International Journal of Mathematics and
Computer Science, **18**(2023), no. 3, 451–461

Novel Forgery Mechanisms in Multivariate Signature Schemes

Nurul Amiera Sakinah Abdul Jamal[1], **Muhammad Rezal Kamel Ariffin**[1,2], **Kamilah Abdullah**[1,3]

[1]Institute for Mathematical Research
Universiti Putra Malaysia
43400, Selangor, Malaysia

[2]Department of Mathematics
Faculty of Science
Universiti Putra Malaysia
43400, Selangor, Malaysia

[3]Department of Mathematics
Faculty of Computer and Mathematical Sciences
Universiti Teknologi MARA Shah Alam
40450 Shah Alam, Selangor, Malaysia

email: amierasakinah@gmail.com, rezal@upm.edu.my,
kamilah@tmsk.uitm.edu.my

(Received November 1, 2022, Revised December 12, 2022,
Accepted February 16, 2023, Published March 31, 2023)

Abstract

Multivariate cryptography is listed among the promising candidates for post-quantum cryptography primitives. Its hard problem depends on the difficulty of solving m multivariate quadratic equations in n variables over a finite field, hence the name Multivariate Quadratic Problem (MQP). In this paper, we present three multivariate digital signature forgery mechanisms by a rogue service provider. We also lay out techniques to identify two of such mechanisms. As for

Key words and phrases: Multivariate signature schemes, Multivariate Quadratic Problem, Underdetermined system, Rogue service provider, weak public key, post-quantum cryptography.
AMS (MOS) Subject Classifications: 94A60.
The corresponding author is Muhammad Rezal Kamel Ariffin.
ISSN 1814-0432, 2023, http://ijmcs.future-in-tech.net

a potential signature forgery mechanism via Greatest Common Divisors of evaluated polynomials in the system, it is still an open question on how to detect it. This third strategy seems to inherit the NP-hard difficulties of a random MQP in totality.

1 Introduction

The basic multivariate public key cryptosystem (MPKC) is built up from an invertible quadratic map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^m$ (central map) and two invertible affine (or linear) maps $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$. The *public key* is given by $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$ where $\mathcal{S}$, $\mathcal{F}$ and $\mathcal{T}$ are the *private keys*. The security of MPKC is based on the MQP which is proven to be NP-hard by Garey and Johnson [1]. MQP falls into three categories; underdetermined system ($m < n$), determined system ($m = n$), and overdetermined system ($m > n$). Undetermined system is applied in the digital signature schemes of multivariate cryptography. The most promising multivariate signature schemes are UOV [2] and Rainbow [3]. The existing algorithms to solve underdetermined system [2],[4],[5],[6],[7],[8],[9] have either narrow applicable range or exponential running-time. Therefore, this research provides two types of non-randomized MQP which are easy to solve and if the non-randomized systems satisfy $m < n$, forging a digital signature is possible.

Digital signature can be defined as a procedure which utilizes mathematics in order to authenticate digital documents as well as to provide message integrity. An adversary who wants to forge the signature must be able to produce a valid signature by manipulating the mathematical algorithms. In multivariate digital signature schemes, the hash value of the document d is computed such that $z = H(d)$ and is compared with the value of $P(\mathbf{s}) = z$ where $\mathbf{s}$ is the signature. If $z = z$, accept the signature, otherwise reject the signature. Therefore, the goal of an adversary is either to get the secret keys $\mathcal{S}, \mathcal{F}$ and $\mathcal{T}$, or to forge a valid signature $\mathbf{s}$ such that $P(\mathbf{s}) = z = z$.

In this work, we identify parameters provided by a rogue multivariate signature schemes service provider that will enable the service provider or third party to forge the signature of the owner of the parameters. In the first scenario, we show that the solution for a multivariate quadratic polynomial is also a solution for other multivariate quadratic polynomials in the same system $\mathcal{P}$ if every polynomials can be written as multiple of one of the polynomial i.e. $f_j(x) = kf_i(x)$. Then, we prove that the solution for a system $\mathcal{P}$ is also a solution for the summation of all the polynomials in $\mathcal{P}$. By manipulating these two properties, we put forward two potential mechanisms by a rogue service provider that enables them to forge signatures, and the techniques to identify the mechanisms. Next, we prove that for $i = 1, \ldots, m$, $f_i(\mathbf{x}) \equiv 0 (\text{mod } q)$ if and only if $q = \gcd(f_i(\mathbf{x}), f_j(\mathbf{x}))$ for $i \neq j$ $(i, j = 1, \ldots, m)$, there exist a mechanism by a rogue system provider that seems to inherit the NP-hard difficulties of a random MQP in totality. As such, with the current literature a client of the rogue service provider is unable to identify the weak system provided to him. Our mechanisms and attacks can actually be used for any class of multivariate quadratic polynomial systems. They are not restricted to the number of equations and variables.

The layout of the paper is structured as follows. In Section 2, we begin by introducing the mathematical notations used in MPKC and the standard process of encryption scheme and signature scheme. Then, we present our main results and we include relevant examples in Section 3. We discuss the time complexity in Section 4 and we briefly sum up our work in Section 5.

2 Preliminaries

In this section we provide some preliminaries for notations and cryptographic primitives in multivariate cryptography.

2.1 Matrix Representation

Quoting verbatim from [10], we define the matrix representation in multivariate cryptography as follows:

Definition 2.1. *(Multivariate Quadratic Polynomials.) Let $\mathbb{F} = \mathbb{F}_q$ be a finite field with q elements. We denote m as the number of equations and n as the number of variables. A system $\mathcal{P} = (p^{(1)}, \ldots, p^{(m)})$ of multivariate quadratic polynomials is defined as*

$$\begin{aligned} p^{(1)}(x_1, \ldots, x_n) &= \sum_{i=1}^{n} \sum_{j=1}^{n} p_{ij}^{(1)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)} \\ &\vdots \\ p^{(m)}(x_1, \ldots, x_n) &= \sum_{i=1}^{n} \sum_{j=1}^{n} p_{ij}^{(m)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)}. \end{aligned}$$

2.2 The Multivariate Quadratic Problem (MQP)

Quoting verbatim from [11], we define MQP as follows:

Definition 2.2. *Let $\mathbb{F} = \mathbb{F}_q$ be a finite field with q elements. Given a system $\mathcal{P} = (p^{(1)}(x), \dots, p^{(m)}(x))$ of m multivariate quadratic polynomials in n variables, find a vector $\mathbf{x} = (x_1, \dots, x_n)$ such that*

$$p^{(1)}(\mathbf{x}) = \dots = p^{(m)}(\mathbf{x}) = 0.$$

Garey and Johnson [1] has proved that MQP is NP-hard even for the quadratic polynomials over GF(2). More exactly, solving MQP is as hard as solving 3SAT problem since 3SAT problem can be reduced to MQP [12].

3 Novel Forgery Mechanisms for Multivariate Signature Schemes

In this section we present our main results.

3.1 MQP with the structure $f_j(x) = k_j f_1(x)$

We begin by presenting the first theorem which describes the relation of solution for multivariate quadratic polynomials that can be written into $f_j(x) = k_j f_1(x)$.

Theorem 3.1. *Let $\mathcal{P} = (f_1(x), \dots, f_m(x))$ be a system of m multivariate quadratic polynomials in n variables over $\mathbb{F}_q$. If $f_j(x)$ $(j = 2, \dots, m)$ can be written into $f_j(x) = k_j f_1(x)$ where $k_j \in \mathbb{F}_q$, then the solutions for $f_i(x) = 0$ for any $(i = 1, \dots, m)$ is also the solutions for $f_j(x) = 0$, for all $j \neq i$.*

Proof. Suppose $f_j(x)$ $(j = 2, \dots, m)$ can be written into $f_j(x) = k_j f_1(x)$

$$\begin{aligned} f_2(x) &= k_2 f_1(x) \\ &\vdots \\ f_m(x) &= k_m f_1(x) \end{aligned}$$

where $k_j \in \mathbb{Z}_q$ and suppose we have a solution set $\mathbf{x} = (x_1, \dots, x_m)$ such that $f_1(\mathbf{x}) = f_1(x_1, \dots, x_n) = 0$. Then,

$$\begin{aligned} f_2(\mathbf{x}) &= k_2 f_1(\mathbf{x}) = k_2(0) = 0 \\ &\vdots \\ f_m(\mathbf{x}) &= k_m f_1(\mathbf{x}) = k_m(0) = 0. \end{aligned}$$

Thus, if we can solve $f_i(x) = 0$ such that $f_i(\mathbf{x}) = 0$ we have also solved the whole system. □

Corollary 3.2. *Let $\mathcal{P} = (f_1(x), \ldots, f_m(x))$ be a system of m multivariate quadratic polynomials in n variables over $\mathbb{F}_q$ and $f_j(x)$ $(j = 2, \ldots, m)$ can be written into $f_j(x) = k_j f_1(x)$ where $k_j \in \mathbb{Z}_q$. Suppose for an arbitrary $\mathbf{x}$, $f_1(\mathbf{x}) = z_1$ then for $k_j(i = 2, \ldots, m) \in \mathbb{Z}_q$,*

$$\begin{aligned} f_2(\mathbf{x}) &= z_2 = k_2 z_1 \\ &\vdots \\ f_m(\mathbf{x}) &= z_m = k_m z_1. \end{aligned}$$

Based on Corollary 1, it is easy to find $\mathbf{s}' \neq \mathbf{s}$ such that $\mathcal{P}(\mathbf{s}') = z'$ and $z' = z$.

3.1.1 Digital Signature Forgery Mechanism 1

The system $\mathcal{P}$ of which its polynomials can be written as $f_j = k_j f_1$ is constructed by choosing two random invertible affine maps $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$. Next, choose a central map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^m$ of which its polynomials can also be written as $f_j = k_j f_1$. All maps $\mathcal{S}$, $\mathcal{T}$ and $\mathcal{F}$ are kept secret. Then, compute $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$.

We note here that, as the modulus q gets larger, the published system $\mathcal{P}$ seems randomized. That is, the constants of the equations seem not to relate to one another and to identify whether there exists the relation $f_j(x) = k_j f_1(x)$, without a proper algorithm the complexity is $O(q)$. Nevertheless, from Theorem 1 if we can solve $f_i(x) = 0$ then, we also solve the whole system.

3.1.2 Identifying digital signature forgery from Mechanism 1

From Theorem 1 and Corollary 1, we now put forward an algorithm to identify a system that will allow digital signature forgery to occur from Mechanism 1.

Algorithm 1 Identifying digital signature forgery from Mechanism 1

Input: The system $\mathcal{P} = (f_1(x), \ldots, f_m(x))$ of multivariate quadratic polynomials over $\mathbb{F}_q$

Output: $\mathcal{P}$ is a forgeable system

```
1. for $j = 2$ to $m$ do
2.     $k_j = c_{f_j} \cdot c_{f_1}^{-1} \bmod q$ where $c_{f_j}$ and $c_{f_1}$ are the coefficients of polynomial $f_j(x)$ and $f_1(x)$ respectively.
3.     If $f_j(x) = k_j f_1(x)$, then $\mathcal{P}$ is a forgeable system.
4. end for
5. else $\mathcal{P}$ is not a forgeable system.
6. return
```

For discussion on the complexity of Algorithm 1, refer to Section 4 in this article.

3.2 MQP with the structure $f_j(x) = f_i(x) + f_h(x)$

The lemma below describes the relation of solution for multivariate quadratic polynomials that can be written into $f_j = f_i(x) + f_h(x)$.

Lemma 3.3. *Let $\mathcal{P} = (f_1(x), \ldots, f_m(x))$ be a system of m multivariate quadratic polynomials in n variables over $\mathbb{F}_q$. Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ be the solution of each $f_i(x)$ $(i = 1, \ldots, m)$ such that $f_1(\mathbf{x}) = \ldots = f_m(\mathbf{x}) = 0$. Set $f_h(x) = f_1(x) + f_2(x) + \ldots + f_m(x)$ over $\mathbb{F}_q$. Then $f_h(\mathbf{x}) = 0$.*

Proof.

$$\begin{aligned} f_h(\mathbf{x}) &= (f_1 + f_2 + \ldots + f_m)(\mathbf{x}) \\ &= f_1(\mathbf{x}) + f_2(\mathbf{x}) + \ldots + f_m(\mathbf{x}) \\ &= 0 + 0 + \ldots + 0 = 0. \end{aligned}$$

□

3.2.1 Digital Signature Forgery Mechanism 2

The system $\mathcal{P}$ of which its polynomials can be written as $f_j = f_i(x) + f_h(x)$ is constructed by choosing two invertible affine maps $\mathcal{S} : \mathbb{F}^2 \rightarrow \mathbb{F}^2$ and

$\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$, and a central map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^2$. All maps $\mathcal{S}$, $\mathcal{T}$ and $\mathcal{F}$ are kept secret. Then, compute $\mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$ to output two equations $f_1(x)$ and $f_2(x)$. For $f_j(x)$ $(j = 3, \dots, m)$, set $f_j(x) = f_i(x) + f_h(x)$ where $i = 1, \dots, j-1$ and $h = 1, \dots, j-1$. Publish $\mathcal{P} = (f_1(x), \dots, f_m(x))$ as public key over $\mathbb{F}_q$.

We note here that, the published system $\mathcal{P}$ seems randomized. That is, the constants of the equations seem not to relate to one another and to identify whether there exists the relation $f_j(x) = f_i(x) + f_h(x)$, without a proper algorithm the complexity is the same complexity as solving MQP which is NP-hard. Nevertheless, from Lemma 1 if we can solve $f_1(x) = 0$ and $f_2(x) = 0$ then, we also solve $f_j(x) = 0$ i.e. $f_1(\mathbf{x}) = f_2(\mathbf{x}) = 0$ and $f_j(\mathbf{x}) = 0$ for $j = 3, \dots, m$.

3.2.2 Identifying digital signature forgery from Mechanism 2

We now put forward from Lemma 1 an algorithm to identify a system that will allow digital signature forgery to occur from Mechanism 2.

Algorithm 2 Identifying digital signature forgery from Mechanism 2

Input: The system $\mathcal{P} = (f_1(x), \dots, f_m(x))$ of multivariate quadratic polynomials over $\mathbb{F}_q$

Output: $\mathcal{P}$ is a forgeable system

```
for $j = 3$ to $m$ do
    for $i = 1$ to $j - 1$ do
        for $h = i$ to $j - 1$ do
            $f_i(x) + f_h(x)$
            If $f_j(x) = f_i(x) + f_h(x)$, then $\mathcal{P}$ is a forgeable system.
        end for
    end for
end for
else $\mathcal{P}$ is not a forgeable system.
return
```

For discussion on the complexity of Algorithm 2, refer to Section 4 in this article.

3.3 Greatest Common Divisor-Based Digital Signature Forgery Mechanism

The theorem below describes the relation between a set of polynomials and its Greatest Common Divisors (GCD).

Theorem 3.4. *Let $\mathcal{P} = (f_1(x), \ldots, f_m(x))$ be a system of m multivariate quadratic polynomials in n variables over $\mathbb{F}_q$. Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ where at least one of x_i is not zero. For all $i \neq j(i, j = 1, \ldots, m)$, if*

$$\gcd(f_i(\mathbf{x}), f_j(\mathbf{x})) = q \text{ then } f_1(\mathbf{x}) = \ldots = f_m(\mathbf{x}) = 0.$$

Proof. Since at least one of x_i is not zero, then $f(\mathbf{x}) \geq x_i > 0$. So, $f(\mathbf{x}) = 0$ prior to modular reduction is not possible. From textbook congruence relation definition, $f(\mathbf{x}) = a + kq$, the integer k corresponds to the modular reduction value. When $k = 0$ corresponds to no modular reduction upon the value of $f(\mathbf{x})$ while when $k > 0$ corresponds to the modular reduction upon the value of $f(\mathbf{x})$.

If $\gcd(f_i(\mathbf{x}), f_j(\mathbf{x})) = q$, then

$$\begin{gathered} f_1(\mathbf{x}) = k_1 q \\ \vdots \\ f_m(\mathbf{x}) = k_m q. \end{gathered}$$

This implies $f_i(\mathbf{x}) \equiv 0 (\text{mod } q)$ for all $i = 1, \ldots, m$. □

3.3.1 Digital Signature Forgery Mechanism 3

We present an algorithm to construct a system that will allow digital signature forgery to occur based on Theorem 2, which outputs system $\mathcal{P}$ which seems to follow the hardness definition of MQP in totality.

Algorithm 3 The GCD-Based Forgeable Signature Schemes Parameters Generation

Input: The system $\mathcal{P} = (f_1(x), \ldots, f_m(x))$ of multivariate quadratic polynomials over integers and $\mathbf{x} = (x_1, \ldots, x_n)$
Output: The system $\mathcal{P} = (f_1(x), \ldots, f_m(x))$ of multivariate quadratic polynomials over $\mathbb{F}_q$ such that $f_1(\mathbf{x}) = \ldots = f_m(\mathbf{x}) = 0$

```
1. repeat
2.     Substitute $\mathbf{x} = (x_1, \ldots, x_n)$ into $f_1(x), \ldots, f_m(x)$.
3.     Compute the GCD of $f_i(\mathbf{x}) \in \mathbb{Z}$ for $i = 1, \ldots, m$.
4.     Set the GCD as $q$.
5. until $q$ is greater than every constants of each terms in $f_i(x)$ $(i = 1, \ldots, m)$
6. return $q$ and $\mathcal{P}$
```

4 Time Complexity for Algorithms 1 and 2

For Algorithm 1, the complexity is given by $O(m)$ where m is the number of equations. This is because, one only needs to execute Algorithm 1 for the first constant only. As for Algorithm 2, the complexity is given by $O(m^3)$ where m is the number of equations, This is due to steps $1-3$ in Algorithm 2.

For a practical multivariate signature scheme, the number of equations in the system must be of polynomial size. As such, $O(m)$ and $O(m^3)$ is of polynomial running time.

5 Conclusion

In conclusion, we have put forward three strategies of potential digital signature forgery mechanisms by rogue service provider. For digital signature forgery mechanism 1 and 2, we have identified strategies to identify whether the provided parameters will allow digital signature forgery to occur. However, for forgery mechanism 3 it is still an open question on how to identify it. This discussion shows empirical evidence that rogue multivariate signature schemes service provider has the potential to be a rogue service provider via mechanism 3. That is, we have identified a mechanism where an unknowingly trusting client does not have the means within the current literature to do due diligence to examine the parameters provided to him by the rogue service provider. We have proven that the rogue service provider can forge the signature of its clients. Finally, we point out that the complexity of Algorithm 1 is better than the complexity of Algorithm 2 in terms of identifying a forgeable system.

Acknowledgment. The research was supported by Ministry of Education of Malaysia with Fundamental Research Grant Scheme (FRGS/1/2019/STG06/UPM/02/8).

References

[1] Michael R. Garey, David S. Johnson, Computers and intractability: a guide to the theory of NP-hardness, (1979).

[2] Aviad Kipnis, Jacques Patarin, Louis Goubin, Unbalanced oil and vinegar signature schemes, International Conference on the Theory and Applications of Cryptographic Techniques, Springer, Berlin, Heidelberg, (1999), 206–222.

[3] Jintai Ding, Dieter Schmidt, Rainbow, a new multivariable polynomial signature scheme, International conference on applied cryptography and network security, Springer, Berlin, Heidelberg, (2005), 164–175.

[4] Nicolas Courtois, Louis Goubin, Willi Meier, Jean-Daniel Tacier, Solving underdefined systems of multivariate quadratic equations, International Workshop on Public Key Cryptography, Springer, Berlin, Heidelberg, (2002), 211–227.

[5] Yasufumi Hashimoto, Algorithms to solve massively under-defined systems of multivariate quadratic equations, IEICE transactions on fundamentals of electronics, communications and computer sciences, **94**, no. 6, (2011), 1257–1262.

[6] Enrico Thomae, Christopher Wolf, Solving underdetermined systems of multivariate quadratic equations revisited, International Workshop on Public Key Cryptography, Springer, Berlin, Heidelberg, (2012), 156–171.

[7] Hiroyuki Miura, Yasufumi Hashimoto, Tsuyoshi Takagi, Extended algorithm for solving underdefined multivariate quadratic equations, International Workshop on Post-Quantum Cryptography, Springer, Berlin, Heidelberg, (2013), 118–135.

[8] Chen-Mou Cheng, Yasufumi Hashimoto, Hiroyuki Miura, Tsuyoshi Takagi, A polynomial-time algorithm for solving a class of underdetermined multivariate quadratic equations over fields of odd characteristics, International Workshop on Post-Quantum Cryptography, Springer, Cham, (2014), 40–58.

[9] Heliang Huang, Wansu Bao, Algorithm for Solving Massively Underdefined Systems of Multivariate Quadratic Equations over Finite Fields, arXiv preprint arXiv:1507.03674, (2015).

[10] Jintai Ding, Albrecht Petzoldt, Dieter S. Schmidt, Multivariate Cryptography, Multivariate Public Key Cryptosystems, Springer, New York, NY, (2020), 7–23.

[11] Jintai Ding, Albrecht Petzoldt, Current state of multivariate cryptography, IEEE Security & Privacy, **15**, no. 4, (2017), 28–36.

[12] Jacques Patarin, Louis Goubin, Trapdoor one-way permutations and multivariate polynomials, International conference on information and communications security, Springer, Berlin, Heidelberg, (1997), 356–368.