Research Article

Delaram Kahrobaei, Ludovic Perret, and Martina Vigorito*

Security analysis of ZKPoK based on MQ problem in the multi-instance setting

https://doi.org/10.1515/jmc-2024-0046
received November 30, 2024; accepted February 23, 2025

Abstract: Bidoux and Gaborit introduced a new general technique to improve zero-knowledge (ZK) proof-of-knowledge (PoK) schemes for a large set of well-known post-quantum hard computational problems such as the syndrome decoding, the permuted kernel, the rank syndrome decoding, and the multivariate quadratic (MQ) problems. In particular, the authors' idea in the study of Bidoux and Gaborit was to use the structure of these problems in the multi-instance setting to minimize the communication complexity of the resulting ZKPoK schemes. The security of the new schemes is then related to new hard problems. In this article, we focus on the new multivariate-based ZKPoK and the corresponding new underlying problem: the so-called $\mathrm{DiffMQ}_{\mathrm{H}}$. We present a new efficient probabilistic algorithm for solving the $\mathrm{DiffMQ}_{\mathrm{H}}$ which is polynomial-time if $m - n \in O(1)$. We also present experimental results showing that the algorithm is efficient in practice.

Keywords: multivariate cryptography, MQ problem, ZkPok protocol

MSC 2020: 11T06, 11T55, 11T71, 12E20

1 Introduction

With the advent of post-quantum cryptography [1] following the development of Shor's algorithm, many cryptographers have focused on finding quantum-resistant public-key systems. Multivariate cryptography is one of the main families of post-quantum primitives. The security of these systems is based on the difficulty of solving a set of randomly chosen nonlinear multivariate polynomials over a finite field. So far, there is no evidence that quantum computers can solve such sets of multivariate polynomials efficiently.

Motivated by this, Bidoux and Gaborit, in [2,3], introduced a novel general technique to enhance zero-knowledge (ZK) proof-of-knowledge (PoK) schemes for a broad class of well-known computational problems that are difficult in the post-quantum setting. In particular, they focused on the multivariate quadratic (MQ) problem, for which the definition is provided below. In the following, we denote as $\mathbb{F}_q$ a finite field with q elements, where $q = p^s$, p is a prime, and s is a positive integer.

Definition 1.1. (MQ problem) Let m and n be positive integers. We define by $\mathrm{MQ}(n, m, \mathbb{F}_q)$ the family of systems of m multivariate quadratic polynomials $\{\mathcal{F} = (p_1, \ldots, p_m) \in \mathbb{F}_q[x_1, \ldots, x_n]^m\}$ such that $\forall \ell, 1 \le \ell \le m$:

$$p_\ell(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{i,j}^{(\ell)} x_i x_j + \sum_{1 \le i \le n} c_i^{(\ell)} x_i + k^{(\ell)} \qquad \text{where } a_{i,j}^{(\ell)}, c_i^{(\ell)}, k^{(\ell)} \in \mathbb{F}_q. \tag{1}$$

* **Corresponding author: Martina Vigorito,** Departments of Mathematics, University of Salerno, Salerno, Italy, e-mail: marvigorito@unisa.it
Delaram Kahrobaei: Departments of Computer Science and Mathematics, Queens College, City University of New York, New York, United States of America; Initiative for the Theoretical Sciences, Graduate Center, City University of New York, New York, United States of America; Department of Computer Science and Engineering, Tandon School of Engineering, New York University, New York, United States of America, e-mail: delaram.kahrobaei@york.ac.uk
Ludovic Perret: Sorbonne University, CNRS, LIP6, PolSys, Paris, France; Laboratoire de Recherche de l'EPITA, 94270 Le Kremlin-Bicêtres, France, e-mail: ludovic.perret@epita.fr

Given $\mathcal{F} \in \mathrm{MQ}(n, m, \mathbb{F}_q)$ and $\boldsymbol{v} = (v_1, \ldots, v_m) \in \mathbb{F}_q^m$, the MQ problem asks to find $\boldsymbol{s} \in \mathbb{F}_q^n$ such that

$$p_1(\boldsymbol{s}) = v_1, \ldots, p_m(\boldsymbol{s}) = v_m.$$

We will call the $\mathrm{MQ_H}$ the restriction of the MQ to homogeneous polynomials.

The solution of the MQ remains computationally challenging, as it is known to be NP-hard [4]. This hardness forms the foundation of various cryptographic schemes, particularly in the field of post-quantum cryptography, where the security of multivariate public-key cryptosystems relies on the difficulty of solving large instances of the MQ. In fact, these problems are widely used as the basis for many proposed post-quantum digital signature schemes, for example, Biscuit signature scheme [5], GeMSS [6], UOV signature scheme [7], and MAYO signatures [8].

In this article, we investigate the security of a new ZKPoK based on the MQ introduced in the studies of Bidoux and Gaborit [2,3]. The ZKPoK schemes are significant due to their practical applications in cryptography [9–11]. One of the key reasons to study these schemes is that they provide a foundation for constructing highly efficient digital signature schemes, [12–14]. By leveraging the properties of zero-knowledge proofs, it is possible to design digital signatures that offer both strong security guarantees and improved performance. This makes ZKPoK particularly attractive for real-world implementations where efficiency and security are crucial.

One way to construct a signature scheme is to first construct a ZKPoK scheme and then transform it to a non-interactive signature scheme with a transformation such as the Fiat-Shamir transform [14] or the Unruh transform [15]. Looking at the NIST Post-Quantum Standardization project, three of the Round II signature schemes, MQDSS, Picnic, and Dilithium, use this approach [16].

Considering the significance of ZKPoK, Bidoux and Gaborit [2,3] presented a new ZKPoK scheme, which we will call MQBG, which is related to new variants of the $\mathrm{MQ_H}$ such as the $\mathrm{MQ_H^+}$. This problem occurs in the multi-instance setting and it is defined as follows.

Definition 1.2. ($\mathrm{MQ_H^+}$ problem) Let m and n be positive integers, we define by $\mathrm{MQ_H}(n, m, \mathbb{F}_q)$ the family of systems of m multivariate quadratic homogeneous polynomials $\{\mathcal{F} = (p_1, \ldots, p_m) \in \mathbb{F}_q[x_1, \ldots, x_n]^m\}$ such that $\forall \ell, 1 \le \ell \le m$:

$$p_\ell(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{i,j}^{(\ell)} x_i x_j, \quad \text{where } a_{i,j}^{(\ell)} \in \mathbb{F}_q. \tag{2}$$

Given $\mathcal{F} \in \mathrm{MQ_H}(n, m, \mathbb{F}_q)$ and $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_M \in \mathbb{F}_q^m$. The $\mathrm{MQ_H^+}$ problem asks to find $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_M \in \mathbb{F}_q^n$ such that

$$\mathcal{F}(\boldsymbol{s}_1) = \boldsymbol{v}_1, \ldots, \mathcal{F}(\boldsymbol{s}_M) = \boldsymbol{v}_M.$$

Bidoux and Gaborit [2,3] claimed that the security of this MQBG relies on a new intermediate problem which is called the differential multivariate quadratic homogeneous ($\mathrm{DiffMQ_H^+}$) problem in a multi-instance version that follows.

Definition 1.3. ($\mathrm{DiffMQ_H^+}$ problem) Let $M \ge 1$, m, n be positive integers, $\mathcal{F} \in \mathrm{MQ_H}(n, m, \mathbb{F}_q)$ and $(\boldsymbol{u}_1, \boldsymbol{v}_1)$, $\ldots, (\boldsymbol{u}_M, \boldsymbol{v}_M) \in \mathbb{F}_q^n \times \mathbb{F}_q^m$ such that $\mathcal{F}(\boldsymbol{u}_1) = \boldsymbol{v}_1, \ldots, \mathcal{F}(\boldsymbol{u}_M) = \boldsymbol{v}_M$. Given $\kappa_1, \kappa_2 \in \mathbb{F}_q^*$, the $\mathrm{DiffMQ_H^+}$ problem asks to find $(\boldsymbol{c}, \boldsymbol{d}_1, \boldsymbol{d}_2) \in \mathbb{F}_q^m \times \mathbb{F}_q^n \times \mathbb{F}_q^n$ such that

$$\mathcal{F}(\boldsymbol{d}_1) + \boldsymbol{c} = \kappa_1^2 \boldsymbol{v}_{\mu_1} \quad \text{and} \quad \mathcal{F}(\boldsymbol{d}_2) + \boldsymbol{c} = \kappa_2^2 \boldsymbol{v}_{\mu_2}, \tag{3}$$

with $\mu_1, \mu_2 \in [1, \ldots, M]$.

More precisely, the $\mathrm{DiffMQ_H^+}$ is related to the special soundness of MQBG, that is the property of a cryptographic protocol, which ensures that if an adversary can convince a verifier of a false statement with some probability, then there exists an efficient algorithm that can extract a witness from any such convincing interaction.

1.1 Organization of the article and main results

This article is structured as follows. In Section 2, we describe MQBG. Section 3 presents the main result of this work, that is, a probabilistic polynomial-time algorithm for solving the $\mathrm{DiffMQ}_{\mathrm{H}}^{+}$, in particular, we will prove the following theorem:

Theorem 1.1. *Let $\mathcal{F} \in \mathrm{MQ}_{\mathrm{H}}(n, m, \mathbb{F}_q)$, where m and n are positive integers. Then, there exists a probabilistic polynomial-time algorithm that solves the* $\mathrm{DiffMQ}_{\mathrm{H}}^{+}$ *with probability $O(1/q^{m-n})$.*

To do so, we show that the $\mathrm{DiffMQ}_{\mathrm{H}}^{+}$ reduces to solving a linear system generated from the polar form of multivariate public-key quadratic polynomials. In Section 3.1, we report the experimental results obtained in Magma V2.20-3 that confirm our claim, that is the algorithm is efficient and succeeds with probability $O(1/q^{m-n})$, where m denotes the number of polynomials and n the number of variables. Note that Bidoux and Gaborit [3] only proposed parameters of the MQ with $m = n$; in this case, our algorithm returns a solution with probability one.

It was initially claimed that the $\mathrm{DiffMQ}_{\mathrm{H}}^{+}$ is not easier than the $\mathrm{MQ}_{\mathrm{H}}^{+}$ (see [3, Theorem 8]), i.e., if there exists a polynomial-time algorithm solving the $\mathrm{DiffMQ}_{\mathrm{H}}^{+}$ with success probability p, then there exists a polynomial-time algorithm solving the $\mathrm{MQ}_{\mathrm{H}}^{+}$ with probability $\left(1 - \frac{1}{q^{m-n}}\right)p$. This statement was then revisited in the updated version [2]. However, the $\mathrm{DiffMQ}_{\mathrm{H}}^{+}$ was still defined and the complexity was not known until now. The contribution of this work is to show that the problem on which the proof of the special soundness of MQBG is based, see [3, Appendix G], can be solved in polynomial time, meaning that the security of MQBG needs to be improved.

2 Description of the protocol and security analysis

The MQ-based ZKPoK introduced in the study of Bidoux and Gaborit [3], which we will call MQBG, is inspired by the recent ZKPoK proposed by Wang [12]. In particular, these protocols use the polar form associated with a set of quadratic equations:

Definition 2.1. (Polar form) Let m, n be positive integers and $\mathcal{F} \in \mathrm{MQ}_{\mathrm{H}}(n, m, \mathbb{F}_q)$. The polar form $\mathcal{F}' \in \mathbb{F}_q[x_1, \ldots, x_n, y_1, \ldots, y_n]^m$ associated with $\mathcal{F}$ is defined as follows:

$$\mathcal{F}'(\boldsymbol{x}, \boldsymbol{y}) = \mathcal{F}(\boldsymbol{x} + \boldsymbol{y}) - \mathcal{F}(\boldsymbol{x}) - \mathcal{F}(\boldsymbol{y}), \tag{4}$$

with $\boldsymbol{x} = (x_1, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, \ldots, y_n)$ being variables.

Note that the polar form of a multivariate quadratic map is symmetric and bilinear.

We can now quickly recall the basics of MQBG from the study of Bidoux and Gaborit [3], which is depicted in Figure 1.

Let $\mathcal{F} \in \mathrm{MQ}_{\mathrm{H}}(n, m, \mathbb{F}_q)$ be a system of m multivariate quadratic homogeneous polynomials in n variables, and $\mathcal{F}' : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q^n$ be its polar form. We can rewrite (4) as follows:

$$\mathcal{F}(\boldsymbol{x}) - \mathcal{F}(\boldsymbol{x} - \boldsymbol{y}) = \mathcal{F}'(\boldsymbol{y}, \boldsymbol{x} - \boldsymbol{y}) + \mathcal{F}(\boldsymbol{y}).$$

The specificity of MQBG is to use an instance of the MQ_{H} with $M > 1$ solutions. The secret key sk is given by $(\boldsymbol{x}_i)_{i\in[1,M]} \in (\mathbb{F}_q^n)^M$ and the public key pk is composed by $\mathcal{F} \in \mathrm{MQ}_{\mathrm{H}}(n, m, \mathbb{F}_q)$ and $(\boldsymbol{y}_i)_{i\in[1,M]} = (\mathcal{F}(\boldsymbol{x}_i))_{i\in[1,M]} \in (\mathbb{F}_q^m)^M$. The challenge $\mathsf{ch}_{\mathsf{struct}}$ from the verifier V is a tuple $(\mu, \kappa, \alpha) \in [1, M] \times \mathbb{F}_q^* \times [1, N]$.

A trick of this protocol is the introduction of a technique to split the secret using $\mathcal{F}'$. If $k \in \mathbb{F}_q^*$ is one of the challenges chosen by the verifier V and $\boldsymbol{x}_\mu \in \mathbb{F}_q^n$ the secret corresponding to the challenge $\mu \in [1, M]$, then the element $k\boldsymbol{x}_\mu \in \mathbb{F}_q^n$ is divided into

$$k\boldsymbol{x}_\mu = \boldsymbol{s}_0 + \boldsymbol{u} \quad \text{where } \boldsymbol{s}_0, \boldsymbol{u} \in \mathbb{F}_q^n.$$

In a preprocessing phase, the prover P generates additive shares $\boldsymbol{u}_i \in \mathbb{F}_q^n$ and $\boldsymbol{v}_i \in \mathbb{F}_q^m$ for random $\boldsymbol{u} \in \mathbb{F}_q^n$ and $\mathcal{F}(\boldsymbol{u}) \in \mathbb{F}_q^m$ respectively. During protocol execution, P begins with $k\boldsymbol{x}_\mu - \boldsymbol{u}$ and locally computes $\mathcal{F}'(\boldsymbol{u}_i, \boldsymbol{s}_0) + \boldsymbol{v}_i$ which constitute shares of $\mathcal{F}(k\boldsymbol{x}_\mu) - \mathcal{F}(\boldsymbol{s}_0)$. These are recombined and V replaces $\mathcal{F}(k\boldsymbol{x}_\mu)$ with $k^2\boldsymbol{y}_\mu$ to check the knowledge of the secret by the prover P.

Regarding the security of MQBG, an analysis is provided in [3, Appendix G].

$\mathbf{Prover}((\boldsymbol{x}_i)_{i\in[1,M]}, \mathcal{F}, (\boldsymbol{y}_i)_{i\in[1,M]})$		$\mathbf{Verifier}(\mathcal{F}, (\boldsymbol{y}_i)_{i\in[1,M]})$
$\theta \xleftarrow{\$} \{0,1\}^\lambda$		
for $i \in [1, N-1]$ **do**		
$\theta_i \xleftarrow{\$,\theta} \{0,1\}^\lambda,\ \phi_i \xleftarrow{\$,\theta_i} \{0,1\}^\lambda$		
$\boldsymbol{u}_i \xleftarrow{\$,\phi_i} \mathbb{F}_q^n,\ \boldsymbol{v}_i \xleftarrow{\$,\phi_i} \mathbb{F}_q^m$		
$r_{1,i} \xleftarrow{\$,\theta_i} \{0,1\}^\lambda$		
$\mathsf{com}_{1,i} = \mathsf{Com}(r_{1,i}, \phi_i)$		
end		
$\theta_N \xleftarrow{\$,\theta} \{0,1\}^\lambda$		
$\phi_N \xleftarrow{\$,\theta_N} \{0,1\}^\lambda$		
$\boldsymbol{u}_N \xleftarrow{\$,\phi_N} \mathbb{F}_q^n$		
$\boldsymbol{u} = \sum_{i\in[1,N]} \boldsymbol{u}_i$		
$\boldsymbol{v}_N = \mathcal{F}(\boldsymbol{u}) - \sum_{i\in[1,N-1]} \boldsymbol{v}_i$		
$r_{1,N} \xleftarrow{\$,\theta_N} \{0,1\}^\lambda,\ \mathsf{com}_{1,N} = \mathsf{Com}(r_{1,N}, \boldsymbol{v}_N \,\|\, \phi_N)$		
$\mathsf{com}_1 = \mathsf{Hash}((\mathsf{com}_{1,i})_{i\in[1,N]})$		
	$\xrightarrow{\quad \mathsf{com}_1 \quad}$	
		$(\mu, \kappa) \xleftarrow{\$} [1, M] \times \mathbb{F}_q^*$
	$\xleftarrow{\quad \mu, \kappa \quad}$	
$\boldsymbol{s}_0 = \kappa \cdot \boldsymbol{x}_\mu - \boldsymbol{u}$		
for $i \in [1, N]$ **do**		
$\boldsymbol{s}_i = \mathcal{F}'(\boldsymbol{u}_i, \boldsymbol{s}_0) + \boldsymbol{v}_i$		
end		
$\mathsf{com}_2 = \mathsf{Hash}(\boldsymbol{s}_0 \,\|\, (\boldsymbol{s}_i)_{i\in[1,N]})$		
	$\xrightarrow{\quad \mathsf{com}_2 \quad}$	

Figure 1: The MQBG.

$\alpha \xleftarrow{\$} [1, N]$

α ⟵

$\boldsymbol{z}_1 = \kappa \cdot \boldsymbol{x}_\mu - \boldsymbol{u}$
if $\alpha \neq N$ **do**
  $z_2 = \boldsymbol{v}_N \,||\, (\theta_i)_{i \in [1,N] \setminus \alpha}$
else
  $z_2 = (\theta_i)_{i \in [1,N] \setminus \alpha}$
end
$\mathsf{rsp} = (\boldsymbol{z}_1, z_2, \mathsf{com}_{1,\alpha})$

⟶ rsp

Compute $(\bar{\phi}_i, \bar{r}_{1,i}, \bar{\boldsymbol{u}}_i, \bar{\boldsymbol{v}}_i)_{i \in [1,N] \setminus \alpha}$ from z_2
$\bar{\boldsymbol{s}}_0 = \boldsymbol{z}_1$
for $i \in [1, N] \setminus \alpha$ **do**
  $\bar{\boldsymbol{s}}_i = \mathcal{F}'(\bar{\boldsymbol{u}}_i, \bar{\boldsymbol{s}}_0) + \bar{\boldsymbol{v}}_i$
end
$\bar{\boldsymbol{s}}_\alpha = \kappa^2 \cdot \boldsymbol{y}_\mu - \mathcal{F}(\boldsymbol{z}_1) - \sum_{i \in [1,N] \setminus \alpha} \bar{\boldsymbol{s}}_i$,
$\bar{\mathsf{com}}_{1,\alpha} = \mathsf{com}_{1,\alpha}$
for $i \in [1, N] \setminus \alpha$ **do**
  if $i \neq N$ **do**
    $\bar{\mathsf{com}}_{1,i} = \mathsf{Com}\big(\bar{r}_{1,i},\, \bar{\phi}_i\big)$
  else
    $\bar{\mathsf{com}}_{1,N} = \mathsf{Com}\big(\bar{r}_{1,N},\, \bar{\boldsymbol{v}}_N \,||\, \bar{\phi}_N\big)$
  end
end
$b_1 \longleftarrow \big(\mathsf{com}_1 = \mathsf{Hash}\big((\mathsf{com}_{1,i})_{i \in [1,N]}\big)\big)$,
$b_2 \longleftarrow \big(\mathsf{com}_2 = \mathsf{Hash}\big(\boldsymbol{z}_1 \,||\, (\bar{\boldsymbol{s}}_i)_{i \in [1,N]}\big)\big)$
return $b_1 \wedge b_2$

Figure 1: (*Continued*)

3 Polynomial-time algorithm for solving the $\mathrm{DiffMQ}^{+}_{\mathrm{H}}$

In this section, we present a polynomial-time algorithm that solves the $\mathrm{DiffMQ}^{+}_{\mathrm{H}}$ with probability $O(1/q^{m-n})$. The main idea here is that the $\mathrm{DiffMQ}^{+}_{\mathrm{H}}$ can be reduced to the problem of finding a collision on the quadratic system $\mathcal{F} \in \mathrm{MQ}_{\mathrm{H}}(n, m, \mathbb{F}_q)$. Although the MQ_{H} is hard, the problem of finding a collision is much easier in the case of quadratic equations [17,18].

Theorem 3.1. *Let $\mathcal{F} \in \mathrm{MQ}_{\mathrm{H}}(n, m, \mathbb{F}_q)$, where m and n are positive integers. Then, there exists a probabilistic polynomial-time algorithm that solves the* $\mathrm{DiffMQ}^{+}_{\mathrm{H}}$ *with probability $O(1/q^{m-n})$.*

Proof. The idea is to consider the polar form $\mathcal{F}' : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q^m$ associated with $\mathcal{F}$ (see Definition 4). Therefore, this polar form is bilinear and equal to

$$\mathcal{F}'(\boldsymbol{x}, \boldsymbol{y}) = \mathcal{F}(\boldsymbol{x} + \boldsymbol{y}) - \mathcal{F}(\boldsymbol{x}) - \mathcal{F}(\boldsymbol{y}). \tag{5}$$

Let $(\boldsymbol{s}_1, \boldsymbol{v}_1), \ldots, (\boldsymbol{s}_M, \boldsymbol{v}_M) \in \mathbb{F}_q^n \times \mathbb{F}_q^m$ and $\mathcal{F}(\boldsymbol{s}_1) = \boldsymbol{v}_1, \ldots, \mathcal{F}(\boldsymbol{s}_M) = \boldsymbol{v}_M$ and $\kappa_1, \kappa_2 \in \mathbb{F}_q^*$. We present now an algorithm that recovers $(\boldsymbol{c}, \boldsymbol{d}_1, \boldsymbol{d}_2) \in \mathbb{F}_q^m \times \mathbb{F}_q^n \times \mathbb{F}_q^n$ such that

$$\mathcal{F}(\boldsymbol{d}_1) + \boldsymbol{c} = \kappa_1^2 \boldsymbol{v}_1 \quad \text{and} \quad \mathcal{F}(\boldsymbol{d}_2) + \boldsymbol{c} = \kappa_2^2 \boldsymbol{v}_2. \tag{6}$$

Note then that we restrict (3) to $\mu_1 = 1$ and $\mu_2 = 2$.

The algorithm has two main steps. First, we eliminate $\boldsymbol{c} \in \mathbb{F}_q^m$ and recover $(\boldsymbol{d}_1, \boldsymbol{d}_2) \in \mathbb{F}_q^n \times \mathbb{F}_q^n$ by solving a linear system. We then recover the $\boldsymbol{c} \in \mathbb{F}_q^n$ that fits the $(\boldsymbol{d}_1, \boldsymbol{d}_2)$ recovered in the first step.

Recovering $\boldsymbol{d}_1$ and $\boldsymbol{d}_2$ using the polar form

Let $\boldsymbol{\Delta}, \boldsymbol{d}_1 \in \mathbb{F}_q^n$ and set $\boldsymbol{d}_2 = \boldsymbol{d}_1 + \boldsymbol{\Delta} \in \mathbb{F}_q^n$. We consider the difference of the two equations of (6). This allows eliminating $\boldsymbol{c}$ and yields

$$\mathcal{F}(\boldsymbol{d}_1 + \Delta) - \mathcal{F}(\boldsymbol{d}_1) = \kappa_2^2 \boldsymbol{v}_2 - \kappa_1^2 \boldsymbol{v}_1.$$

From (5), we obtain that $\mathcal{F}(\boldsymbol{d}_1 + \Delta) - \mathcal{F}(\boldsymbol{d}_1)$

$$\mathcal{F}'(\boldsymbol{d}_1, \boldsymbol{\Delta}) + \mathcal{F}(\boldsymbol{\Delta}) = \kappa_2^2 \boldsymbol{v}_2 - \kappa_1^2 \boldsymbol{v}_1. \tag{7}$$

Recall that $\mathcal{F}'$ is bilinear. By randomly sampling $\boldsymbol{\Delta}$, we can recover $\boldsymbol{d}_1$ by solving a linear system of m equations in n variables. The success probability of this step is $1/q^{m-n}$. Remark that this step is independent from $\boldsymbol{c}$.

Recovering $\boldsymbol{c}$

Let $\boldsymbol{d}_1 \in \mathbb{F}_q^n$ be a solution of the linear system (7). From the very definition of a $\mathrm{DiffMQ}_{\mathrm{H}}^{+}$ solution and (6), we set $\boldsymbol{c}$ as

$$-\mathcal{F}(\boldsymbol{d}_1) + \kappa_1^2 \boldsymbol{v}_{\mu_1} \in \mathbb{F}_q^m. \tag{8}$$

Correctness of $\boldsymbol{d}_2$

It remains to show that $\boldsymbol{d}_2 = \boldsymbol{d}_1 + \boldsymbol{\Delta}$ found at the first step is correct, i.e.,

$$\mathcal{F}(\boldsymbol{d}_2) + \boldsymbol{c} = \kappa_2^2 \boldsymbol{v}_{\mu_2}.$$

By definition, we have

$$\begin{aligned} \mathcal{F}(\boldsymbol{d}_2) + \boldsymbol{c} &= \mathcal{F}(\boldsymbol{d}_1) + \mathcal{F}'(\boldsymbol{d}_1, \Delta) + \mathcal{F}(\Delta) + \boldsymbol{c} \\ &= \mathcal{F}(\boldsymbol{d}_1) + (\kappa_2^2 \boldsymbol{v}_{\mu_2} - \kappa_1^2 \boldsymbol{v}_{\mu_1}) + (-\mathcal{F}(\boldsymbol{d}_1) + \kappa_1^2 \boldsymbol{v}_{\mu_1}) \\ &= \kappa_2^2 \boldsymbol{v}_{\mu_2}. \end{aligned}$$

□

3.1 Experimental results

The following tests were run on a MacBook Air with Apple chip M_2, 8 GB, SSD 512 GB and using Magma V2.20-3 (STUDENT). For each n, 100 tests were run with a timeout of 24 h per test. We fix $n = m$, $q = 31$, $M = 2$, $\mu_1 = 1$, $\mu_2 = 2$, and k_1, k_2 are chosen randomly in $\mathbb{F}_q^*$.

n	Successful tests	Failed tests	Time to generate matrix (s)	Time to compute solution (s)	Time to verify (s)
10	99	1	0.420	0.001	0.000
15	95	5	3.165	0.002	0.000
20	98	2	13.839	0.009	0.001
25	97	3	44.607	0.017	0.002
30	94	6	118.949	0.028	0.004

The following tests were run with $m < n$, i.e. $m = n - 2$ and the same setting we used before:

n	m	Successful tests	Failed tests	Time to generate matrix (s)	Time to compute solution (s)	Time to verify (s)
10	8	100	0	0.269	0.001	0.000
15	13	100	0	2.344	0.002	0.001
20	18	100	0	11.222	0.009	0.001
25	23	100	0	37.736	0.016	0.002
30	28	100	0	103.552	0.029	0.002

From these tables, we can see that the polynomial-time algorithm that solves the $\mathrm{DiffMQ}_{\mathrm{H}}^{+}$ works very fast, in polynomial-time as we expected. There are some cases where the algorithm failed, but most of the time it succeeded especially when the number of equations is smaller than the number of variables. Hence, the above tests confirm our Theorem 1.1.

Acknowledgement: We thank Daniel Escudero and Javier Verbel for fruitful discussions. MV thanks Sorbonne University, CNRS, LIP6, PolSys, which hosted her in the Winter 2024 and the University of Salerno for their financial support. MV is a member of the “National Group for Algebraic and Geometric Structures, and their Applications” (GNSAGA - INdAM). The authors are grateful for the valuable comments of the reviewers that improved the manuscript. These results were presented in September 2024 at CIFRIS24, the Italian Congress of De Cifris (www.decifris.it/cifris24).

Funding information: MV received financial support from GNSAGA - INdAM. Funded by the European Union - Next Generation EU, Missione 4 Componente 1 CUP B53D23009410006, PRIN 2022- 2022PSTWLB - Group Theory and Applications. MV thanks the University of Salerno and Erasmus Traineeship grant for their financial support.

Author contributions: All authors have accepted responsibility for the entire content of this manuscript and consented to its submission to the journal, reviewed all results, and approved the final version of the manuscript.

Conflict of interest: The authors declare no conflict of interest.

Ethical approval: The research conducted is not related to human or animal use.

Data availability statement: Data sharing is not applicable to this article as no data sets were generated or analyzed during the current study.

References

[1] Bernstein D, Lange T. Post-quantum cryptography. Nature. 2017;549:188–94.

[2] Bidoux L, Gaborit P. Compact post-quantum signatures from proofs of knowledge leveraging structure for the sfPKP, sfSD and sfRSD problems. In: Hajji SE, Mesnager S, Souidi EM, editors. Codes, Cryptology and Information Security - 4th International Conference, C2SI 2023, Rabat, Morocco, May 29–31, 2023, Proceedings. vol. 13874 of Lecture Notes in Computer Science. Springer; 2023. p. 10–42. doi: 10.1007/978-3-031-33017-9_2.

[3] Bidoux L, Gaborit P. Shorter signatures from proofs of knowledge for the SD, MQ, PKP and RSD problems. In: arXiv Preprint; 2022. Initial version, April 2022, Creative Commons Attribution 4.0 International. https://arxiv.org/abs/2204.02915.

[4] Bellini E, Makarim RH, Sanna C, Verbel J. An estimator for the hardness of the MQ problem. IACR; 2022. Cryptology ePrint Archive, Paper 2022/708. https://eprint.iacr.org/2022/708.

[5] Bettale L, Kahrobaei D, Perret L, Verbel JA. Biscuit: new MPCitH signature scheme from structured multivariate polynomials. In: Pöpper C, Batina L, editors. Applied Cryptography and Network Security – 22nd International Conference, ACNS 2024, Abu Dhabi, United Arab Emirates, March 5–8, 2024, Proceedings, Part I. vol. 14583 of Lecture Notes in Computer Science. Springer; 2024. p. 457–86. doi: 10.1007/978-3-031-54770-6_18.

[6] Casanova A, Faugère J, Macario-Rat G, Patarin J, Perret L, Ryckeghem J. GeMSS: AGreat Multivariate Signature Scheme;. NIST round 3 post-quantum submission. Gaithersburg, Maryland, United States: National Institute of Standards and Technology (NIST).

[7] Kipnis A, Patarin J, Goubin L. Unbalanced oil and vinegar signature schemes. In: Stern J, editor. Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2–6, 1999, Proceedings. vol. 1592 of Lecture Notes in Computer Science. Springer; 1999. p. 206–22. doi: 10.1007/3-540-48910-X_15.

[8] Beullens W. MAYO: Practical post-quantum signatures from oil-and-vinegar maps. In: Aitawy R, Hülsing A, editors. Selected Areas in Cryptography - 28th International Conference, SAC 2021, Virtual Event, September 29–October 1, 2021, Revised Selected Papers. vol. 13203 of Lecture Notes in Computer Science. Springer; 2021. p. 355–76. doi: 10.1007/978-3-030-99277-4_17.

[9] Cayrel PL, Véron P, Alaoui SMEY. A zero-knowledge identification scheme based on the q-ary syndrome decoding problem. In: Biryukov A, Gong G, Stinson DR, editors. Selected Areas in Cryptography. vol. 6544 of Lecture Notes in Computer Science. Springer; 2010. p. 171–86. https://hal-univ-tln.archives-ouvertes.fr/hal-00674249/document.

[10] Stern J. A new paradigm for public key identification. IEEE Trans Inform Theory. 1996;42(6):1757–68. https://www.di.ens.fr/users/stern/data/St55b.pdf.

[11] Sakumoto K, Shirai T, Hiwatari H. Public-key identification schemes based on multivariate quadratic polynomials. In: Rogaway P, editor. Advances in Cryptology - CRYPTO 2011. vol. 6841 of Lecture Notes in Computer Science. Springer; 2011. p. 706–23. https://www.iacr.org/archive/crypto2011/68410703/68410703.pdf.

[12] Wang W. Shorter Signatures from MQ; 2022. https://eprint.iacr.org/2022/344. Cryptology ePrint Archive, Paper 2022/344.

[13] Beullens W. Sigma Protocols for MQ, PKP and SIS, and Fishy Signature Schemes; 2019. Cryptology ePrint Archive, Paper 2019/490. https://eprint.iacr.org/2019/490.

[14] Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems. In: Oswald E, Fischlin M, editors., Advances in Cryptology - EUROCRYPT 2015. Lecture Notes in Computer Science(), vol. 9057. Berlin, Heidelberg: Springer; 2015. https://doi.org/10.1007/978-3-662-46803-6_25

[15] Unruh D. Non-interactive zero-knowledge proofs in the quantum random oracle model. In: Theory of Cryptography, 12th Theory of Cryptography Conference (TCC 2015). Springer; 2015. p. 755–84.

[16] Yesina M, Shahov BS. Analysis and research of digital signature algorithm Picnic. Radiotekhnika. 2020;4(203):19–24. https://doi.org/10.30837/rt.2020.4.203.02.

[17] Bettale L, Faugère J, Perret L. Security analysis of multivariate polynomials for hashing. In: Yung M, Liu P, Lin D, editors. Information Security and Cryptology, 4th International Conference, Inscrypt 2008, Beijing, China, December 14–17, 2008, Revised Selected Papers. vol. 5487 of Lecture Notes in Computer Science. Springer; 2008. p. 115–24. doi: 10.1007/978-3-642-01440-6_11.

[18] Ding J, Yang B. Multivariate polynomials for hashing. In: Pei D, Yung M, Lin D, Wu C, editors. Information Security and Cryptology, Third SKLOIS Conference, Inscrypt 2007, Xining, China, August 31–September 5, 2007, Revised Selected Papers. vol. 4990 of Lecture Notes in Computer Science. Springer; 2007. p. 358–71. doi: 10.1007/978-3-540-79499-8_28.