SEMARAK ILMU PUBLISHING

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Novel Weakness Multivariate Quadratic Structures Detected within Macaulay Matrix

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

[1] Institute for Mathematical Research, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia
[2] Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia
[3] College of Computing, Informatics and Mathematics, Al-Khawarizmi Building, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia

ARTICLE INFO

Article history:
Received 25 September 2023
Received in revised form 19 February 2024
Accepted 15 June 2024
Available online 31 July 2024

Keywords:
Multivariate Public-Key Cryptosystem; Multivariate Quadratic problem; Macaulay matrix; Gaussian elimination

ABSTRACT

The security of a Multivariate Public-Key Cryptosystem (MPKC) is based on the hard mathematical problem of solving Multivariate Quadratic (MQ) equations over finite fields, also known as the MQ problem. An MPKC has the potential to be a post-quantum cryptosystem. In this paper, we identify new weaknesses in the Macaulay matrix identified via Wang's technique, which was initially designed for solving multivariate quadratic equation systems. This new weakness occurs in the case of random coefficients in any column vector for different variables of monomials and random coefficients are assigned to other monomials. The weakness is exposed through the use of Gaussian elimination to obtain a univariate equation. We illustrate our findings using a random example.

1. Introduction

Cryptography stands as a vital element of computer and network security, guaranteeing the confidentiality and integrity of data while shielding it from unauthorized intrusion. Furthermore, there has been a heightened public demand for cryptographic systems, particularly driven by the extensive utilization of e-commerce in the digital economy, including Internet banking, shopping, and payments. Cryptographic techniques hold the utmost importance in ensuring secure communication within contemporary society [1,2]. Currently, these techniques rely on number theoretic problems like factoring large integers and solving discrete logarithms. However, the emergence of quantum computers threatens the security of widely used encryption methods such as RSA [3], and ECC. Shor's polynomial time quantum algorithm poses a threat as it can efficiently solve these problems [4]. In the field of quantum cryptography, a cryptographic algorithm exhibits security against attacks from both quantum and classical computers [5].

In response to the vulnerability introduced by quantum computers, researchers are actively investigating novel public key systems with the capacity to withstand potential attacks. Among these

* *Corresponding author.*
E-mail address: rezal@upm.edu.my

https://doi.org/10.37934/araset.49.2.149159

systems, the multivariate public key cryptosystem (MPKC) has gained prominence. This system employs multivariate polynomials and stands as a post-quantum cryptography solution [6].

The fundamental structure of the MPKC consists of components: an invertible quadratic map denoted as $\mathcal{F}: \mathbb{F}^n \to \mathbb{F}^m$ (the central map), and two invertible affine (or linear) maps referred to $\mathcal{S}: \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{T}: \mathbb{F}^n \to \mathbb{F}^n$. In this system, the public key is represented as $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$ with $\mathcal{S}, \mathcal{F}$ and $\mathcal{T}$ are the private keys [7,8]. The security of MPKC relies on solving systems of multivariate quadratic (MQ) polynomial equations over finite fields, known as the MQ problem, and is an NP-hard problem [9]. The MQ problem involves with the identification of a candidate vector $\mathbf{x} = (x_1, \cdots, x_n)$ for which the system of polynomials satisfies the condition $\mathcal{P}(\mathbf{x}) = 0$ [10,11]. The challenge to identify the candidate vector $\mathbf{x}$, does not imply that the vector $\mathbf{x}$ is unique. Rather, it implies the task of determining a candidate vector $\mathbf{x}$ is NP-hard.

As indicated in [9], the initial multivariate public key scheme was introduced by Ong, Schnorr, and Shamir in 1984 [12], yet its security was compromised within a year [13]. Subsequent improved versions faced a similar fate and were subsequently broken [14]. Fell and Diffie [15] introduced the first scheme utilizing multiple polynomials, but they acknowledged its insecurity for practical key sizes. In 1985, Imai and Matsumoto [16] presented a distinct trapdoor approach, considered the first modern MQ scheme. This foundational concept was further refined in 1988 [17] and led to the development of several related schemes. However, numerous security claims were found to be erroneous, leading to ongoing competition between scheme cryptographers and cryptanalysts. Numerous schemes were proposed, but most of them were broken within a few years, leading to the gradual damaging of the reputation of MQ schemes over time.

Recent studies show that the Multivariate Quadratic (MQ) system is the foundation of all multivariate cryptosystems. Other well-established multivariate cryptosystems, such as C^* [18], HFE [19-21], UOV [22], SFLASH [23], TT cryptosystem (TTM) [24], Tame-like Multivariate Cryptosystem (TTS) [25], TRMC [26], TRMS [27], and Rainbow [28], also depend on the MQ problem. These systems use trapdoor transformations, which are multivariate quadratic polynomial maps with specific properties enabling the computational feasibility of finding their inverse maps.

During the Post-Quantum Cryptography 2013 conference, Tao *et al.* introduced a novel encryption scheme known as SimpleMatrix encryption scheme [29]. This cryptographic scheme not only demonstrates efficiency but also exhibits resilience against well-known attacks targeting multivariate cryptosystems. However, the SimpleMatrix scheme has an issue of decryption failures with non-negligible probability. Various papers, including [30,31], have proposed solutions to minimize the probability of decryption failures occurring, but a comprehensive solution is still lacking. Moreover, the approach outlined in [32] results in increased key and ciphertext sizes for the SimpleMatrix scheme. Subsequently, the previous study of [33] enhanced the Simple Matrix scheme by introducing new techniques and improvements. Continuing this, another version of SimpleMatrix encryption scheme is proposed in a previous study [34] to eliminate the decryption failure.

In summary, the emergence of quantum computers poses a challenge to cryptographic techniques, prompting the exploration of solutions like MPKC in the realm of post-quantum cryptography. While the SimpleMatrix encryption scheme holds promise, its decryption failure issues require resolution. Various proposals have been presented to mitigate these failures, although a comprehensive solution is yet to be achieved, and some proposed strategies increase the size of keys and ciphertexts.

Contribution. The one-step Gaussian elimination method, which is based on principles from linear algebra, is proposed in this study. We also provide a numerical example of how to solve the polynomial system $p_1(\mathbf{x}) = \cdots = p_m(\mathbf{x}) = 0$ which would be to find the possible solutions for $\mathbf{x} = (x_1, \ldots, x_n)$. This study is distinct from past studies in two ways.:

i. The one-step Gaussian elimination method provides an alternative method for identifying the solutions of the candidates.
ii. The techniques for structuring manipulation of the Macaulay matrix.

The remaining sections are arranged as follows: Section 2 provides a preliminary study on Multivariate Quadratic Polynomials, while Section 3 presents the General Workflow of the Multivariate Cryptography Scheme. Section 4 describes the Novel Weakness of Macaulay Matrix Structures, followed by Section 5 illustrating an example of the weak Macaulay structure of the public system $\mathcal{P}$. Finally, conclusions are drawn in Section 6.

2. Preliminaries on Multivariate Quadratic Polynomials

This section reviews the basic terminology and cryptographic primitives that are utilized in multivariate cryptography.

2.1 Matrix Representation

In multivariate cryptography, the matrix representation is defined as follows:

Definition 1. (*Multivariate Quadratic Polynomial*) [34]
Let $\mathbb{F}_q$ be a finite field with q elements. We denote m as the number of equations and n as the number of variables. A system $\mathcal{P} = (p_1, \dots, p_m)$ of multivariate quadratic polynomials is defined as

$$p_1(x_1, \dots, x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} t_{ij}^{(1)} \cdot x_i x_j + \sum_{i=1}^{n} t_i^{(1)} \cdot x_i + t_0^{(1)}$$
$$p_2(x_1, \dots, x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} t_{ij}^{(2)} \cdot x_i x_j + \sum_{i=1}^{n} t_i^{(2)} \cdot x_i + t_0^{(2)}$$
$$\vdots$$
$$p_m(x_1, \dots, x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} t_{ij}^{(m)} \cdot x_i x_j + \sum_{i=1}^{n} t_i^{(m)} \cdot x_i + t_0^{(m)}$$

Definition 2. *Let $\mathcal{P}\left(p_1(\mathbf{x}), \dots, p_m(\mathbf{x})\right)$ be a system of multivariate quadratic polynomials and $p_i(\mathbf{x}) = p_i(x_1, \dots, x_n)$ for $i = 1, 2, \dots, m$.*

*(a) The **lexicographical ordering** of monomials is a defined arrangement based on the order in which the monomials (excluding the coefficient) would be positioned as words in an alphabet with letters $x_1, x_2, \dots, x_n$* [35].
*(b) The **chosen lexicographical ordering** of monomials is a well-defined arrangement in which the priority of solving a variable is applied to monomials listed from two variables to one variable.*

Throughout this research, the public system of polynomials will undergo transformation into the Macaulay matrix following Definition 2(b), and the resulting matrix will be solved using Gaussian elimination.

The priority of solving a variable is demonstrated by the chosen lexicographical ordering of monomials. For illustrative purposes, let us consider the elimination of x_3 as the initial step. It is

feasible to derive a univariate polynomial in terms of x_3 ensuring that its degree does not exceed d. The univariate polynomial over the finite field is then solved. Thus, the potential value(s) of x_3 are discovered. To achieve this objective, we will proceed by substituting x_3 resulting in the polynomials with a reduced number of variables.

Definition 3. *(Multivariate Quadratic Problem)* [34]
Consider a system $\mathcal{P}(p_1(\mathbf{x}), \dots, p_m(\mathbf{x}))$ of m multivariate quadratic polynomials in n variables over a finite field $\mathbb{F}_q$ with q elements. The objective is to find a vector $\mathbf{x} = (x_1, \dots, x_n)$ that satisfies the condition

$$p_1(\mathbf{x}) = \cdots = p_m(\mathbf{x}) = 0.$$

Theorem 1. [34] *Let $\mathbb{F} = \mathbb{F}_q$ be a finite field with q elements and degree d less than q. Then, there exist $\binom{n+d-1}{d}$ monomials of degree d in $\mathbb{F}(x_1, \dots, x_n)$. Then, the number of monomials of degree less than or equal to d in $\mathbb{F}(x_1, \dots, x_n)$ is given by $\binom{n+d}{d}$.*

Proof.
1. The number of monomials of degree d is obtained by choosing d out of n element of $x_1, \dots, x_n$ with repetition.
2. The elements in the polynomial of degree less than or equal d are elements from the set $\{x_1, \dots, x_n, 1\}$ with repetition.

□

Theorem 2. *The number of monomials with degrees less than or equal to d in $\mathbb{F}_q$ with q elements is given by $\binom{n+d}{d}$. The number of monomials with degree d with distinct variables is given by $\binom{n}{d}$.*

Proof.
1. The total number of monomials with degree less than or equal to d is determined by n elements from the set $\{x_1, .., x_n, 1\}$, with repetition.
2. The total number of monomials with degree less than or equal to d is determined by n elements from the set $\{x_1, \dots, x_n, 1\}$, without repetition.

□

A system of MQ polynomial equations is solved through the transformation of the polynomials into a Macaulay matrix, denoted as matrix M, which is constructed from equations $(p_1(\mathbf{x}), \dots, p_m(\mathbf{x})) = 0$ (Definition 3) and subsequently reduced using the Gaussian elimination procedure. The number of column vectors in the Macaulay matrix M is equivalent to the number of monomials with a degree less than or equal to d, which is $\binom{n+d}{d}$.

Following is the definition of the Macaulay matrix M of degree d corresponding to $\mathcal{P}(\mathbf{x}) = p_1(\mathbf{x}), \dots, p_m(\mathbf{x})$.

Definition 4. *(Macaulay Matrix) The coefficient vectors of the polynomial $p_i(\mathbf{x})$ where $i = 1, 2, \dots, m$ are arranged as the rows of the Macaulay matrix, $M \in \mathbb{F}^{m \times n}$ of degree d, and $e = \binom{n+d}{d}$ is the number of monomials. The matrix M is defined as*

$$M = \begin{bmatrix} p_1(\mathbf{x}) \\ p_2(\mathbf{x}) \\ \vdots \\ p_m(\mathbf{x}) \end{bmatrix} = \begin{bmatrix} c_{1(1)} & c_{1(2)} & \cdots & c_{1(e)} \\ c_{2(1)} & c_{2(2)} & \cdots & c_{2(e)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m(1)} & c_{m(2)} & \cdots & c_{m(e)} \end{bmatrix},$$

where every polynomial $p_i(x_1, \ldots, x_n)$ *for* $i = 1, \ldots, m$.

3. General Workflow of Multivariate Cryptography Scheme [34]

A multivariate public key cryptosystem based on the MQP is constructed from an invertible quadratic map $\mathcal{F}: \mathbb{F}^n \to \mathbb{F}^m$ 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 in the form of $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$ where $\mathcal{S}, \mathcal{F}$ and $\mathcal{T}$ are the private keys.

3.1 Encryption Scheme ($m \geq n$)

Encryption: To encrypt a message $\mathbf{x} \in \mathbb{F}^n$, one simply computes $\mathcal{P}(\mathbf{x}) = \mathbf{z}$.

$$\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}(\mathbf{x})$$
$$\mathbf{w} = \mathcal{T}(\mathbf{x})$$
$$\mathbf{y} = \mathcal{F}(\mathbf{w})$$
$$\mathbf{z} = \mathcal{T}(\mathbf{y})$$

The ciphertext of the message $\mathbf{x}$ is $\mathbf{z} \in \mathbb{F}^m$.

Decryption: The decryption of the ciphertext $\mathbf{z} \in \mathbb{F}^m$, by computes $\mathcal{P}^{-1} = \mathbf{x}$ recursively.

$$\mathbf{y} = \mathcal{S}^{-1}(\mathbf{z})$$
$$\mathbf{w} = \mathcal{F}^{-1}(\mathbf{y})$$
$$\mathbf{x} = \mathcal{T}^{-1}(\mathbf{w})$$

Thus, $\mathbf{x} \in \mathbb{F}^n$ is the plaintext corresponding to the ciphertext $\mathbf{z}$.

Proof of correctness:

$$\begin{aligned} \mathcal{T}^{-1} \circ \mathcal{F}^{-1} \circ \mathcal{S}^{-1}(\mathbf{z}) &= \mathcal{T}^{-1}\left(\mathcal{F}^{-1}\left(\mathcal{S}^{-1}(\mathbf{z})\right)\right) \\ &= \mathcal{T}^{-1}\left(\mathcal{F}^{-1}(\mathbf{y})\right) \\ &= \mathcal{T}^{-1}(\mathbf{w}) \\ &= \mathbf{x} \end{aligned}$$

3.2 Standard Attacks

Two common types of standard attacks employed against multivariate public key schemes are:

i. **Direct Attack**: This kind of attack concentrates on solving the public equation $\mathcal{P}(\mathbf{x}) = \mathbf{z}$ as an n instance of the MQP directly. The examples of direct attack are F4 algorithm [36, 37] and XL algorithm [38,39].
ii. **Structural Attack**: A structural attack requires the unique structure of the central map of a multivariate cryptography scheme to endeavour to recover the private key. For example, Linearization equation attack, MinRank attack and Differential attack.

4. Novel Weakness Macaulay Matrix Structures

In this section, we present our main results.

4.1 Utilizing Wang's Workflow

The following Algorithm 1 is a partial work-flow of Wang's methodology in [38].

Algorithm 1: Solving the Multivariate Quadratic polynomials

Input: The coefficients of public system $\boldsymbol{\mathcal{P}}$, a finite field $\mathbb{F}_{\boldsymbol{q}}$, $\boldsymbol{m}$ quadratic polynomials $\boldsymbol{\mathcal{P}} = \left(\boldsymbol{p_1}(\mathrm{x}), \dots, \boldsymbol{p_m}(\mathrm{x})\right)$ and $\boldsymbol{n}$ variables of $(\boldsymbol{x_1}, \dots, \boldsymbol{x_n})$.

Output: The solution to the system of equations represented by $\boldsymbol{p_1}(\mathrm{x}) = \cdots = \boldsymbol{p_m}(\mathrm{x}) = \boldsymbol{0}$ in $\mathbb{F}_{\boldsymbol{q}}$.

1. **Linearize**: In the chosen-lexicographical ordering sequence (as defined in Definition 2 b)) the monomials of polynomial $\boldsymbol{\mathcal{P}}$ are arranged, starting from monomials involving variables $\boldsymbol{x_i x_j}$ and the single variables $\boldsymbol{x_i}$. The elimination process proceeds with the monomials containing single variables $\boldsymbol{x_i}$ being eliminated last.
2. **Organize:** Generate the Macaulay matrix $\boldsymbol{M}$ using Definition 4 as the basis.
3. **Solve:** Apply Gaussian elimination to the matrix $\boldsymbol{M}$ representing the system of polynomials. During this process, assume that the last non-zero row corresponds to a univariate polynomial equation involving a variable $\boldsymbol{x_n}$. After this elimination phase, determine the root of the obtained univariate equation within the underlying finite field.
4. **Repeat:** Perform substitution of the value obtained in Step 3 into the system $\boldsymbol{\mathcal{P}}$ to simplify the equations. Proceed with the iterative process to solve for the remaining variables.

As a result, when employing Algorithm 1, the monomials are arranged in accordance with Definition 2 b), which causes the single variable to be eliminated last. This arrangement can reduce the iteration of the Gauss elimination process to obtain the last non-zero row of the univariate equation.

4.2 Wang's Strategy for Solving the Macaulay Matrix

Our analysis of the Macaulay matrix's structure follows Wang's method [38], which rearranges the monomials with two variables, $\{x_i x_j\}$ as $i, j = 1, 2, \dots, n$ to benefit Gaussian elimination. The method assigned the power of a variable should be eliminated last according to the monomials' specified order. Instead of making random arrangements of the system, using Wang's approach, consumes less time to solve the system. This study is extension from [40] which applies Wang's strategy.

4.3 Exposing Macaulay Matrix Weak Structures

Breaking the MQ polynomial involves obtaining potential values for the plaintext from the provided public system $\mathcal{P}$ and the ciphertext $\boldsymbol{z}$. This task is an NP-hard problem [9].

Suppose Wang's technique [38] outputs the following Macaulay matrix structure. Set any column vector of $\binom{n}{d}$ with random coefficients for two different variables of degree 2 (i.e. monomial $\{x_i x_j\}$) and denote the column vectors of $\binom{n+d}{d} - \binom{n}{d}$ as R where each entry represents a random coefficient less than q, then the Macaulay matrix M can be redefined as follows:

$$M = \begin{array}{c} \begin{matrix} x_1x_2 & x_1x_3 & \cdots & x_ix_j & x_1^2 & x_1 & \cdots & x_n^2 & x_n & 1 \end{matrix} \\ \begin{bmatrix} * & * & \cdots & * & R & R & \cdots & R & R & R \\ * & * & \cdots & * & R & R & \cdots & R & R & R \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ * & * & \cdots & * & R & R & \cdots & R & R & R \end{bmatrix} \end{array}$$

x_kx_l

Our analysis focuses on the structure of $\{x_kx_l\}$ where $k = 1, 2, 3, \ldots, i$ and $l = 1, 2, 3, \ldots, j$, which can be represented as follows:

(i) $\begin{matrix} x_1x_2 & x_1x_3 & \cdots & x_ix_j \end{matrix}$
$\begin{bmatrix} R & 0 & \cdots & 0 \\ R & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ R & 0 & \cdots & 0 \end{bmatrix}$

Or (ii) $\begin{matrix} x_1x_2 & x_1x_3 & \cdots & x_{n-i}x_{n-j} & \cdots & x_ix_j \end{matrix}$
$\begin{bmatrix} 0 & 0 & \cdots & R & \cdots & 0 \\ 0 & 0 & \cdots & R & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & R & \cdots & 0 \end{bmatrix}$

Or (iii) $\begin{matrix} x_1x_2 & x_1x_3 & \cdots & x_ix_j \end{matrix}$
$\begin{bmatrix} 0 & 0 & \cdots & R \\ 0 & 0 & \cdots & R \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & R \end{bmatrix}$

There is a possibility that the last row corresponds to a univariate equation during the process of row elimination. In the context of this study, we explored the column vector consisting of two different variables with degree two $\{x_ix_j\}$ following certain procedures and strategies. This proposed procedure follows Algorithm 1 to solve the system of equations.

Through our analysis, we successfully obtained the last non-zero row of the univariate equation using the one-step Gaussian elimination process. We put forward a strategy to solve the accompanying MQP and consequently resulting the unique solution of plaintext.

5. Illustrative Example of The Weak Macaulay Structure

For the purpose of illustration, a public system $\mathcal{P}$ of the multivariate quadratic polynomials of the size $\mathbb{F}_{17}$ is given as an example with random coefficients.

Example. Suppose the message vector $\mathbf{x} = (x_1, x_2, x_3) = (4, 7, 5)$ is encrypted into the ciphertext $\mathbf{z} = (16, 11, 11, 7, 11, 13)$ using the general work-flow of multivariate cryptography scheme as discussed in section 3 above. Then, we are given the ciphertext vector $\mathbf{z}$ and the public system $\mathcal{P}(\mathbf{x})$:

$$\mathcal{P}(\mathbf{x}) = \begin{cases} 16x_1x_2 + 0x_1x_3 + 0x_2x_3 + 1x_1^2 + 8x_1 + 10x_2^2 + 8x_2 + 16x_3^2 + 14x_3 \\ 9x_1x_2 + 0x_1x_3 + 0x_2x_3 + 10x_1^2 + 5x_1 + 16x_2^2 + 5x_2 + 6x_3^2 + 11x_3 \\ 0x_1x_2 + 0x_1x_3 + 0x_2x_3 + 3x_1^2 + 11x_1 + 11x_2^2 + 16x_2 + 7x_3^2 + 9x_3 \\ 4x_1x_2 + 0x_1x_3 + 0x_2x_3 + 12x_1^2 + 6x_1 + 12x_2^2 + 2x_2 + 9x_3^2 + 5x_3 \\ 8x_1x_2 + 0x_1x_3 + 0x_2x_3 + 7x_1^2 + 14x_1 + 3x_2^2 + 5x_2 + 11x_3^2 + 16x_3 \\ 10x_1x_2 + 0x_1x_3 + 0x_2x_3 + 14x_1^2 + 10x_1 + 2x_2^2 + 9x_2 + 16x_3^2 + 6x_3 \end{cases}$$

We conduct the following strategies.

Step 1: Transforming the system $\mathcal{P}(\mathbf{x})$ into the form of

$$\mathcal{P}(\mathbf{x}) = \begin{cases} p_1 = 16x_1x_2 + 0x_1x_3 + 0x_2x_3 + 1x_1^2 + 8x_1 + 10x_2^2 + 8x_2 + 16x_3^2 + 14x_3 + 1 = 0 \\ p_2 = 9x_1x_2 + 0x_1x_3 + 0x_2x_3 + 10x_1^2 + 5x_1 + 16x_2^2 + 5x_2 + 6x_3^2 + 11x_3 + 6 = 0 \\ p_3 = 0x_1x_2 + 0x_1x_3 + 0x_2x_3 + 3x_1^2 + 11x_1 + 11x_2^2 + 16x_2 + 7x_3^2 + 9x_3 + 6 = 0 \\ p_4 = 4x_1x_2 + 0x_1x_3 + 0x_2x_3 + 12x_1^2 + 6x_1 + 12x_2^2 + 2x_2 + 9x_3^2 + 5x_3 + 10 = 0 \\ p_5 = 8x_1x_2 + 0x_1x_3 + 0x_2x_3 + 7x_1^2 + 14x_1 + 3x_2^2 + 5x_2 + 11x_3^2 + 16x_3 + 6 = 0 \\ p_6 = 10x_1x_2 + 0x_1x_3 + 0x_2x_3 + 14x_1^2 + 10x_1 + 2x_2^2 + 9x_2 + 16x_3^2 + 6x_3 + 4 = 0 \end{cases}$$

Step 2: From the Wang's technique [33], we produce a Macaulay matrix M of the system $\mathcal{P}$.

$$M = \begin{bmatrix} c_{1(1)} & c_{1(2)} & \cdots & c_{1(10)} \\ c_{2(1)} & c_{2(2)} & \cdots & c_{2(10)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{6(1)} & c_{6(2)} & \cdots & c_{6(10)} \end{bmatrix}$$

$$= \begin{array}{c} \begin{matrix} x_1x_2 & x_1x_3 & x_2x_3 & x_1^2 & x_1 & x_2^2 & x_2 & x_3^2 & x_3 & 1 \end{matrix} \\ \begin{bmatrix} 16 & 0 & 0 & 1 & 8 & 10 & 8 & 16 & 14 & 1 \\ 9 & 0 & 0 & 10 & 5 & 16 & 5 & 6 & 11 & 6 \\ 0 & 0 & 0 & 3 & 11 & 11 & 16 & 7 & 9 & 6 \\ 4 & 0 & 0 & 12 & 6 & 12 & 2 & 9 & 5 & 10 \\ 8 & 0 & 0 & 7 & 14 & 3 & 5 & 11 & 16 & 6 \\ 10 & 0 & 0 & 14 & 10 & 2 & 9 & 16 & 6 & 4 \end{bmatrix} \end{array}$$

Step 3: Execute the Gaussian elimination process and resulting in the following matrix:

$$\widetilde{M} = \begin{array}{c} \begin{matrix} x_1x_2 & x_1x_3 & x_2x_3 & x_1^2 & x_1 & x_2^2 & x_2 & x_3^2 & x_3 & 1 \end{matrix} \\ \begin{bmatrix} 16 & 0 & 0 & 1 & 8 & 10 & 8 & 16 & 14 & 1 \\ 0 & 0 & 0 & 15 & 8 & 13 & 8 & 3 & 16 & 2 \\ 0 & 0 & 0 & 0 & 5 & 7 & 12 & 11 & 2 & 16 \\ 0 & 0 & 0 & 0 & 0 & 15 & 14 & 9 & 10 & 14 \\ 0 & 0 & 0 & 0 & 0 & 0 & 11 & 16 & 10 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 11 & 11 & 10 \end{bmatrix} \end{array}$$

By considering the last row of the matrix $\widetilde{M}$, we have the opportunity to solve the univariate equation.

$$11x_3^2 + 11x_3 + 10 = 0,$$

leading to $x_3 = 5$ in $\mathbb{F}_{17}$. By substitution $x_3 = 5$ into the system $\mathcal{P}(\mathbf{x})$, we will yield

$$M_1 = \begin{array}{c} \begin{matrix} x_1x_2 & x_1^2 & x_1 & x_2^2 & x_2 & 1 \end{matrix} \\ \begin{bmatrix} 16 & 1 & 8 & 10 & 8 & 12 \\ 9 & 10 & 5 & 16 & 5 & 7 \\ 0 & 3 & 11 & 11 & 16 & 5 \\ 4 & 12 & 6 & 12 & 2 & 5 \\ 8 & 7 & 14 & 3 & 5 & 4 \\ 10 & 14 & 10 & 2 & 9 & 9 \end{bmatrix} \end{array}$$

Step 4: Performing the Gaussian elimination procedure yields the subsequent matrix:

$$\widetilde{M_1} = \begin{matrix} x_1x_2 \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} x_1^2 \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} x_1 \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} x_2^2 \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} x_2 \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} 1 \\ \\ \\ \\ \\ \\ \end{matrix} \begin{bmatrix} 16 & 1 & 8 & 10 & 8 & 12 \\ 0 & 15 & 8 & 13 & 8 & 4 \\ 0 & 0 & 5 & 7 & 12 & 12 \\ 0 & 0 & 0 & 15 & 14 & 0 \\ 0 & 0 & 0 & 0 & 11 & 8 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

From the matrix $\widetilde{M_1}$, we can observe that the last non-zero row has the form of a univariate equation. Therefore, we can solve $11x_2 + 8 = 0$ and obtain the solution of $x_2 = 7$.

Iterate the process of substitution and Gaussian elimination, leading to the formation of matrices M_2 and $\widetilde{M_2}$, respectively.

$$M_2 = \begin{matrix} x_1^2 \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} x_1 \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} 1 \\ \\ \\ \\ \\ \\ \end{matrix} \begin{bmatrix} 1 & 1 & 14 \\ 10 & 0 & 10 \\ 3 & 11 & 10 \\ 12 & 0 & 12 \\ 7 & 2 & 16 \\ 14 & 12 & 0 \end{bmatrix} \quad \text{and} \quad \widetilde{M_2} = \begin{matrix} x_1^2 \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} x_1 \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} 1 \\ \\ \\ \\ \\ \\ \end{matrix} \begin{bmatrix} 1 & 1 & 14 \\ 0 & 7 & 6 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

The last non-zero row of $\widetilde{M_2}$, $7x_1 + 6 = 0$ gives the solution of $x_1 = 4$. As a result, we obtain the solution $(x_1, x_2, x_3) = (4, 7, 5)$, which the message of the public system $\mathcal{P}(x_1, x_2, x_3)$ over $\mathbb{F}_{17}$.

6. Conclusions

We presented a mechanism to detect weak multivariate quadratic (MQ) structures through the visualization of the Macaulay matrix corresponding to the public system $\mathcal{P}(\mathbf{x})$. This strategy specifically applies to an overdetermined system using one-step Gaussian elimination. Furthermore, since MQ-based cryptosystems do not exponentially utilize many quadratic equations and variables, this strategy can effectively work for a system of m quadratic equations in n variables within polynomial time. This is possible due to the complexity of Gaussian elimination for a m by n matrix, which is $\mathcal{O}(mn^2)$ [41]. Since this Gaussian elimination technique works for solving the multivariate quadratic problem, it might also be applicable for cubic multivariate schemes.

Acknowledgement

The authors extend sincere appreciation for the invaluable support received from the Institute for Mathematical Research (INSPEM), Universiti Putra Malaysia (UPM), the Ministry of Higher Education (MOHE) and Universiti Teknologi MARA (UiTM), which granted the opportunity to carry out this research.

References

[1] Sarbini, Izzatul Nabila, Tze Jin Wong, Lee Feng Koo, Ahmad Fadly Nurullah Rasedee, Fatin Hana Naning, and Mohammad Hasan Abdul Sathar. "Security Analysis on LUC-type Cryptosystems Using Common Modulus Attack." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 29, no. 3 (2023): 206-213. https://doi.org/10.37934/araset.29.3.206213

[2] Yusof, Siti Nabilah, Muhammad Rezal Kamel Ariffin, Terry Shue Chien Lau, Nur Raidah Salim, Sook-Chin Yip, and Timothy Tzen Vun Yap. "An IND-CPA Analysis of a Cryptosystem Based on Bivariate Polynomial Reconstruction Problem." *Axioms* 12, no. 3 (2023): 304. https://doi.org/10.3390/axioms12030304
[3] Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM* 21, no. 2 (1978): 120-126. https://doi.org/10.1145/357980.358017
[4] Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." *SIAM* review 41, no. 2 (1999): 303-332. https://doi.org/10.1137/S0036144598347011
[5] Yusof, Siti Nabilah, and Muhammad Rezal Kamel Ariffin. "An Empirical Attack on a Polynomial Reconstruction Problem Potential Cryptosystem." *Int. J. Cryptol. Res.* 11 (2021): 31-48.
[6] Takagi, Tsuyoshi. "Post-quantum cryptography." *Lecture Notes in Computer Science* 9606 (2016). https://doi.org/10.1007/978-3-319-29360-8
[7] Garey, Michael R., and David S. Johnson. "Computers and intractability." *A Guide to the* (1979).
[8] Jamal, Nurul Amiera Sakinah Abdul, Muhammad Rezal Kamel Ariffin and Kamilah Abdullah "Novel Forgery Mechanisms in Multivariate Signature Schemes." *International Journal of Mathematics and Computer Science* 18, no. 3 (2023): 451-461.
[9] Bernstein, Daniel J., Johannes Buchmann, and Erik Dahmen. "Post-Quantum Cryptography. –2009." https://doi.org/10.1007/978-3-540-88702-7
[10] Ding, Jintai, and Albrecht Petzoldt. "Current state of multivariate cryptography." *IEEE Security & Privacy* 15, no. 4 (2017): 28-36. https://doi.org/10.1109/MSP.2017.3151328
[11] Abdul Jamal, Nurul Amiera Sakinah, Muhammad Rezal Kamel Ariffin, Siti Hasana Sapar, and Kamilah Abdullah. "New Identified Strategies to Forge Multivariate Signature Schemes." *Symmetry* 14, no. 11 (2022): 2368. https://doi.org/10.3390/sym14112368
[12] Ong, H., Claus-Peter Schnorr, and Adi Shamir. "Efficient signature schemes based on polynomial equations (preliminary version)." In *Advances in Cryptology: Proceedings of CRYPTO 84 4*, pp. 37-46. Springer Berlin Heidelberg, 1985. https://doi.org/10.1007/3-540-39568-7_4
[13] Pollard, J., and C. Schnorr. "An efficient solution of the congruence x^ 2+ ky^ 2= mpmod {n}." *IEEE Transactions on Information Theory* 33, no. 5 (1987): 702-709. doi: 10.1109/TIT.1987.1057350.
[14] Estes, Dennis, Leonard M. Adleman, Kireeti Kompella, Kevin S. McCurley, and Gary L. Miller. "Breaking the Ong-Schnorr-Shamir signature scheme for quadratic number fields." In *Conference on the Theory and Application of Cryptographic Techniques*, pp. 3-13. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985. https://doi.org/10.1007/3-540-39799-X_1
[15] Fell, Harriet, and Whitfield Diffie. "Analysis of a public key approach based on polynomial substitution." In *Conference on the Theory and Application of Cryptographic Techniques*, pp. 340-349. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985. https://doi.org/10.1007/3-540-39799-X_24
[16] Imai, Hideki, and Tsutomu Matsumoto. "Algebraic methods for constructing asymmetric cryptosystems." In *Algebraic Algorithms and Error-Correcting Codes: 3rd International Conference, AAECC-3 Grenoble, France, July 15–19, 1985 Proceedings 3*, pp. 108-119. Springer Berlin Heidelberg, 1986. https://doi.org/10.1007/3-540-16776-5_713
[17] Matsumoto, Tsutomu, and Hideki Imai. "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption." In *Advances in Cryptology—EUROCRYPT'88: Workshop on the Theory and Application of Cryptographic Techniques Davos, Switzerland, May 25–27, 1988 Proceedings 7*, pp. 419-453. Springer Berlin Heidelberg, 1988. https://doi.org/10.1007/3-540-45961-8_39
[18] Patarin, Jacques, Louis Goubin, and Nicolas Courtois. "C−+* and HM: Variations around two schemes of T. Matsumoto and H. Imai." In *Advances in Cryptology—ASIACRYPT'98: International Conference on the Theory and Application of Cryptology and Information Security Beijing, China, October 18–22, 1998 Proceedings*, pp. 35-50. Springer Berlin Heidelberg, 1998. https://doi.org/10.1007/3-540-49649-1_4
[19] Patarin, Jacques. "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms." In *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 33-48. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996. https://doi.org/10.1007/3-540-68339-9_4
[20] Ding, Jintai, and Bo-Yin Yang. "Degree of regularity for HFEv and HFEv." In *International Workshop on Post-Quantum Cryptography*, pp. 52-66. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. https://doi.org/10.1007/978-3-642-38616-9_4
[21] Ding, Jintai, and Dieter Schmidt. "Cryptanalysis of HFEv and internal perturbation of HFE." In *Public Key Cryptography-PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005. Proceedings 8*, pp. 288-301. Springer Berlin Heidelberg, 2005. https://doi.org/10.1007/978-3-540-30580-4_20

[22] Kipnis, Aviad, Jacques Patarin, and Louis Goubin. "Unbalanced oil and vinegar signature schemes." In *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 206-222. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999. https://doi.org/10.1007/3-540-48910-X_15

[23] Akkar, Mehdi-Laurent, Nicolas T. Courtois, Romain Duteuil, and Louis Goubin. "A fast and secure implementation of Sflash." In *International Workshop on Public Key Cryptography*, pp. 267-278. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002. https://doi.org/10.1007/3-540-36288-6_20

[24] Moh, T. "A public key system with signature and master key functions." *Communications in Algebra* 27, no. 5 (1999): 2207-2222. https://doi.org/10.1080/00927879908826559

[25] Yang, Bo-Yin, and Jiun-Ming Chen. "Building secure tame-like multivariate public-key cryptosystems: The new TTS." In *Australasian Conference on Information Security and Privacy*, pp. 518-531. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005. https://doi.org/10.1007/11506157_43

[26] Wang, Lih-Chung, and Fei-Hwang Chang. "Tractable rational map cryptosystem." *manuscript, E-print Archive* 46 (2004).

[27] Wang, Lih-Chung, Yuh-Hua Hu, Feipei Lai, Chun-Yen Chou, and Bo-Yin Yang. "Tractable rational map signature." In *Public Key Cryptography-PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005. Proceedings 8*, pp. 244-257. Springer Berlin Heidelberg, 2005. https://doi.org/10.1007/978-3-540-30580-4_17

[28] Ding, Jintai, and Dieter Schmidt. "Rainbow, a new multivariable polynomial signature scheme." In *International conference on applied cryptography and network security*, pp. 164-175. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005. https://doi.org/10.1007/11496137_12

[29] Tao, Chengdong, Adama Diene, Shaohua Tang, and Jintai Ding. "Simple matrix scheme for encryption." In *Post-Quantum Cryptography: 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013. Proceedings 5*, pp. 231-242. Springer Berlin Heidelberg, 2013. https://doi.org/10.1007/978-3-642-38616-9_16

[30] Tsaban, Boaz. "Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography." *Journal of Cryptology* 28 (2015): 601-622. https://doi.org/10.1007/s00145-013-9170-9

[31] Bettale, Luk, Jean-Charles Faugere, and Ludovic Perret. "Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic." *Designs, Codes and Cryptography* 69 (2013): 1-52. https://doi.org/10.1007/s10623-012-9617-2

[32] Tao, Chengdong, Hong Xiang, Albrecht Petzoldt, and Jintai Ding. "Simple matrix–a multivariate public key cryptosystem (MPKC) for encryption." *Finite Fields and Their Applications* 35 (2015): 352-368. https://doi.org/10.1016/j.ffa.2015.06.001

[33] Petzoldt, Albrecht, Jintai Ding, and Lih-Chung Wang. "Eliminating decryption failures from the simple matrix encryption scheme." *Cryptology ePrint Archive* (2016).

[34] Ding, Jintai, Albrecht Petzoldt, Dieter S. Schmidt, Jintai Ding, Albrecht Petzoldt, and Dieter S. Schmidt. "Multivariate cryptography." *Multivariate Public Key Cryptosystems* (2020): 7-23. https://doi.org/10.1007/978-1-0716-0987-3_2

[35] Koblitz, Neal, Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato. *Algebraic aspects of cryptography*. Vol. 198. Heidelberg: Springer, 1998.

[36] Kurokawa, Takashi, Takuma Ito, Naoyuki Shinohara, Akihiro Yamamura, and Shigenori Uchiyama. "Selection Strategy of F4-Style Algorithm to Solve MQ Problems Related to MPKC." *Cryptography* 7, no. 1 (2023): 10. https://doi.org/10.3390/cryptography7010010

[37] Ito, Takuma, Yuta Hoshi, Naoyuki Shinohara, and Shigenori Uchiyama. "Polynomial selection of F4 for solving the MQ problem." *JSIAM Letters* 14 (2022): 135-138. https://doi.org/10.14495/jsiaml.14.135

[38] Wang, Lih-Chung, Tzer-jen Wei, Jian-Ming Shih, Yuh-Hua Hu, and Chih-Cheng Hsieh. "An algorithm for solving over-determined multivariate quadratic systems over finite fields." *Advances in Mathematics of Communications* 18, no. 1 (2024): 55-90. https://doi.org/10.3934/amc.2022001

[39] Courtois, Nicolas T., and Jacques Patarin. "About the XL Algorithm over GF (2)." In *Topics in Cryptology—CT-RSA 2003: The Cryptographers' Track at the RSA Conference 2003 San Francisco, CA, USA, April 13–17, 2003 Proceedings*, pp. 141-157. Springer Berlin Heidelberg, 2003. https://doi.org/10.1007/3-540-36563-X_10

[40] Abdullah, Kamilah, Muhammad Rezal Kamel Ariffin, and Nurul Amiera Sakinah Abdul Jamal. "A New Macaulay Matrix Structure for Solving Multivariate Quadratic Problem." *International Journal of Cryptology Research* (2022): 31-45.

[41] Gall, François Le, and Florent Urrutia. "Improved rectangular matrix multiplication using powers of the coppersmith-winograd tensor." In *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms*, pp. 1029-1046. Society for Industrial and Applied Mathematics, 2018. https://doi.org/10.1137/1.9781611975031.67