3 such as $c_2 \leftarrow Com(\mathbf{t}_1, \mathbf{d}_0, \mathbf{v} - \mathbf{e}_0 - \mathbf{F}(\mathbf{r}_0))$ and $c_3 \leftarrow Com(\mathbf{t}_0, \mathbf{d}_1, \mathbf{v} - \mathbf{e}_1 - \mathbf{F}(\mathbf{r}_0))$.

Then S can output a valid transcription, and the response holds randomness. Because Com is computationally hiding, our IDS is computationally PQ-HVZK. □

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

Table 5 compares our IDS with other $\mathcal{MQ}$-based IDSs in terms of impersonation probability (soundness) and response size. In this Table, k' is the size of Com and determined by security parameter k ($k' = 2k$ in quantum security). We also assume that n equals m in $\mathcal{MQ}(n, m, \mathbb{F}_q)$ because it is the best choice in terms of hardness of the $\mathcal{MQ}$-problem.

Table 5 Several $\mathcal{MQ}$-based identification schemes (IDSs).

	soundness	response size (bits)
Sakumoto et al. ' s 5-pass IDS [14]	$1/2 + 1/2q$	$k' + 3n\lceil \log q \rceil$
Sakumoto et al. ' s 3-pass IDS [14]	$2/3$	$k' + 3n\lceil \log q \rceil$
Monteiro et al. ' s 3-pass IDS [10]	$1/2$	$2k' + 5n\lceil \log q \rceil$
Proposed IDS	$1/2$	$3k' + 4n\lceil \log q \rceil$

Table 5 shows that our IDS is better in terms of soundness but not good in response size. When we assume that k' and $n\lceil \log q \rceil$ have almost the same value, the response size of our IDS almost equals that of the IDS proposed by Monteiro et al. having the same soundness.

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 PQ-EU-CMA secure in the QROM by the following theorem. This theorem is obtained from lemmas 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 3 and 4. Suppose the DSS applying Unruh transform to 3-pass IDS being PQ-HVZK and having an α-extractor. Let A be a quantum algorithm that breaks the PQ-EU-CMA security of this DSS with probability ϵ. Then, in the QROM there exists an algorithm M^A that breaks the PQ-KOW security of this DSS with success probability*

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

This theorem is slightly changed from Theorem 23 in the study by Unruh [15] because the IDS in the above theorem has an α-extractor and no "special soundness".

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 values are included in the signature twice. For example, $\mathbf{r}_0$ is included in the response when $ch = 0$ and $ch = 1$. 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.

Moreover, the signer can omit the *com* for each round and include a hash over all *com*s instead.

From this discussion, we obtain a signature size per round in our DSS changes to $3k'+8n\lceil\log q\rceil$ from the value in Table 5, and that in the DSS from the IDS proposed by Monteiro et al. changes to $2k' + 10n\lceil\log q\rceil$.

5.3 Proposed Parameters

We provide concrete parameters to make our DSS achieve 128-bit quantum security. We choose $n = m = 128$ and $q = 4$ following the discussion by Chen et al. [2] about the $\mathcal{MQ}$-problem. We can use $t = 3$ or $t = 4$ as the number of blinded responses per round. When we decide t, we can obtain a number of rounds r so that $2^{-r\log\frac{t}{\alpha-1}/2} < 2^{-128}$ from Theorem 3. Then r becomes 438 when $t = 3$, and r becomes 257 when $t = 4$. Therefore, we choose $t = 4$ and $r = 257$ because it decreases the signature size. We also make the bit size of commitment 256 bits.

The signature of our DSS includes all commitments, responses blinded or not blinded, and commitment values for verifying in each IDS. In each round, we include eight values in $\mathbb{F}_4^{128}$ and three commitments. Because an element in $\mathbb{F}_4^{128}$ is 256 bits, the signature size is $256 + (256\times 8 + 256\times 3)\times 257 = 723,968$ bits $(90,496$ bytes$)$.

Table 1 compares our DSS with SOFIA and other DSSs obtained from the 3-pass IDSs of Sakumoto et al. and Monteiro et al. Our DSS is the best in terms of signature size. Compared to the signature size of SOFIA, that of our DSS decreases by up to about 30%.

6. Conclusion

We proposed a $\mathcal{MQ}$-based 3-pass, 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 secure in the QROM, and the signature size is smaller than all other DSSs, such as SOFIA, obtained from applying the Unruh transform to other $\mathcal{MQ}$-based IDSs.

In current studies, [5,9] showed the security of a DSS having some settings from the Fiat-Shamir transform is proved in the QROM. We leave a question whether an MQDSS, applying the Fiat-Shamir transform to the $\mathcal{MQ}$-based 5-pass IDS proposed by Sakumoto et al., is secure in the QROM as a future work.

References

[1] 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).

[2] 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).

[3] N. T. Courtois: Efficient Zero-knowledge Authentication Based on a Linear Algebra Problem MinRank, *ASIACRYPT 2001*, 2248 of LNCS, 402-421 (2001).

[4] J. Ding and D. Schmidt: Rainbow, a New Multivariate Polynomial Signature Scheme, *ACNS 2005*, 3531 of LNCS, 164-175 (2005).

[5] J. Don, S. Fehr, C. Majenz and C. Schaffner: Security of the Fiat-Shamir Transformation in the Quantum Random-oracle Model, *to apper in CRYPTO 2019*, `http://arxiv.org/abs/1902.07556` (2019).

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

[7] A. Fiat and A. Shamir: How to Prove yourself: Practical Solutions to Identification and Signature Problems, *CRYPTO 1986*, 263 of LNCS, 186-194 (1987).

[8] M. R. Garey and D. S. Johnson: *Computers and Intractability: A Guide to the Theory of NP-completeness*, W. H. Freeman (1979).

[9] Q. Liu and M. Zhandry: Revisiting Post-quantum Fiat-Shamir, *to apper in CRYPTO 2019*, `https://eprint.iacr.org/2019/262` (2019).

[10] F. S. Monteiro, D. H. Goya and R. Terada: Improved Identification Protocol Based on the MQ Problem, *IEICE*, E98-A (2015).

[11] NIST: Post-quantum Cryptography, Round 2 Submissions, `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions` (2019).

[12] 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).

[13] 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).

[14] K. Sakumoto, T. Shirai and H. Hiwatari: Public-key Identification Scheme Based on Multivariate Quadratic Polynomials, *CRYPTO 2011*, 6841 of LNCS, 706-723 (2011).

[15] D. Unruh: Non-interactive Zero-knowledge Proofs in the

Quantum Random Oracle Model, *EUROCRYPT 2015*, 9057 of LNCS, 755-784 (2015).
[16] M. Zhandry: Secure Identity-based Encryption in the Quantum Random Oracle Model, *CRYPTO 2012*, 7417 of LNCS, 758-775 (2012).

Appendix

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

A.1 PQ-EU-CMA in the ROM

We show that a quantum algorithm that breaks the PQ-EU-CMA can be used to extract a valid secret key. Our proof is mainly based on the proof in the study by Chen et al. [2].

Lemma 1. *Let k be the security parameter and $t, r \in \mathbb{N}$ be the parameters in Tables 3 and 4. Suppose the DSS applying Unruh transform to 3-pass IDS having an α-extractor. Let A be a quantum algorithm that implements a post-quantum key-only-attack (PQ-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 PQ-KOW security of the IDS in essentially the same running time as the given A and with success probability*

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

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. [2]. 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: $(com^{(j)}, ch^{(i,j)}, resp^{(i,j)})$, and $\mathbf{E}_{\neg ext}$: $\forall j \in \{1, \ldots, r\}$, $T(j,i)$ is valid in at most $\alpha - 1$ elements of $\{1, \ldots, t\}$. 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

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

as A can try at most q_H tuples.

Consequently, we obtain the following:

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

□

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

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

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. [2].

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 3 and 4. Suppose the DSS applying Unruh transform to 3-pass IDS being PQ-HVZK and having an α-extractor. Let A be a quantum algorithm that breaks the PQ-EU-CMA security of the signature scheme with probability ϵ. Then, in the classical ROM there exists an algorithm M^A that breaks the PQ-KOW security of a DSS in essentially the same running time as the given A and with success probability*

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

A.2 PQ-EU-CMA in the QROM

We show that a quantum algorithm that breaks the PQ-EU-CMA can be used to extract a valid secret key in the QROM. Our proof is mainly based on the proofs in previous studies [2, 15].

Lemma 3. *Let k be the security parameter and $t, r \in \mathbb{N}$ be the parameters in Tables 3 and 4. Suppose the DSS applying Unruh transform to 3-pass IDS having an α-extractor. Let A be a quantum algorithm that implements a PQ-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 PQ-KOW security of the IDS with success probability*

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

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. [2] and Theorem 18 in that by Unruh [15]. 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 [16] 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 by a random polynomial degree $2q-1$ and inverting the polynomial. Second, the probability of $\epsilon_A \cap \epsilon_{\neg ext}$ changes to $2(q_H+1)2^{-(r\log\frac{t}{\alpha-1})/2}$ by Lemma 7 in the study by Unruh [15]. □

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

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

Moreover, M^A only manipulates H and leaves G untouched.

This lemma is almost the same as Theorem 15 in the study by Unruh [15].

We obtained Theorem 3 in Section V from these two lemmas.