Disproving the Linearity of the Polynomials after the Pre-image Substitution in the System of the Third Attempt of MAYO

Anna Stefano Narivelomanana
annanarivelomanana07@gmail.com
Antananarivo, Madagascar

Abstract

In this work, we analyze the mathematical aspect of the MAYO signature scheme. Following the specification of MAYO, we generate the keys where the secret key is a matrix and the public key is a system of quadratic polynomial of multiple variables; then use them to sign. During the signing procedure, we disprove the claim that the polynomial only has a constant part and a linear part after sampling values for the vinegar variables. Technically, we provide the mathematical expression of an arbitrarily polynomial of the system after substitution and discover that in addition of having a constant part and a linear part, the polynomial also has a quadratic part. The quadratic state of the polynomials after substitution allows us to conclude that signing fails with the third attempt of MAYO.

Introduction

In light of the progress made in the quantum field and as a precaution against the arrival of the powerful quantum computers [14], cryptographers continously suggest different cryptographic schemes that are quantum resistant. MAYO [1] is a multivariate post-quantum signature scheme introduced by Beullens in 2021; and currently being standardized by the National Institute of Standards and Technology (NIST) [10], [13]. It originated from the oil and vinegar introduced by Pantarin in 1997 [9, 11].

Digital signatures are important in information securing and has the role of authentication which is the same as the pen-and-ink signature. In this

work, we analyze the mathematical aspect of the MAYO algorithm by following step by step the procedure according to the specification. First, we generate the secret key, which is a matrix. Next, following some steps, we expand the public key which is a system of multivariate polynomial. Next, we proceed with the signing, and finally conclude that the signing procedure has an issue and that we can not obtain a valid signature.

Preliminary

List of necessary parameters

- q: the size of the finite field $\mathbb{F}_q$
- m: the number of polynomials
- n: the number of variables
- o: the number of oils variables
- v: the number of vinegar variables with $v = n - o$

Multivariate Quadratic Problem

The word multivariate comes from "multiple" and "variable". As this indicates, we allow working on polynomials involving multiple variables where the polynomials are quadratic homogenous [3] that has the following form:

$$p(x_1, \ldots, x_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{ij} x_i x_j$$

The terms can be a multiplication of an oil variable and a vinegar variable $o_i v_j$ or two vinegar variables $v_i v_j$ but not two oil variables $o_i o_j$ [15].

Like the Original Oil and Vinegar problem [**?**] and the other current multivariate schemes like the Unbalanced Oil and Vinegar problem [16] and the Rainbow problem [17], the MAYO problem consists of finding a solution $(v_1, \ldots, v_{n-o}, o_1, \ldots, o_o)$ of a system of polynomials [12]. Here $\mathcal{P}^*$ is described in the equation (3).

Claim

According to MAYO specification [6], to solve the system of MAYO, the signer first samples values for the vinegar variables at random, and then solves for the oil variables such that the system $\mathcal{P}^*$ has became a system of m linear equations in ko variables after substituting the vinegar variables.

General Disproof

In this section, we focus on the mathematical aspect of MAYO following the specification as described in [1] and the details are given in [6].

The goal of this section is to show that all polynomials of $\mathcal{P}^*$ remain quadratic after substitution. To do so, we arbitrarily take one polynomial and show that it remains quadratic after substitution, then conclude that all the polynomials remain quadratic after substitution.

Let's first generate the secret key.

Generate the secret key

Let $\alpha_{i,j} \in \mathbb{F}_q$ for all $i, j \in [n]$ and let O the secret key which is a (n-o)-by-o matrix that we generate once at random.

$$O = \begin{pmatrix} \alpha_{o_{1,1}} & \cdots & \alpha^o_{1,o} \\ \vdots & \ddots & \vdots \\ \alpha^o_{n-o,1} & \cdots & \alpha^o_{n-o,o} \end{pmatrix}$$

Let's now generate the public key.

Let's show that p_{index}, the index-th polynomial of the system $\mathcal{P}^*$, remains quadratic after substituting the vinegar variables with the value of the pre-image.

Generate the public key

The public key is a system of m quadratic polynomials, where for an arbitrary polynomial of the system, the construction procedure follow some steps.

Let $index \in [m]$ and let's construct the polynomial p_{index}.

- **Generate** $P^{(1)}$

  $P^{(1)}$ is an upper triangular (n-o)-by-(n-o) matrix.

$$P^{(1)}_{index} = \begin{pmatrix} \alpha_{1,1} & \alpha_{1,2} & \dots & \alpha_{1,n-o} \\ 0 & \alpha_{2,2} & \dots & \alpha_{2,n-o} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & \alpha_{n-o,n-o} \end{pmatrix}$$

- **Generate** $P^{(2)}$

  $P^{(2)}$ is a (n-o)-by-o matrix. (The column iteration starts from $n-o+1$ and end until n.)

$$P^{(2)}_{index} = \begin{pmatrix} \alpha_{1,n-o+1} & \dots & \alpha_{1,n} \\ \alpha_{2,n-o+1} & \dots & \alpha_{2,n} \\ \vdots & \ddots & \vdots \\ \alpha_{n-o,n-o+1} & \dots & \alpha_{n-o,n} \end{pmatrix}$$

- **Compute** $P^{(3)}$

  $P^{(3)}$ is obtained by using the formula:

$$P^{(3)} = O^T P^{(1)}_{index} O - O^T P^{(2)}_{index}$$

  and is an upper triangular o-by-o matrix. (The row and column iterations start from $n-o+1$ and end until n.)

$$P^{(3)}_{index} = \begin{pmatrix} \alpha_{n-o+1,n-o+1} & \dots & \alpha_{n-o+1,n} \\ \alpha_{n-o+2,n-o+1} & \dots & \alpha_{n-o+2,n} \\ \vdots & \ddots & \vdots \\ \alpha_{n,n-o+1} & \dots & \alpha_{n,n} \end{pmatrix}$$

- **Build the matrix P representative of the polynomial**

  By substituting $P^{(1)}_{index}$, $P^{(2)}_{index}$ and $P^{(3)}_{index}$ in the matrice bellow,

$$P_{index} = \begin{pmatrix} P^{(1)}_{index} & P^{(2)}_{index} \\ 0 & P^{(3)}_{index} \end{pmatrix}$$

we get an upper triangular n-by-n matrix define as:

$$P_{index} = \begin{pmatrix} \alpha_{1,1} & \alpha_{1,2} & \dots & \alpha_{1,n-o} & \alpha_{1,n-o+1} & \dots & \alpha_{1,n} \\ 0 & \alpha_{2,2} & \dots & \alpha_{2,n-o} & \alpha_{2,n-o+1} & \dots & \alpha_{2,n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \alpha_{n-o,n-o} & \alpha_{n-o,n-o+1} & \dots & \alpha_{n-o,n} \\ \vdots & \ddots & \ddots & 0 & \alpha_{n-o+1,n-o+1} & \dots & \alpha_{n-o+1,n} \\ \vdots & \ddots & \ddots & \ddots & 0 & \dots & \alpha_{n-o+2,n} \\ \vdots & \ddots & \ddots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & \dots & \dots & 0 & 0 & \alpha_{n,n} \end{pmatrix}$$

- **Construct the polynomial p of the basic system $\mathcal{P}$**

Let $x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ the vector representative of the variables and let's construct the quadratic polynomial using the formula:

$$p_{index}(x) = x^T P_{index} x \tag{1}$$

We get:

$$p_{index}(x) = \alpha_{1,1}x_1^2 + \alpha_{1,2}x_1x_2 + \dots + \alpha_{n-o,n}x_{n-o}x_n + \alpha_{n-o+1,n-o+1}x_{n-o+1}^2 + \\ \dots + \alpha_{n-1,n}x_{n-1}x_n + \alpha_{n,n}x_n^2$$

that can be written in a general formula:

$$p_{index}(x) = \sum_{A=1}^{n}\sum_{B=A}^{n} \alpha_{A,B}x_Ax_B \tag{2}$$

- **Construct the polynomial of the system of MAYO**

Let $\mathcal{P}$ the system of quadratic polynomials where each polynomial p_{index} for $index \in [m]$ has the form describe in the above equation (2):

$$\mathcal{P}(x) = \begin{cases} p_1(x) \\ \vdots \\ p_m(x) \end{cases}$$

The MAYO signature scheme involves a system of polynomial denoted $\mathcal{P}^*$ that has the form:

$$\mathcal{P}^*(X_1, \ldots, X_k) = \sum_{i=1}^{k} E_{ii}\mathcal{P}(X_i) + \sum_{i=1}^{k}\sum_{j=i+1}^{k} E_{ij}\mathcal{P}'(X_i, X_j) \qquad (3)$$

where k is a parameter that multiplies the number of variables in order to make the system k time larger, the E_{ii}-s and E_{ij}-s are m-by-m matrices in $\mathbb{F}_q$, and $\mathcal{P}'(x, y)$ is the differential of $\mathcal{P}$ define as:

$$\mathcal{P}'(x, y) := \mathcal{P}(x + y) - \mathcal{P}(x) - \mathcal{P}(y).$$

Compute the representative vector of the first part of the MAYO system

Let $i \in [k]$, and let the matrix E_{ii} define as:

$$E_{ii} = \begin{pmatrix} e^i_{11} & \cdots & e^i_{1m} \\ \vdots & \ddots & \vdots \\ e^i_{m1} & \cdots & e^i_{mm} \end{pmatrix}$$

Let $\mathcal{P}(X_i)$ the vector representation of the system $\mathcal{P}$ as a function of the variable X_i. Let's compute the matrix representation of the system $E_{ii}\mathcal{P}(X_i)$ for i in $[k]$,

$$E_{ii}\mathcal{P}(X_i) = \begin{pmatrix} e^i_{11} & \cdots & e^i_{1m} \\ \vdots & \ddots & \vdots \\ e^i_{m1} & \cdots & e^i_{mm} \end{pmatrix} \begin{pmatrix} p_1(X_i) \\ \vdots \\ p_m(X_i) \end{pmatrix}$$

$$E_{ii}\mathcal{P}(X_i) = \begin{pmatrix} e^i_{11}p_1(X_i) + \cdots + e^i_{1m}p_m(X_i) \\ \vdots \\ e^i_{m1}p_1(X_i) + \cdots + e^i_{mm}p_m(X_i) \end{pmatrix}$$

In the same way, let's compute the matrix representative of the system $E_{ij}\mathcal{P}'(X_i, X_j)$ for i, j in $[k]$,

Construct the polynomial p' of the differential system $\mathcal{P}'$

Let $X_i = \begin{pmatrix} x_1^i \\ x_2^i \\ \vdots \\ x_n^i \end{pmatrix}$ and $X_j = \begin{pmatrix} x_1^j \\ x_2^j \\ \vdots \\ x_n^j \end{pmatrix}$ the representative vectors of two variables. As the representative vector of their sum, we have $X_i + X_j = \begin{pmatrix} x_1^i + x_1^j \\ x_2^i + x_2^j \\ \vdots \\ x_n^i + x_n^j \end{pmatrix}$.

Let $\mathcal{P}(X_i + X_j)$ the system of quadratic polynomials where each polynomial $p_{index}(X_i + X_j)$ has the form as describe in equation 2. We have:

$$\mathcal{P}(X_i + X_j) = \begin{cases} p_1(X_i + X_j) \\ \vdots \\ p_m(X_i + X_j) \end{cases}$$

Let's recall that $p_{index}(X_i + X_j)$ is obtained by using the formula in (1):

$$p_{index}(X_i + X_j) = (X_i + X_j)^T P_{index}(X_i + X_j)$$

We get:

$$\begin{aligned} p_{index}(X_i + X_j) = {} & \alpha_{1,1}(x_1^i + x_1^j)^2 + \alpha_{1,2}(x_1^i + x_1^j)(x_2^i + x_2^j) + \cdots + \\ & \alpha_{n-o+1,n-o+1}(x_{n-o+1}^i + x_{n-o+1}^j)^2 + \cdots + \alpha_{n-1,n}(x_{n-1}^i + \\ & x_{n-1}^j)(x_n^i + x_n^j) + \alpha_{n,n}(x_n^i + x_n^j)^2 \end{aligned}$$

$$\begin{aligned} p_{index}(X_i + X_j) = {} & \alpha_{1,1}(x_1^i)^2 + \alpha_{1,1}(x_1^j)^2 + \alpha_{1,2}x_1^i x_2^i + \alpha_{1,2}x_1^i x_2^j + \alpha_{1,2}x_1^j x_2^i + \\ & \alpha_{1,2}x_2^j x_2^j + \cdots + \alpha_{n-o+1,n-o+1}(x_{n-o+1}^i)^2 + \alpha_{n-o+1,n-o+1}(x_{n-o+1}^j)^2 + \\ & \cdots + \alpha_{n-1,n}x_{n-1}^i x_n^i + \alpha_{n-1,n}x_{n-1}^i x_n^j + \alpha_{n-1,n}x_{n-1}^j x_n^i + \\ & \alpha_{n-1,n}x_{n-1}^j x_n^j + \alpha_{n,n}(x_n^i)^2 + \alpha_{n,n}(x_n^j)^2 \end{aligned}$$

In the same way, using the formula in equation (1), we can obtain the expression of the polynomials $p_{index}(X_i)$ and $p_{index}(X_j)$. We can now compute $p'_{index}(X_i, X_j)$ using the formula of the differential of p. We have:

$$\begin{aligned} p'_{index}(X_i, X_j) &= p_{index}(X_i + X_j) - p_{index}(X_i) - p_{index}(X_j) \\ &= \alpha_{1,2}x_1^i x_2^j + \alpha_{1,2}x_1^j x_2^i + \cdots + \cdots + \alpha_{n-1,n}x_{n-1}^i x_n^j + \alpha_{n-1,n}x_{n-1}^j x_n^i \end{aligned}$$

That can be written a general way:

$$p'_{index}(X_i, X_j) = \sum_{A=1}^{n-1} \sum_{B=A+1}^{n} (\alpha_{A,B}x_A^i, x_B^j + \alpha_{A,B}x_A^j x_B^i) \tag{4}$$

Compute the representative vector of the second part of the MAYO system

Let i and j in $[k]$, and let the matrix E_{ij}

$$E_{ij} = \begin{pmatrix} e_{11}^{ij} & \cdots & e_{1m}^{ij} \\ \vdots & \ddots & \vdots \\ e_{m1}^{ij} & \cdots & e_{mm}^{ij} \end{pmatrix}$$

Let's compute the system matrix $E_{ij}\mathcal{P}'(X_i, X_j)$ for i, j in $[k]$,

$$E_{ij}\mathcal{P}'(X_i, X_j) = \begin{pmatrix} e_{11}^{ij} & \cdots & e_{1m}^{ij} \\ \vdots & \ddots & \vdots \\ e_{m1}^{ij} & \cdots & e_{mm}^{ij} \end{pmatrix} \begin{pmatrix} p'_1(X_i, X_j) \\ \vdots \\ p'_m(X_i, X_j) \end{pmatrix}$$

$$E_{ij}\mathcal{P}'(X_i, X_j) = \begin{pmatrix} e_{11}^{ij}p'_1(X_i, X_j) + \cdots + e_{1m}^{ij}p_m(X_i, X_j) \\ \vdots \\ e_{m1}^{ij}p'_1(X_i, X_j) + \cdots + e_{mm}^{ij}p'_m(X_i, X_j) \end{pmatrix}$$

Construction of the polynomial of MAYO

Since the system of MAYO is describe as:

$$\mathcal{P}^*(X_1,\ldots,X_k) = \sum_{i=1}^{k} E_{ii}\mathcal{P}(X_i) + \sum_{i=1}^{k}\sum_{j=i+1}^{k} E_{ij}\mathcal{P}'(X_i,X_j)$$

By substituting $E_{ii}\mathcal{P}(X_i)$ and $E_{ij}\mathcal{P}'(X_i,X_j)$, we can get the vector representative of the system $\mathcal{P}^*(X_1,\ldots,X_k)$ define with the formula:

$$\begin{aligned}\mathcal{P}^*(X_1,\ldots,X_k) = &\sum_{i=1}^{k}\begin{pmatrix} e^i_{11}p_1(X_i)+\cdots+e^i_{1m}p_m(X_i)\\ \vdots \\ e^i_{m1}p_1(X_i)+\cdots+e^i_{mm}p_m(X_i)\end{pmatrix}\\ &+\sum_{i=1}^{k}\sum_{j=i+1}^{k}\begin{pmatrix} e^{ij}_{11}p'_1(X_i,X_j)+\cdots+e^{ij}_{1m}p'_m(X_i,X_j)\\ \vdots \\ e^{ij}_{m1}p'_1(X_i,X_j)+\cdots+e^{ij}_{mm}p'_m(X_i,X_j)\end{pmatrix}\end{aligned}$$

In the following, we focus on two iteration $i \in [k]$ and $j \in [k]$,where $j > i$, in order to have the expression of the polynomial in function of two arbitrarily variables X_i and X_j which are independent from all the other variables of the big polynomial.

Let $index \in [m]$. Let's see the detailed expression of the polynomial $p^*_{index}(X_1,\ldots,X_k)$. We have:

$$\begin{aligned}p^*_{index}(X_1,\ldots,X_k) = &\sum_{i=1}^{k}(e^i_{index\,1}p_1(X_i)+\cdots+e^i_{index\,m}p_m(X_i))\\ &+\sum_{i=1}^{k}\sum_{j=i+1}^{k}(e^{ij}_{index\,1}p'_1(X_i,X_j)+\cdots+e^{ij}_{index\,m}p'_m(X_i,X_j))\end{aligned}$$

$p^*_{index}(X_1, \ldots, X_k)$ is a polynomial of multiple variables. Let's see that for $i, j \in [k]$, a part of p^*_{index} remains quadratic after substitution.

Let's denote by $E^{index}_{ii} p_{index}$ and $E^{index}_{ij} p'_{index}$ the expressions:

$$E^{index}_{ii} p_{index}(X_i) = e^i_{index\,1} p_1(X_i) + \cdots + e^i_{index\,m} p_m(X_i)$$
$$E^{index}_{ij} p'_{index}(X_i, X_j) = e^{ij}_{index\,1} p'_1(X_i, X_j) + \cdots + e^{ij}_{index\,m} p'_m(X_i, X_j)$$

We get the expression of the index-th polynomial of the system $\mathcal{P}^*$:

$$p^*_{index}(X_1, \ldots, X_k) = \sum_{i=1}^{k} E^{index}_{ii} p_{index}(X_i) + \sum_{i=1}^{k} \sum_{j=i+1}^{k} E^{index}_{ij} p'_{index}(X_i, X_j) \tag{5}$$

Let $i \in [k]$ and $j \in [k]$. Let's see the expression of $E^{index}_{ii} p_{index}$ in function of the variable X_i and the expression of $E^{index}_{ij} p'_{index}$ in function of the variables X_i and X_j.

By substituting each polynomial of $E^{index}_{ii} p_{index}$ with the formula in (2) and each polynomial of $E^{index}_{ij} p'_{index}$ with the formula in (4); and using the variables X_i and X_j, we have:

$$E^{index}_{ii} p_{index}(X_i) = e^i_{index\,1} \sum_{A=1}^{n} \sum_{B=A}^{n} \alpha^1_{A,B} x^i_A x^i_B + \cdots + e^i_{index\,m} \sum_{A=1}^{n} \sum_{B=A}^{n} \alpha^m_{A,B} x^i_A x^i_B$$

and:

$$E^{index}_{ij} p'_{index}(X_i, X_j) = e^{ij}_{index\,1} \sum_{A=1}^{n-1} \sum_{B=A+1}^{n} (\alpha^1_{A,B} x^i_A x^j_B + \alpha^1_{A,B} x^j_A x^i_B) + \cdots +$$
$$e^{ij}_{index\,m} \sum_{A=1}^{n-1} \sum_{B=A+1}^{n} (\alpha^m_{A,B} x^i_A x^j_B + \alpha^m_{A,B} x^j_A x^i_B)$$

That can be written in simplified expressions:

$$E_{ii}^{index} p_{index}(X_i) = \sum_{A=1}^{n} \sum_{B=A}^{n} \left(e_{index1}^{i} \alpha_{A,B}^{1} + \cdots + e_{index\,m}^{i} \alpha_{A,B}^{m} \right) x_A^i x_B^i$$

and:

$$E_{ij}^{index} p'_{index}(X_i, X_j) = \sum_{A=1}^{n-1} \sum_{B=A+1}^{n} (e_{index1}^{ij} \alpha_{A,B}^{1} + \cdots + e_{index\,m}^{ij} \alpha_{A,B}^{m})(x_A^i x_B^j + x_A^j x_B^i)$$

By substituting $E_{ii}^{index} p_{index}(X_i)$ and $E_{ij}^{index} p'_{index}(X_i, X_j)$ respectively with the above aquations in the equation (5), we have the expression of the polynomial of the MAYO system as a function of X_i for $i \in \{1, \ldots, k\}$:

$$p^*_{index}(X_1, \ldots, X_k) = \sum_{i=1}^{k} \sum_{A=1}^{n} \sum_{B=A}^{n} \left(e_{index1}^{i} \alpha_{A,B}^{1} + \cdots + e_{index\,m}^{i} \alpha_{A,B}^{m} \right) x_A^i x_B^i$$
$$+ \sum_{i=1}^{k} \sum_{j=i+1}^{k} \sum_{A=1}^{n-1} \sum_{B=A+1}^{n} (e_{index1}^{ij} \alpha_{A,B}^{1} + \cdots + e_{index\,m}^{ij} \alpha_{A,B}^{m})(x_A^i x_B^j + x_A^j x_B^i)$$

Signing

Let $\mathcal{O}$ the vector space containing all the column vectors of the secret key O. Let $\omega^i = (\omega_1^i, \omega_2^i, \ldots, \omega_{n-o-1}^i, \omega_{n-o}^i)$ and $\omega^j = (\omega_1^j, \omega_2^j, \ldots, \omega_{n-o-1}^j, \omega_{n-o}^j)$ two vectors of $\mathcal{O}$, and let's substitute $X_i^{1 \to n-o} = (x_1^i, x_2^i, \ldots, x_{n-o-1}^i, x_{n-o}^i)$ with ω^i and $X_j^{1 \to n-o} = (x_1^j, x_2^j, \ldots, x_{n-o-1}^j, x_{n-o}^j)$ with ω^j.

After substitution we get:

$$E_{ii} p_{index}(\omega^i) = \sum_{A=1}^{n-o} \sum_{B=A}^{n-o} \left(e_{index1}^{i} \alpha_{A,B}^{1} + \cdots + e_{index\,m}^{i} \alpha_{A,B}^{m} \right) \omega_A^i \omega_B^i + \sum_{A=1}^{n-o} \sum_{B=n-o+1}^{n} (e_{index1}^{i} \alpha_{A,B}^{1} +$$
$$\cdots + e_{index\,m}^{i} \alpha_{A,B}^{m}) \omega_A^i x_B^i + \sum_{A=1}^{n-o+1} \sum_{B=A}^{n} \left(e_{index1}^{i} \alpha_{A,B}^{1} + \cdots + e_{index\,m}^{i} \alpha_{A,B}^{m} \right) x_A^i x_B^i \tag{6}$$

and:

$$E_{ij}p'_{index}(\omega^i,\omega^j) = \sum_{A=1}^{n-o}\sum_{B=A+1}^{n-o}(e^{ij}_{index1}\alpha^1_{A,B}+\cdots+e^{ij}_{index\,m}\alpha^m_{A,B})(\omega^i_A\omega^j_B+\omega^j_A\omega^i_B)+$$
$$\sum_{A=1}^{n-1}\sum_{B=A+1}^{n}(e^{ij}_{index1}\alpha^1_{A,B}+\cdots+e^{ij}_{index\,m}\alpha^m_{A,B})(\omega^i_Ax^j_B+\omega^j_Ax^i_B)+$$
$$\sum_{A=1}^{n-1}\sum_{B=A+1}^{n}(e^{ij}_{index1}\alpha^1_{A,B}+\cdots+e^{ij}_{index\,m}\alpha^m_{A,B})(x^i_Ax^j_B+x^j_Ax^i_B) \tag{7}$$

We can see that the sum of the terms from $A = n-o+1$ of both equations (6) and (7) remain quadratic.

If we take (5) and substitute with the values of the equations (6) and (7), we have the expression of one arbitrarily polynomial p^*_{index} of the system $\mathcal{P}^*$ after substitution.

$$p^*_{index}(\omega) = \sum_{i=1}^{k}\sum_{A=1}^{n-o}\sum_{B=A}^{n-o}\left(e^i_{index1}\alpha^1_{A,B}+\cdots+e^i_{index\,m}\alpha^m_{A,B}\right)\omega^i_A\omega^i_B +$$
$$\sum_{i=1}^{k}\sum_{j=i+1}^{k}\sum_{A=1}^{n-o}\sum_{B=A+1}^{n-o}(e^{ij}_{index1}\alpha^1_{A,B}+\cdots+e^{ij}_{index\,m}\alpha^m_{A,B})(\omega^i_A\omega^j_B+\omega^j_A\omega^i_B) \quad \text{(constant)} \quad +$$

$$\sum_{i=1}^{k}\sum_{A=1}^{n-o}\sum_{B=n-o+1}^{n}(e^i_{index1}\alpha^1_{A,B}+\cdots+e^i_{index\,m}\alpha^m_{A,B})\omega^i_Ax^i_B+\sum_{i=1}^{k}\sum_{j=i+1}^{k}\sum_{A=1}^{n-o}\sum_{B=n-o+1}^{n}(e^{ij}_{index1}\alpha^1_{A,B}+$$
$$\cdots+e^{ij}_{index\,m}\alpha^m_{A,B})(\omega^i_Ax^j_B+\omega^j_Ax^i_B) \quad \text{(linear)} \quad +$$

$$\sum_{i=1}^{k}\sum_{A=n-o+1}^{n}\sum_{B=A}^{n}(e^i_{index1}\alpha^1_{A,B}+\cdots+e^i_{index\,m}\alpha^m_{A,B})x^i_Ax^i_B+\sum_{i=1}^{k}\sum_{j=i+1}^{k}\sum_{A=n-o+1}^{n-1}\sum_{B=A+1}^{n}(e^{ij}_{index1}\alpha^1_{A,B}+$$
$$\cdots+e^{ij}_{index\,m}\alpha^m_{A,B})(x^i_Ax^j_B+x^j_Ax^i_B) \quad \text{(quadratic)}$$

The expression of the equation $p^*_{index}(\omega)$ above disproves that an arbitrarily polynomial of the system of MAYO is linear after substitution [4]. In addition to having a constant and a linear part, the polynomials of the

system of MAYO also have a quadratic part.

As a conclusion, for all $index \in [m]$, the polynomial $p^*_{index}(X_1, \ldots, X_k)$ of the system of MAYO is not linear after substitution.

Consequence

The fact that we don't have linear polynomials after subtitution has an impact on the global specification of the algorithm.

Signing fails. According to the specification of MAYO, signing basically means solving the system of polynomial in such a way that we have a signature s satisfying $\mathcal{P}^*(s) = t$. Since we have non-linear polynomials after substitution, then the resolution of a linear system $Ax = y$ described in the MAYO.Sign algorithm of the MAYO specification and the algorithm proposed by Hashimoto [2], the Gröbner Bases [7], the Hybrid Approach [8], and all the other existing algorithm to solve multivariate systems over finite fields can not allow us to have a valid signature.

Conclusion

To concude, we proved in this work that the third attempt version of MAYO has an algorithmic mistake. When algorithmically analyzing the MAYO signing algorithm, we discovered that the polynomials of the system $\mathcal{P}^*$ are not linear after substituting the vinegar variables with the values of the preimage.

This work opens some problems:

Problem 1: The verify functions of the C and Sage implemented versions of MAYO currently work. The question is why? What other mistakes can we find? The implementation procedure of the MAYO algorithm is open to analysis.

Poblem 2: Since the system resolution procedure define in the signing algorithm of the current version of MAYO is designed for a system of linear polynomials, that state is open to resolution ideas. What can we do to fix that matter of MAYO?

References

[1] Ward Beullens. *MAYO: Practical Post-Quantum Signatures from Oil-and-Vinegar Maps*. Cryptology ePrint Archive, Paper 2021/1144. https://eprint.iacr.org/2021/1144.pdf (2021).

[2] Yasufumi Hashimoto. *An Improvement of Algorithms to Solve Under-Defined Systems of Multivariate Quadratic Equations*. Cryptology ePrint Archive, Paper 2021/1045. https://eprint.iacr.org/2021/1045.pdf (2021).

[3] Enrico Thomae and Christopher Wolf. *Solving Underdetermined Systems of Multivariate Quadratic Equations Revisited*. In: Public Key Cryptography - PKC 2012. Springer, vol. 7293, pp. 156-171. https://www.iacr.org/archive/pkc2012/72930159/72930159.pdf (2012).

[4] Florian Hirner, Michael Streibl, Florian Krieger, Ahmet Can Mert, and Sujoy Sinha Roy. *Whipping the MAYO Signature Scheme using Hardde Platforms*. Cryptology ePrint Archive, Paper 2023/1267. https://eprint.iacr.org/2023/1267.pdf (2023).

[5] Douglas R. Stinson and Maura B. Paterson. *Cryptography: Theory and Practice*. CRC Press, (2018).

[6] W. Beullens, F. Campos, S. Celi, B. Hess and M. J. Kannwischer. *MAYO*. https://pqmayo.org/assets/specs/mayo-round2.pdf, (accessed: September 2025).

[7] Jean-Charles Faugère. *A New Efficient Algorithm for Computing Gröbner Bases (F4)*. Journal of Pure and Applied Algebra, **139**(1):61-88, 1999. https://www.sciencedirect.com/science/article/pii/S0022404999000055 (DOI: https://doi.org/10.1016/S0022-4049(99)00005-5).

[8] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. *Solving Polynomial Systems over Finite Fields: Improved Analysis of the Hybrid Approach*. In: Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC), July 2012, pp. 67-74. DOI: https://inria.hal.science/hal-00776070/document.

[9] Aviad Kipnis, Jacques Patarin, and Louis Goubin. *Unbalanced Oil and Vinegar Signature Schemes*. In: Advances in Cryptology — EUROCRYPT '99, editor Jacques Stern. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 206-222, 1999. ISBN: 978-3-540-48910-8.

[10] NIST. *NIST Announces 14 Candidates to Advance to the Second Round of the Additional Digital Signatures for the Post-Quantum Cryptography Standardization Process*. 2024. URL: https://csrc.nist.gov/News/2024/pqc-digital-signature-second-round-announcement, Accessed: 2025-09-13.

[11] Jacques Patarin. *The Oil and Vinegar Signature Scheme*. In: Dagstuhl Workshop on Cryptography, September 1997.

[12] Ward Beullens. *Mayo: Practical Post-quantum Signatures from Oil-and-Vinegar Maps*. URL: https://www.youtube.com/watch?v=mgW-waIhPf0, Note: September 2021.

[13] NIST. *Round 1 Additional Signatures - Post-Quantum Cryptography: Digital Signature Schemes: Csrc*. Jun 2023. URL: https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures, Accessed: 2025-09-15.

[14] Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, and Audun Jøsang. *The Impact of Quantum Computing on Present Cryptography*. CoRR, abs/1804.00200, Jun 2018. URL: https://arxiv.org/pdf/1804.00200.

[15] Smarkelon. *Demystifying Multivariate Cryptography*. NCC, 2023. URL: https://www.nccgroup.com/research-blog/demystifying-multivariate-cryptography/, Accessed: 2025-09-18.

[16] W. Beullens, M.-S. Chen, J. Ding, B. Gong, M. J. Kannwischer, J. Patarin, B.-Y. Peng, D. Schmidt, C.-J. Shih, C. Tao, and B.-Y. Yang. *UOV: Unbalanced Oil and Vinegar. Algorithm Specifications and Supporting Documentation, Version 2.0*. 2025.

[17] Jintai Ding and Dieter Schmidt. *Rainbow, a New Multivariable Polynomial Signature Scheme*. In: Applied Cryptography and Network Security, editor John Ioannidis, Angelos Keromytis, and Moti Yung. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 164-175, 2005. ISBN: 978-3-540-31542-1.