International Journal of Cryptology Research 12(1): 31 - 45 (2022)

A New Macaulay Matrix Structure for Solving Multivariate Quadratic Problem

Kamilah Abdullah[*1,3], **Muhammad Rezal Kamel Ariffin**[1,2], and **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]*School of Mathematical Sciences, College of Computing, Informatics and Media, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia*

E-mail: kamilah@tmsk.uitm.edu.my
[*]*Corresponding author*

ABSTRACT

The security of a Multivariate Public-Key Cryptosystem (MPKC) depends on the complexity of solving Multivariate Quadratic (MQ) equations over finite fields, also known as the MQ problem. In this study, we propose a new approach to solving the system of MQ equations based on the Macaulay matrix, which is constructed from the coefficients of these equations. This approach works on zero coefficients for different variables (monomials) and random coefficients for other monomials by applying the one-step Gaussian elimination to obtain a univariate equation.

Keywords: Multivariate Public-Key Cryptosystem, Multivariate Quadratic problem, Gaussian elimination

1 INTRODUCTION

In an era where information technology is highly demanded, the transmission of information via the internet becomes crucial where all processes, transactions, or communications are through public channels. Public-key cryptography (PKC) is one of the fundamental tools that can secure this situation. The security of the current PKC is based on two hard mathematical problems known as the integer factorization problem and the discrete logarithm problem. These two problems were proven to be solved in polynomial time once a quantum computer existed. Therefore, the formulation of robust alternatives to the current cryptosystems that are able to resist quantum computing-based attacks is needed. Among such alternatives, multivariate cryptography is one of the preferences that seems promising to be able to resist against quantum computer attacks.

Multivariate cryptography is based on the hard mathematical problem of solving a system of multivariate polynomials. According to current research, multivariate cryptosystems are all based on the Multivariate Quadratic (MQ) system (Ding et al., 2020). The MQ problem is proved to be NP-hard (Nondeterministic polynomial-time) (Fraenkel and Yesha, 1979; Garey and Johnson, 1979), and it seems that using quantum computers will not provide any benefits to solving it (Barker et al., 2021). However, the NP-hard situation does not prove the in existence of certain polynomials which would render the MQ problem solvable.

In the case of the overdetermined MQ polynomial system, several algorithms are acknowledged to solve the system. Among these algorithms are Grobner-basis computation (Faugère, 1999, 2002), linearization (Buchmann et al., 2009; Courtois et al., 2000; Wang et al., 2022) and algorithms based on SAT-solvers (Bard et al., 2007). As a result, one can assess an overdetermined system that can be implemented as a Multivariate Public Key Cryptosystem (MPKC). Currently, there are many MPKCs such as SimpleMatrix Encryption (Petzoldt et al., 2016; Tao et al., 2013, 2015), variants of Hidden Field Encryption (Faugère and Joux, 2003; Ping et al., 2017), and Extension Field

Cancellation (Chakraborty et al., 2021; Smith-Tone and Verbel, 2020).

This paper focuses on producing methods for assessing the security of MPKC. We are motivated in this direction because there might be certain structures of equations that will result in MPKC to be insecure, that is we study the problem of solving certain classes of multivariate polynomial equations.

Contribution. This paper proposed a new approach based on linear algebra techniques known as the one-step Gaussian elimination. We also illustrate a numerical example solving the polynomial system $p^{(1)}(\mathbf{x}) = \ldots = p^{(m)}(\mathbf{x}) = 0$, which would obtaining the candidates solution for $\mathbf{x} = (x_1, \ldots, x_n)$. This research differs from previous works in 2 aspects:

- The one-step gauss elimination presents a new process to obtain the candidates' solution.
- The strategies in manipulating the structure of the Macaulay matrix.

This paper is structured as follows. Firstly, the preliminaries of fundamental definitions and concepts are presented in section 2. Followed by the numerical illustration in Section 3. Finally, the conclusion is provided in Section 4.

2 PRELIMINARIES

In this section, fundamental definitions and concepts used in this paper are discussed. MPKC involved the problem of solving systems of multivariate quadratic polynomials where the number of equations in the system is denoted by m and the number of variables is denoted by n.

Definition 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

$$\begin{aligned}
p_1(x_1, \ldots, x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} c_{ij}^{(1)} \cdot x_i x_j + \sum_{i=1}^{n} c_i^{(1)} \cdot x_i + c_0^{(1)} \\
p_2(x_1, \ldots, x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} c_{ij}^{(2)} \cdot x_i x_j + \sum_{i=1}^{n} c_i^{(2)} \cdot x_i + c_0^{(2)} \\
&\vdots \\
p_m(x_1, \ldots, x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} c_{ij}^{(m)} \cdot x_i x_j + \sum_{i=1}^{n} c_i^{(m)} \cdot x_i + c_0^{(m)}.
\end{aligned}$$

Definition 2. *Let $\mathcal{P}(x_1, \ldots, x_n)$ be a system of multivariate quadratic polynomials.*

*a) We define the **lexicographical ordering** of monomials are listed in the same order in which the monomials (omitted the value of coefficients) would exist in terms of words in alphabet consisting of $x_1, x_2, \ldots, x_n$ letters (Koblitz et al., 1998).*

*b) We define the **chosen-lexicographical ordering** of monomials are listed from two variables to a single variable and subject to the priority of solving a variable.*

Example 2.1. *a) Let $\mathcal{P}(x_1, x_2, x_3, x_4) = 5x_4x_2 + 3x_3^2 + 2x_3x_4 + 2x_3x_1 + 3x_1^2 + x_1 + x_4^2 + 4x_3x_2$. The polynomial is rewritten as*

$$\mathcal{P}(x_1, \ldots, x_4) = 3x_1^2 + 2x_1x_3 + x_1 + 4x_2x_3 + 5x_2x_4 + 3x_3^2 + 2x_3x_4 + x_4^2$$

under the lexicographical ordering.

b) The example describe in a) is rewritten as

$$\mathcal{P}(x_1, \ldots, x_4) = 2x_1x_3 + 4x_2x_3 + 5x_2x_4 + 2x_3x_4 + 3x_1^2 + x_1 + 3x_3^2 + x_4^2$$

under the chosen-lexicographical ordering.

For this study, Definition b) will be used throughout the process of transforming the system of polynomials into the Macaulay matrix to be solved using Gaussian elimination.

The chosen-lexicographical ordering of monomials reflexes the priority of solving a variable. As an illustration, assume x_3 to be eliminated first. A univariate polynomial in terms of x_3 with a degree at most d is obtained. Then, one solves the univariate polynomial over the finite field. Hence, the possible value(s) of x_3 are obtained. To this end, we will now substitute x_3 in order to obtain the polynomials with fewer variables.

2.1 The Multivariate Quadratic Problem

In this section, we state definitions and theorems related to solving Multivariate Quadratic (MQ) equations.

Definition 3. *(Ding et al., 2020) (Problem of Solving Polynomial Systems (PoSSo)) Let $\mathbb{F} = \mathbb{F}_q$ be a finite field with q elements. Given a system $\mathcal{P} = (p_1(x), \ldots, p_m(x))$ of m multivariate quadratic polynomials in n variables, find a vector $\mathbf{x} = (x_1, \ldots, x_n)$ such that*

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

The Polynomial System Solving is known as NP-hard even if the input polynomials are quadratics. This PoSSo is also called *MQ*.

The following theorems imply that every system of MQ can be simplified to an illustration in which the polynomial system is given in the standard form.

Theorem 2.1. *(Ding et al., 2020) Let $\mathbb{F}$ be a finite field with q elements and degree $d < q$. Then, there exist $\binom{n+d-1}{d}$ monomials of degree d in $\mathbb{F}[x_1, \ldots, x_n]$. The number of monomials of degree $\leq d$ in $\mathbb{F}[x_1, \ldots, x_n]$ is given by $\binom{n+d}{d}$.*

Proof.

1. The number of monomials of degree d is obtain by choosing d out of n element of $x_1, \ldots, x_n$, with repetition.
2. The elements in polynomial of degree $\leq d$ are elements from the set $\{x_1, \ldots, x_n, 1\}$, with repetition.

□

Example 2.2. *Let the degree $d = 2$ and $n = 2$. Then, the elements consist of x_1 and x_2. The number of monomials of degree 2 is $\binom{3}{2} = 3$ in $\mathbb{F}[x_1, x_2]$. The monomials involve are x_1x_2, x_1^2, and x_2^2. While the polynomial of degree ≤ 2 and total number of monomials are $\binom{4}{2} = 6$ consists of 2 elements $\{x_1, x_2\}$ are $x_1x_2, x_1^2, x_1, x_2^2, x_2$ and c, where c is a constant of polynomial.*

Theorem 2.2. *The number of monomials of degree $\leq d$ in $\mathbb{F}_q$ with q elements is given by $\binom{n+d}{d}$. The number of monomials with degree d with different elements is given by $\binom{n}{d}$.*

Proof.

1. The total number of monomials of degree $\leq d$ is according to n elements from the set $\{x_1, \ldots, x_n, 1\}$, with repetition.
2. The total number of monomials of degree $\leq d$ is according to n elements from the set $\{x_1, \ldots, x_n, 1\}$, without repetition.

□

Example 2.3. *Let $d = 2$ and $n = 3$. Then, the elements are x_1, x_2, and x_3. Thus, the total number of monomials is $\binom{5}{2} = 10$ elements. The monomials obtained are $x_1x_2, x_1x_3, x_2x_3, x_1^2, x_1, x_2^2, x_2, x_3^2, x_3, c$. Whilst, the number of different elements as a monomial with degree d is $\binom{3}{2} = 3$ which are x_1x_2, x_1x_3 and x_2x_3, without repetition.*

In order to solve a system of MQ polynomial equations, we incorporate the polynomials in the Macaulay matrix that is constructed from the equations $(p_1(x), \ldots, p_m(x)) = 0$ (Definition 3) and it is reduced by a reduction algorithm known as Gaussian elimination. Then, the number of the monomials of degree $\leq d$ is $\binom{n+d}{d}$, that is the number of column vectors in the Macaulay matrix M.

Here, the Macaulay matrix M of degree d with respect to $p(\mathbf{x}) = p_1(\mathbf{x}), \ldots, p_m(\mathbf{x})$ is defined as follows.

Definition 4. ***(Macaulay Matrix)*** *The Macaulay matrix $M \in \mathbb{F}^{m \times n}$ of degree d contains the coefficient vectors of the polynomials $p_i(\boldsymbol{x})$ where $i \in \{1, \ldots, m\}$ as its rows. Define the matrix M as*

$$M = \begin{bmatrix} p_1(\boldsymbol{x}) \\ p_2(\boldsymbol{x}) \\ \vdots \\ p_m(\boldsymbol{x}) \end{bmatrix}$$

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

Algorithm 1 shows the general process of solving Multivariate Quadratic polynomials using Gaussian elimination.

Algorithm 1 Solving the Multivariate Quadratic polynomials

Input: The Multivariate Quadratic system consists of m quadratic polynomial $\mathcal{P} = (p_1(x), \ldots, p_m(x))$ in n variables of $(x_1, \ldots, x_n)$ and coefficients in a finite field $\mathbb{F}_q$.

Output: The solution in $\mathbb{F}_q$ of the system of the equations $p_1(\mathbf{x}) = \ldots = p_m(\mathbf{x}) = 0$.

1. **Linearize:** Consider the sequence of monomial based on chosen-lexicographical ordering (Definition 2 b)) in the variables $x_i x_j$ and x_i. The ordering of the monomials of polynomial $\mathcal{P}$ must be containing single variables (i.e. x_i) is eliminated last.

2. **Organize:** Generate the Macaulay matrix M based on Definition 4.

3. **Solve:** Perform Gauss elimination on the system M. Assume that this step yields one last non-zero univariate polynomial equation in some variable x_n. Find the root of this equation in the underlying finite field.

4. **Repeat:** Substitute the value obtain in Step 3 into the system $\mathcal{P}$ and simplify the equations. Repeat the process to solve for other variables.

3 THE ATTACK

In this section, we construct the Organized Gaussian Elimination(OGE) to illustrate the proposed method. The process of OGE is the modification matrix to rearrange the columns of two different variables of monomials as identified coefficients.

Organized Gaussian Elimination: In order to obtain a univariate equation using one-step Gaussian elimination, we strategies the column vectors of the Macaulay matrix with variables $\{x_i x_j\}$ as $i, j = 1, \ldots, n$ to be studied.

Algorithm 2 Organized Gaussian Elimination with Column of Two Different Variables

Input: The Macaulay matrix M (Definition 4).
Output: The potential solutions of $\mathbf{x} = \{x_1, \ldots, x_n\}$.

1. Setting the column vectors of matrix M with two different variables $\{x_i x_j\}$ as the set of zeroes coefficient.
2. Apply one-step Gaussian elimination and assume this process will obtain the last non-zero row of a univariate equation.
3. Solve the equation to obtain the variable in step 2 and substitute the value into the matrix M.
4. Update and simplify the matrix M and repeat the process from the step 2 to step 4 and solve other variables $\{x_{n-1}, \ldots, x_1\}$.

3.1 Cryptanalysis of Multivariate Quadratic Polynomial

Cryptanalysis of the MQ polynomial is to obtain the value of candidates for plaintext which gives zero for each equation m in the polynomial. The process of row elimination has the opportunity for the last row to represent the univariate equation.

We considered the column vector of two different variables with degree two $\{x_i x_j\}$ based on the following procedures and strategies. The proposed procedure is as follows:

Step 1: Define the MQ system of equations over the finite field $\mathbb{F}$ is a set of m polynomial equations of degree at most 2 in $\mathbb{F}[x_1, \ldots, x_n]$ of the form:

$$\mathcal{P}(\mathbf{x}) = \begin{cases} p_1(x_1, \ldots, x_n) & = 0 \\ p_2(x_1, \ldots, x_n) & = 0 \\ \vdots & \\ p_m(x_1, \ldots, x_n) & = 0 \end{cases} \tag{1}$$

where for every $k \in 1, \ldots, m$, the system can be determine in the form of

$$\mathcal{P}_k(x_1, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} c_{ij}^{(k)} \cdot x_i x_j + c_i^{(k)} \cdot x_i + c_0^{(k)}$$

with $c^{(k)}$ in finite field $\mathbb{F}$.

Step 2: Form the Macaulay matrix M of the initial system $\mathcal{P}(\mathbf{x})$.

$$M = \begin{bmatrix} p_1(\mathbf{x}) \\ p_2(\mathbf{x}) \\ \vdots \\ p_m(\mathbf{x}) \end{bmatrix} = \begin{bmatrix} coeff(p_1, c_1) & coeff(p_1, c_2) & \cdots & coeff(p_1, c_{n+d}) \\ coeff(p_2, c_1) & coeff(p_2, c_1) & \cdots & coeff(p_2, c_{n+d}) \\ \vdots & \vdots & \ddots & \vdots \\ coeff(p_m, c_1) & coeff(p_m, c_1) & \cdots & coeff(p_m, c_{n+d}) \end{bmatrix}$$

$$= \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1(n+d)} \\ c_{21} & c_{22} & \cdots & c_{2(n+d)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{m(n+d)} \end{bmatrix}$$

Step 3: Apply the process of Gaussian Elimination (GE) to the Macaulay matrix M. This one-step GE will obtain a new matrix which resulting the last non-zero univariate equation form. Solving this equation will obtain the value of variable x_n.

Step 4: Substitute the value obtained into the original system in step 1 and solve for x_{n-1}. Repeat step 2 until obtaining x_1.

The OGE demonstrates the benefits of using zero coefficients on monomials of two different variables $x_i x_j$ where $i, j = 1, \ldots, n$. Subsequently, by analyzing the column space of zero monomials using one-step GE, we manage to obtain the last non-zero univariate equation.

Case: Zero coefficients of two different monomials

Set the column vectors of $\binom{n}{d}$ are zero elements for two different variables

for monomial degree 2 of $\{x_i x_j\}$ and the column vectors of $\binom{n+d}{d} - \binom{n}{d}$ represent by R which is random coefficient < q, then the Macaulay matrix M can be rewritten as

$$M = \begin{array}{c} \begin{matrix} x_1x_2 & x_1x_3 & \dots & x_ix_j & x_1^2 & x_1 & \dots & x_n^2 & x_n & 1 \end{matrix} \\ \left[\begin{matrix} \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & R & R & R & R & R & R \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & R & R & R & R & R & R \\ \vdots & \vdots & \ddots & \vdots & R & R & R & R & R & R \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & R & R & R & R & R & R \end{matrix}\right] \end{array}$$

3.2 Random Example

For implementation purposes, an example is presented using a random number for a system $\mathcal{P}$ of multivariate quadratic polynomials of $\mathbb{F}_q$.

Consider a system of six quadratic equations (m = 6) in n = 3 variables, $\mathbf{x} = \{x_1, x_2, x_3\}$ over $\mathbb{F}_{17}$ (the finite field with 17 elements).The system $\mathcal{P}$ is given by

$$\mathcal{P}(\mathbf{x}) = \begin{cases} 0x_1x_2 + 0x_1x_3 + 0x_2x_3 & + & x_1^2 + 15x_1 + 12x_2^2 + 7x_2 + 11x_3^2 + 8x_3 + 0 \\ 0x_1x_2 + 0x_1x_3 + 0x_2x_3 & + & 9x_1^2 + 1x_1 + 0x_2^2 + 9x_2 + 3x_3^2 + 0x_3 + 12 \\ 0x_1x_2 + 0x_1x_3 + 0x_2x_3 & + & 0x_1^2 + 3x_1 + 1x_2^2 + 6x_2 + 6x_3^2 + 16x_3 + 15 \\ 0x_1x_2 + 0x_1x_3 + 0x_2x_3 & + & 12x_1^2 + 4x_1 + 4x_2^2 + 5x_2 + 5x_3^2 + 3x_3 + 13 \\ 0x_1x_2 + 0x_1x_3 + 0x_2x_3 & + & 3x_1^2 + 6x_1 + 5x_2^2 + 6x_2 + 10x_3^2 + 3x_3 + 5 \\ 0x_1x_2 + 0x_1x_3 + 0x_2x_3 & + & 3x_1^2 + 15x_1 + 9x_2^2 + 16x_2 + 9x_3^2 + 6x_3 + 11 \end{cases}$$

Step 1: Setting the system $\mathcal{P}$ in the form of

$$\mathcal{P}(\mathbf{x}) = \begin{cases} p_1(x_1, \dots, x_n) & = 0 \\ p_2(x_1, \dots, x_n) & = 0 \\ \vdots & \\ p_m(x_1, \dots, x_n) & = 0 \end{cases} \tag{2}$$

Step 2: Form the Macaulay matrix M of the system $\mathcal{P}$.

$$M = \begin{bmatrix} p_1(\mathbf{x}) \\ p_2(\mathbf{x}) \\ \vdots \\ p_m(\mathbf{x}) \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1(n+d)} \\ c_{21} & c_{22} & \cdots & c_{2(n+d)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{m(n+d)} \end{bmatrix}$$

$$= \begin{array}{c} \begin{matrix} x_1x_2 & x_1x_3 & x_2x_3 & x_1^2 & x_1 & x_2^2 & x_2 & x_3^2 & x_3 & 1 \end{matrix} \\ \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 & 15 & 12 & 7 & 11 & 8 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 9 & 1 & 0 & 9 & 3 & 0 & 12 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 3 & 1 & 6 & 6 & 16 & 15 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 12 & 4 & 4 & 5 & 5 & 3 & 13 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 3 & 6 & 5 & 6 & 10 & 3 & 5 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 3 & 15 & 9 & 16 & 9 & 6 & 11 \end{bmatrix} \end{array}$$

Step 3: Perform the process of Gaussian elimination and obtain the following matrix:

$$\tilde{M} = \begin{array}{c} \begin{matrix} x_1x_2 & x_1x_3 & x_2x_3 & x_1^2 & x_1 & x_2^2 & x_2 & x_3^2 & x_3 & 1 \end{matrix} \\ \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 & 15 & 12 & 7 & 11 & 8 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 2 & 11 & 14 & 6 & 13 & 12 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 0 & 3 & 4 & 11 & 10 & 11 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 0 & 0 & 11 & 0 & 7 & 15 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 0 & 0 & 0 & 5 & 0 & 6 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 0 & 0 & 0 & 0 & 8 & 10 \end{bmatrix} \end{array}$$

In the last row of the matrix $\tilde{M}$, we can solve the univariate equation

$$8x_3 + 10 = 0, \tag{3}$$

leading to $x_3 = 3$ in $\mathbb{F}_{17}$. By substitution $x_3 = 3$ into the system $\mathcal{P}$ yield

$$M_1 = \begin{array}{c} \begin{matrix} x_1x_2 & x_1^2 & x_1 & x_2^2 & x_2 & 1 \end{matrix} \\ \left[\begin{array}{cccccc} \mathbf{0} & 1 & 15 & 12 & 7 & 4 \\ \mathbf{0} & 9 & 1 & 0 & 9 & 5 \\ \mathbf{0} & 0 & 3 & 1 & 6 & 15 \\ \mathbf{0} & 12 & 4 & 4 & 5 & 16 \\ \mathbf{0} & 3 & 6 & 5 & 6 & 2 \\ \mathbf{0} & 3 & 15 & 9 & 16 & 8 \end{array}\right] \end{array}$$

Performing Gaussian elimination on M_1, we obtain the solution of $x_2 = 6$ and repeat the process of substitution yielding the solution of $x_1 = 5$. Therefore, we have found the solution $(x_1, x_2, x_3) = (5, 6, 3)$ of the original system $\mathcal{P}(x_1, x_2, x_3) = 0$ over $\mathbb{F}_{17}$.

4 CONCLUSION

We presented a new approach for solving the Multivariate Quadratic problem for an overdetermined system using one-step Gaussian elimination. Our proposed method known as Organized Gaussian Elimination (OGE) eliminated the two different variables (monomials) by setting them as zero coefficients.
We define a system with m multivariate quadratic equations in n variables, then the proposed algorithm identified the system with the number of $\binom{n+d}{d}$ monomials in the finite field of $\mathbb{F}_q$ of $x_1, \ldots, x_n$ variables. Then, we generate a Macaulay matrix M over $\mathbb{F}_q$ and perform one-step Gaussian elimination and resulting in the form of a univariate equation. Finally, the potential value(s) of solving variable is substituted to the original system and the remaining part of the matrix performs the repeated process.
This paper only discusses solving multivariate quadratic polynomials of overdetermined systems. However, the proposed algorithm can be generalized to other constraints related to two different variables of monomials or other higher-degree cases. Therefore, considerable future work is to analyze the complexity of the methodology.

ACKNOWLEDGEMENTS

The first author would like to further express appreciation to the Institute for Mathematical Research (INSPEM), Universiti Putra Malaysia (UPM), and the Ministry of Higher Education (MOHE) for giving the opportunity to conduct this research.

REFERENCES

Bard, G. V., Courtois, N. T., and Jefferson, C. (2007). Efficient methods for conversion and solution of sparse systems of low-degree multivariate polynomials over gf (2) via sat-solvers. *Cryptology ePrint Archive*.

Barker, W., Souppaya, M., and Newhouse, W. (2021). Migration to post-quantum cryptography. pages 1–15.

Buchmann, J. A., Ding, J., Mohamed, M. S. E., and Mohamed, W. S. A. E. (2009). Mutantxl: Solving multivariate polynomial equations for cryptanalysis. In *Dagstuhl seminar proceedings*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik.

Chakraborty, O., Faugère, J.-C., and Perret, L. (2021). Cryptanalysis of the extension field cancellation cryptosystem. *Des. Codes Cryptogr.*, 89:1335–1364.

Courtois, N., Klimov, A., Patarin, J., and Shamir, A. (2000). Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 392–407. Springer.

Ding, J., Petzoldt, A., and Schmidt, D. S. (2020). Multivariate cryptography. In *Multivariate Public Key Cryptosystems*, pages 7–23. Springer.

Faugère, J.-C. (1999). A new efficient algorithm for computing gröbner bases (f4). *Journal of Pure and Applied Algebra*, 139:61–88.

Faugère, J.-C. (2002). A new efficient algorithm for computing gröbner bases without reduction to zero (f5). In *ISSAC '02*.

Faugère, J.-C. and Joux, A. (2003). Algebraic cryptanalysis of hidden field equation (hfe) cryptosystems using gröbner bases. In *CRYPTO*.

Fraenkel, A. S. and Yesha, Y. (1979). Complexity of problems in games, graphs and algebraic equations. *Discrete Applied Mathematics*, 1(1-2):15–30.

Garey, M. R. and Johnson, D. S. (1979). Computers and intractability. *A Guide to the Theory of NP-Completeness*.

Koblitz, N., Menezes, A. J., Wu, Y.-H., and Zuccherato, R. J. (1998). *Algebraic aspects of cryptography*, volume 198. Springer.

Petzoldt, A., Ding, J., and chung Wang, L. (2016). Eliminating decryption failures from the simple matrix encryption scheme. *IACR Cryptol. ePrint Arch.*, 2016:10.

Ping, Y., Wang, B., Yang, Y., and Tian, S. (2017). Building secure public key encryption scheme from hidden field equations. *Secur. Commun. Networks*, 2017:9289410:1–9289410:6.

Smith-Tone, D. and Verbel, J. A. (2020). A rank attack against extension field cancellation. In *PQCrypto*.

Tao, C., Diene, A., Tang, S., and Ding, J. (2013). Simple matrix scheme for encryption. In *Post-Quantum Cryptography*.

Tao, C., Xiang, H., Petzoldt, A., and Ding, J. (2015). Simple matrix - a multivariate public key cryptosystem (mpkc) for encryption. *Finite Fields Their Appl.*, 35:352–368.

Wang, L.-C., Wei, T.-j., Shih, J.-M., Hu, Y.-H., and Hsieh, C.-C. (2022). An algorithm for solving over-determined multivariate quadratic systems over finite fields. *Advances in Mathematics of Communications*.