A Multivariate Signature Based On Block Matrix Multiplication

Adama Diene[1], Shaima Thabet, Yahya Yusuf

Department of Math. Sciences, UAE University - Al-Ain, United Arab Emirates

Abstract

An oil and vinegar scheme is a signature scheme based on multivariate quadratic polynomials over finite fields. The system of polynomials contains n variables, divided into two groups: v vinegar variables and o oil variables. The scheme is called balanced (OV) or unbalanced (UOV), depending on whether $v = 0$ or not, respectively. These schemes are very fast and require modest computational resources, which make them ideal for low-cost devices such as smart cards. However, the OV scheme has been already proven to be insecure and the UOV scheme has been proven to be very vulnerable for many parameter choices. In this paper, we propose a new multivariate public key signature whose central map consists of a set of polynomials obtained from the multiplication of block matrices. Our construction is motivated by the design of the Simple Matrix Scheme for Encryption and the UOV scheme. We show that it is secure against the Separation Method, which can be used to attack the UOV scheme, and against the Rank Attack, which is one of the deadliest attacks against multivariate public key cryptosystems. Some theoretical results on matrices with polynomial entries are also given, to support the construction of the scheme.

Keywords: Multivariate Public Key Cryptosystem, Random polynomial, Oil Vinegar signature, Provable Security

1. Introduction

Multivariate public key cryptosystems (MPKCs) were first introduced in 1988 by Matsumoto and Imai [1] with their scheme, called C* or MI. The

[1] Corresponding Author

doi:10.20944/preprints202004.0392.v1

public key of an MPKC is a system of multivariate polynomials—mostly quadratic—over a finite field. In general, the structure of an MPKC can be described, as follows.
Let k be a finite field with q elements. A public key is a map
$\bar{F} : k^n \to k^m$, which is constructed as $\bar{F} = \mathcal{L}_1 \circ F \circ \mathcal{L}_2$, where $\mathcal{L}_1$ and $\mathcal{L}_2$ are two random invertible affine transformations over k^n and k^m, respectively. The central map $F : k^n \to k^m$ is a non-linear multivariate polynomial map which has the property of being easily invertible (i.e., computationally). The key to building a good MPKC is to find a good polynomial system F which makes the cryptosystem secure.

The security of an MPKC is based on the fact that solving a set of multivariate polynomial equations over a finite field, in general, has been proven to be an NP-hard problem [2]. However, this does not guarantee that MPKCs are secure. Nevertheless, this property makes the family of MPKCs a good candidate for the Post Quantum Cryptography (PQC) era, if well designed. On the other hand, due to Shor's algorithm [3], the well-known number theoretic-based cryptosystems(e.g., RSA, ECC, and the Diffie–Hellman key exchange scheme) have been proven to be insecure if a quantum computer is built.

These facts have inspired many researchers to become involved in the area of MPKCs, which underwent very fast development in the late 1990s. Since then, there have been many attempts to build MPKCs. Unfortunately, most of the existing MPKCs have problems, due to the facts that randomness has not been well-used and that cryptanalysts usually exploit the structure of the family of polynomials involved to attack the MPKCs (see [4, 5, 6, 7, 8, 1, 1, 1, 1]). Direct attacks using algorithms to solve the multivariate systems are also often used to attack MPKCs [1, 1, 1, 1, 1, 1]. As mentioned in [1], the deadliest attacks for MPKCs are Rank attacks [8], which consist of finding some quadratic forms with low rank associated with the central map. Even if the parameters are carefully chosen, there still exist few successful designs, such as the Rainbow scheme proposed by Ding and Schmidt [2, 2], the Simple Matrix Scheme for Encryption [1], and the HFEv^- [2, 2, 2]. Indeed, this work was mostly inspired by the constructions in [1, 2]. We use the multiplication of block matrices to design our new proposed scheme. The arguments that prove its security are very similar to those used in [1, 2].

The rest of this paper is organized as follows. We recall the description of a UOV scheme from [2, 2] in Section 2. In Section 3, we introduce some theoretical groundwork concerning matrices with polynomial entries. These results support the construction of the new proposed scheme, which is introduced in the second part of Section 3. Section 4 discusses the security of our scheme and Section 5 concludes the paper.

2. Preliminaries

The initial Oil and Vinegar scheme was defeated with the separation method attack. However, a huge number of multivariate schemes have been proven to be vulnerable to the MinRank attack. In this section, we recall the descriptions of these two algebraic attacks. A short description of the UOV scheme is also given.

2.1. Multivariate Public Key Cryptosystems and UOV Scheme

2.1.1. Multivariate Public Key Cryptosystems

The main characteristic of a Multivariate public-key cryptosystem is that its public keys consist of a set of non-linear algebraic polynomials

$$p = (p_1(x_1, ..., x_n), ..., p_m(x_1, ..., x_n)) \in k[x_1, ..., x_n]^m.$$

To encrypt a message or to verify a signature, one needs only to evaluate this set of polynomials at a given point $(a_1, ..., a_n)$. Decryption and signing are done with the help of the private key by solving the system

$$p_1(z_1, ..., z_n) = 0, ..., p_m(z_1, ..., z_n) = 0. \tag{1}$$

However, without the private key, solving the system should be impossible (or, at least, very hard) to ensure the security of the cryptosystem. To build a secure system, we start by very carefully choosing a trapdoor

$$f(x) = (f_1(x_1, ..., x_n), ..., f_m(x_1, ..., x_n)) \in k[x_1, ..., x_n]^m,$$

which is easy to solve. That is, given $y = (y_1, ..., y_m) \in k^m$, we have an efficient method for computing the solutions of

$$f_1(x_1, ..., x_n) = y_1, ..., f_m(x_1, ..., x_n) = y_m.$$

doi:10.20944/preprints202004.0392.v1

Then, denoting by $GL_i(k)$ the set of all $i \times i$ invertible matrices with entries in k, we choose $(\mathcal{L}_1, \mathcal{L}_2) \in GL_m(k) \times GL_n(k)$ and compose f with $\mathcal{L}_1$ and $\mathcal{L}_2$ from the left and right, respectively, to obtain

$$p = (f_1(x \cdot \mathcal{L}_2), \ldots, f_m(x \cdot \mathcal{L}_2)) \cdot \mathcal{L}_1 = (p_1(x), \ldots, p_m(x)), \tag{2}$$

where $x = (x_1, ..., x_n)$.

In some cases, $\mathcal{L}_1$ or $\mathcal{L}_2$ may be the identity of $GL_m(k)$ or $GL_n(k)$, respectively. The private key of these systems consists of $(\mathcal{L}_1, \mathcal{L}_2) \in GL_m(k) \times GL_n(k)$ and the polynomial $f_1, \ldots, f_m$, while the public key consists of the field k and the set of algebraic polynomials:
$p = (p_1(x_1, ..., x_n), ..., p_m(x_1, ..., x_n)) \in k[x_1, ..., x_n]^m$ mentioned above.

2.1.2. Oil and Vinegar Polynomials

In this subsection, we give a quick description of the Unbalanced Oil and Vinegar (UOV) scheme and its known cryptanalysis, for illustrative purposes. The basic building block for an OV or UOV scheme is the Oil and Vinegar polynomial.

An Oil and Vinegar polynomial is a quadratic multivariate polynomial with $o + v = n$ variables, where o represents the number of oil variables and v the number of vinegar variables. The non-linear terms appear only in the following two cases: between vinegar variables, or with one vinegar variable and one oil variable. In other words, there is no quadratic term with oil variables only.
More precisely, let k be a finite field with q elements, $x_1, x_2, ..., x_o$ be the o oil variables, and $x'_1, x'_2, ..., x'_v$ be the v vinegar variables. An Oil and Vinegar polynomial is any (total degree two) polynomial $f \in k[x_1, ..., x_o, x'_1, x'_2, ..., x'_v]$ of the form

$$f = \sum_{i=1}^{o}\sum_{j=1}^{v} a_{ij}x_i x'_j + \sum_{i=1}^{v}\sum_{j=i}^{v} b_{ij}x'_i x'_j + \sum_{i=1}^{o} c_i x_i + \sum_{j=1}^{v} d_j x'_j + e, \tag{3}$$

where $a_{ij}, b_{ij}, c_i, d_j, e \in k$.

2.1.3. Oil and Vinegar map and scheme

Let $F : k^n \longrightarrow k^o$ be a polynomial map of the form

$$F(x_1, ..., x_o, x'_1, ..., x'_v) = (f_1(x_1, ..., x_o, x'_1, ..., x'_v), ...f_o(x_1, ..., x_o, x'_1, ..., x'_v)),$$

where $f_1, f_2, ...f_o \in k[x_1, x_2, ..., x_o, x'_1, x'_2, ..., x'_v]$ are Oil and Vinegar polynomials. Then, F is called an Oil and Vinegar map.

The trapdoor for an OV or UOV scheme is a set of Oil and Vinegar polynomial maps, where the public key is a map

$$p = (p_1(x), \ldots, p_o(x)) = (f_1(x \cdot \mathcal{L}_2), \ldots, f_o(x \cdot \mathcal{L}_2)).$$

In the context described above, $\mathcal{L}_1$ is the identity of $GL_o(k)$ and composition by $\mathcal{L}_2 \in GL_n(k)$ is carried out to mix the oil and vinegar variables. The private key is $\mathcal{L}_2$ and the central map is F. For the OV and UOV schemes, there is no need to use a second linear transformation $\mathcal{L}_1$. These schemes are designed only for the signature.

To sign a message $y = (y_1, y_2, ..., y_o)$, we need to find a vector $w = (w_1, w_2, ..., w_n)$ such that $p(w) = y$. To do so, we first choose v random values for the vinegar variables $x'_1, x'_2, ..., x'_v$ and substitute them into the system to obtain o linear equations in the o variables $x_1, x_2, ..., x_o$. This linear system has a high probability of having a solution. If it does not, we change the values of the vinegar variables $x'_1, x'_2, ..., x'_v$ and try again until a solution in k^o is found. Then, we apply $\mathcal{L}_2^{-1} \in GL_n(k)$.

To verify whether w is a signature for y, it suffices to check that $p(w) = y$.

2.2. Attacks against the UOV Scheme

In this subsection, we present two of the most well-known attacks against the UOV scheme; namely, the Separation Method attack and the MinRank attack, which was performed for the first time on the HFE scheme.

2.2.1. Separation Method Attack

The separation attack was introduced by Kipnis and Shamir [8], in order to defeat the original Oil and Vinegar scheme. It has been extended to many other systems containing two different sets of variables. The idea consists of finding an invariant subspace of the subspace spanned by the n polynomials of the public key. This invariant subspace represents the Oil subspace and its complement is the Vinegar subspace. Once this separation is done, one can easily forge arbitrary signatures.

2.2.2. MinRank attack

As mentioned earlier, one of the deadliest attacks against multivariate public key cryptosystems is the MinRank attack, which is an attack based on the MinRank problem. This problem can be formulated as follows:
Given positive integers N, n, r with $r \leq n$ and N matrices $M_1, ..., M_N$ of dimension $n \times n$, find a non-trivial linear combination M of $M_1, M_2, ..., M_N$ such that $Rank(M) \leq r$.
If $r = n - 1$, the MinRank problem has been proven to be NP-complete. However, for small r, it may be easily solvable. Therefore, all MPKCs which have the property that some quadratic form associated to their central maps has a low rank are vulnerable to this attack. We give an illustration by describing the MinRank attack on the HFE scheme [2]. The attack was first performed by Kipnis and Shamir [8], who showed that the security of HFE can be reduced to a MinRank problem.

2.2.3. The HFE Scheme

The HFE cryptosystem was proposed by Jacques Patarin in [2]. It can be described as follows: Let $q = p^e$, where p is a prime number and $e \geq 1$. Let K be an extension of degree n of the finite field $k = \mathbb{F}_q$. Clearly, $K \cong k^n$.

Let $\phi : K \to k^n$ be a k-linear isomorphism map between the finite field K and the n-dimensional vector space k^n. The central map of HFE is a univariate polynomial $F(x)$ of the following form

$$F(x) = \sum_{i=0}^{r-1} \sum_{j=0}^{r-1} \alpha_{ij} x^{q^i + q^j} + \sum_{i=0}^{r-1} \beta_i x^{q^i} + \gamma \in K[x], \tag{4}$$

where $\alpha_{ij}, \beta_i, \gamma \in K$ and r is a small constant, chosen in a way such that $F(x)$ can be efficiently inverted. The public key is given by

$$P = T \circ \phi \circ F \circ \phi^{-1} \circ S,$$

where $T : k^n \longrightarrow k^n$ and $S : k^n \longrightarrow k^n$ are two invertible linear transformations and the private key consists of T, F, and S.

2.2.4. MinRank Attack on HFE

In [8], Kipnis and Shamir showed that an attacker can ignore lower degree monomials and still be able to recover the key. Furthermore, the public key P and the transformations S, T, T^{-1} satisfy the following theorem.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 22 April 2020 doi:10.20944/preprints202004.0392.v1

Theorem 1. *For the maps S, T, T^{-1} given in the HFE, there exist maps G^*, S^*, T^*, T^{*-1} over K such that*

$$S^*(x) = \sum_{i=0}^{n-1} s_i x^{q^i}, \qquad T^{*-1}(x) = \sum_{i=0}^{n-1} t_i x^{q^i}, \tag{5}$$

and $G^*(x) = T^*(F(S^*(x)))$. Moreover, $G^*(x)$ can be expressed in the form:

$$G^*(x) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} g_{ij} x^{q^i+q^j} = \underline{x} G \underline{x}^t, \tag{6}$$

where $\underline{x} = (x, x^q, \ldots, x^{q^{n-1}})$ is a vector over K, $\underline{x}^t$ is the transposition of $\underline{x}$, and $G = [g_{ij}]$ is a matrix over K.

The theorem implies the identity $T^{*-1}(G^*(x)) = F(S^*(x))$ which, in turn, implies that

$$G' = \sum_{i=0}^{n-1} t_k G^{*k} = WFW^t,$$

where $F = [\alpha_{ij}]$ over K, G^{*k} and W are two matrices over K whose respective (i, j) entries are $g^{q^k}_{i-k,j-k}$, and $s^{q^i}_{i-j}$, where $i-k$, $j-k$, and $i-j$ are computed modulo n.

As the rank of WFW^t is no more than r, recovering $t_0, t_1, \ldots, t_{n-1}$ can be reduced to solving a MinRank problem; that is, finding $t_0, t_1, \ldots, t_{n-1}$ such that

$$Rank(\sum_{i=0}^{n-1} t_k G^{*k}) \leq r. \tag{7}$$

Once the values $t_0, t_1, \ldots, t_{n-1}$ are found, T and S can be easily computed. Therefore, the key point in the HFE attack is to solve the MinRank problem.

Just as for the HFE, many other multivariate schemes have been proven to be insecure using the MinRank attack. In [1], Billet and Gilbert used the MinRank attack against the Rainbow scheme [19] with the parameters $(2^8, 6, 6, 5, 5, 11)$, which forms a layer-based variant of the UOV scheme.

3. Our New Scheme

In this section, we describe the proposed scheme. As stated in the introduction, we were mainly inspired by the construction of the Simple Matrix Scheme [1] and the Unbalanced Oil Vinegar Signature Scheme [2, 2] to conduct this work. Some theoretical results needed in the description are also presented.

3.1. Theoretical Groundwork

We start with the following theorem. It plays a crucial role in the signing process.

Theorem 2. *Let k be a finite field and denote by k^* the non-zero elements of k. Let $A = (a_{ij})_{u\times u}$ be an invertible $u \times u$ matrix with $a_{ij} \in k$ and C any $(s-u)\times u$ matrix with entries in k. Let B be a $u\times(s-u)$ matrix whose entries are random multivariate linear polynomials. Assume $D = CA^{-1}B+E$, where E is a $(s-u) \times (s-u)$ invertible matrix.*

Then, the block matrix

$$M = \begin{pmatrix} A_{u\times u} & B_{u\times(s-u)} \\ C_{(s-u)\times u} & D_{(s-u)\times(s-u)} \end{pmatrix}$$

is invertible and the entries of M^{-1} are multivariate affine linear polynomials with coefficients in k.

Proof. Let $M = \begin{pmatrix} A_{u\times u} & B_{u\times(s-u)} \\ C_{(s-u)\times u} & D_{(s-u)\times(s-u)} \end{pmatrix}$ and assume that there exist matrices U, V, X, and Y of dimension $u \times u$, $(s-u) \times (s-u)$, $(s-u) \times u$, and $u \times (s-u)$, respectively, satisfying

$$M = \begin{pmatrix} I & O \\ X & I \end{pmatrix} \begin{pmatrix} U & O \\ O & V \end{pmatrix} \begin{pmatrix} I & Y \\ O & I \end{pmatrix}.$$

Then, we have

$$M = \begin{pmatrix} U & UY \\ XU & XUY + V \end{pmatrix}.$$

By equating the two forms of M, we obtain

$$U = A, \quad X = CA^{-1}, \quad Y = A^{-1}B, \quad \textit{and} \quad V = D - CA^{-1}B.$$

That is,

$$M = \begin{pmatrix} I & O \\ CA^{-1} & I \end{pmatrix} \begin{pmatrix} A & O \\ O & D - CA^{-1}B \end{pmatrix} \begin{pmatrix} I & A^{-1}B \\ O & I \end{pmatrix},$$

which can be inverted, as A^{-1} and $(D - CA^{-1}B)$ are invertible. We have

$$M^{-1} = \begin{pmatrix} I & -A^{-1}B \\ O & I \end{pmatrix} \begin{pmatrix} A^{-1} & O \\ O & (D - A^{-1}CB)^{-1} \end{pmatrix} \begin{pmatrix} I & O \\ -CA^{-1} & I \end{pmatrix},$$

i.e.

$$M^{-1} = \begin{pmatrix} I & -A^{-1}B \\ O & I \end{pmatrix} \begin{pmatrix} A^{-1} & O \\ O & E^{-1} \end{pmatrix} \begin{pmatrix} I & O \\ -CA^{-1} & I \end{pmatrix}.$$

The fact that the entries of M^{-1} are multivariate affine linear polynomials with coefficients in k follows directly from the entries of the matrices A, B, C, and D. □

The matrix in Theorem 2 will play a crucial role in the design of our new scheme. As we will see in the description of the scheme, the polynomials in the public key are the entries of a matrix obtained by multiplying M with another matrix whose entries are random polynomials. The matrix M^{-1} will be used in the signing process. This will help to create a system of linear equations whose solution is the signature x of a given document y.

3.2. Description of the New Scheme

Let $n, m, s \in \mathbb{N}$ be integers satisfying $m = s^2$ and $\frac{4}{3} \leq n \leq 2m$. For $i \in \mathbb{N}$, let k^i denote the set of all i-tuples of elements of k and let $(x_1, x_2, \ldots, x_n) \in k^n$ and $(y_1, y_2, \ldots, y_m) \in k^m$. The polynomial ring with n variables in k is denoted by $k[x_1, \ldots, x_n]$. Let $\mathcal{L}_1 : k^n \to k^n$ and $\mathcal{L}_2 : k^m \to k^m$ be two linear transformations; that is

$$\mathcal{L}_1(x) = L_1 x \quad \text{and} \quad \mathcal{L}_2(y) = L_2 y,$$

where L_1 is an $n \times n$ matrix and and L_2 is an $m \times m$ matrix with entries in k, $x = (x_1, x_2, \ldots, x_n)^t$, $y = (y_1, y_2, \ldots, y_m)^t$, and t denotes matrix transposition.

The Central map

The central map of the new scheme is obtained after performing a series of operations on matrices with polynomial entries. The idea is inspired by the construction of the Simple Matrix Scheme for Encryption, which was the first in this new generation of multivariate polynomial cryptosystems which use matrix multiplication to generate a public key.

For $i = 1, ..., s$, let $p_i, p_i' \in k[x_1, ..., x_n]$, be $2s^2$ random affine polynomials. Define

$$P = \begin{pmatrix} p_1(x)p_1'(x) & p_2(x)p_2'(x) & \ldots & p_s(x)p_s'(x) \\ p_{s+1}(x)p_{s+1}'(x) & p_{s+2}(x)p_{s+2}'(x) & \ldots & p_{2s}(x)p_{2s}'(x) \\ \vdots & \vdots & \ddots & \vdots \\ p_{(s-1)s+1}(x)p_{(s-1)s+1}'(x) & p_{(s-1)s+2}(x)p_{(s-1)s+2}'(x) & \ldots & p_{s^2}(x)p'{}_{s^2}(x) \end{pmatrix},$$

$$M = \begin{pmatrix} A_{u\times u} & B_{u\times(s-u)} \\ C_{(s-u)\times u} & D_{(s-u)\times(s-u)} \end{pmatrix},$$

be a block matrix such that A is invertible and only one of the matrices B and C has linear polynomial entries and the other one has scalar entries.

Let $D = CA^{-1}B + E$, where E is an invertible matrix with entries in k. Define $H = MP$ and let $f_{ij} \in k[x_1, \ldots, x_n]$ be the (i, j) element in H. Then, with this notation, we obtain $s^2 = m$ polynomials $f_{11}, \ldots, f_{1s}, f_{21}, \ldots f_{2s}, \ldots f_{s1}, \ldots f_{ss}$, which can be enumerated as $f_1, f_2, \ldots, f_m$. We define the central map as

$$\mathcal{F}(x_1, \ldots, x_n) = (f_1(x_1, x_2, \ldots, x_n), \ldots, f_m(x_1, x_2, \ldots, x_n))$$

and

$$\bar{\mathcal{F}} = \mathcal{L}_2 \circ \mathcal{F} \circ \mathcal{L}_1 = (\bar{f}_1, \bar{f}_2, \ldots, \bar{f}_m), \tag{8}$$

where $\mathcal{L}_1 : k^n \to k^n$ and $\mathcal{L}_2 : k^m \to k^m$ are as defined above, and $\bar{f}_i \in k[x_1, \ldots, x_n]$ are m multivariate polynomials of degree three. The secret key and the public key are given by:

Secret Key: The secret key is comprised of the following two parts:

1) The invertible linear transformations $\mathcal{L}_1, \mathcal{L}_2$.

2) The matrices M and P.

Public Key: The public key is comprised of the following two parts:

1) The field k, including the additive and multiplicative structure;

2) The maps $\bar{\mathcal{F}}$ or, equivalently, its m total degree three components

$$\bar{f}_1(x_1, x_2, \ldots, x_n), \ldots, \bar{f}_m(x_1, x_2, \ldots, x_n) \in k[x_1, \ldots, x_n].$$

Signing: A signer will sign a message $y_1, ..., y_m$ with $x_1, ..., x_n$ satisfying

$$(y_1, y_2, \ldots, y_m) = \bar{\mathcal{F}}(x_1, x_2, \ldots, x_n). \tag{9}$$

To find $x_1, ..., x_n$,

1 Compute $(\bar{y}_1, \bar{y}_2, \ldots, \bar{y}_n) = \mathcal{L}_2^{-1}(y_1, y_2, \ldots, y_m)$.

2 Put

$$H = \begin{pmatrix} \bar{y}_1 & \bar{y}_2 & \cdots & \bar{y}_s \\ \bar{y}_{s+1} & \bar{y}_{s+2} & \cdots & \bar{y}_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{y}_{(s-1)s+1} & \bar{y}_{(s-1)s+2} & \cdots & \bar{y}_{s^2} \end{pmatrix}.$$

As $H = MP$, we have $P = M^{-1}H$. Notice that M is an invertible matrix with polynomial entries and, so, Theorem 2 can be used to find its inverse.

3 Assign an arbitrary value a_i to each $p_i'(x), i = 1, 2, ..., s^2$ and solve the system $(p_i'(x)) = (a_i)$.

4 Solve the new linear system $P = M^{-1}H, (p_i'(x)) = (a_i)$ for $x_1, ..., x_n$. If there is no solution, we choose new values for the $p_i'(x), i = 1, 2, ..., s^2$ and repeat step 4. Let $(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n)$ be the solution.

5 Compute $(x_1, \ldots, x_n) = \mathcal{L}_1^{-1}(\bar{x}_1, \ldots, \bar{x}_n)$. The signature is $(x_1, \ldots, x_n)$.

Verification:
Anyone can verify the signature by computing

$$(y_1, y_2, \ldots, y_m) = \bar{\mathcal{F}}(x_1, x_2, \ldots, x_n).$$

If true, we accept. Otherwise, we reject.

Some Remarks on the signing process:

- The matrix M used in the description of the new scheme satisfies the conditions of Theorem 2. Therefore, the existence of the inverse M^{-1} is guaranteed by the theorem and the entries of M^{-1} are all multivariate affine linear polynomials with coefficients in k.
- Step 3 is necessary, in case some of the p_i' are not linearly independent. In such a case, there will be no solution and the values for the p_i' should be changed.

  After few tries, a solution will be found: the probability of obtaining at least one solution is very high, as the probability of an $n \times n$ matrix over $\mathbb{F}_q$ being invertible is $(1 - \frac{1}{q})(1 - \frac{1}{q^2}) \cdots (1 - \frac{1}{q^{n-1}})$ (see [2]).
- The relation between m, n, and s may be ignored and the values may be chosen arbitrarily, in general.
- Contrary to the decryption process in [1], there is no failure in the signing process.

The following toy example is based on Theorem 2 and uses aB with linear polynomial entries.

Example Let $k = \mathbb{F}_3$, $s = 3$, $m = s^2 = 9$, and $n = 18$.

Assume

$$A = \left(\begin{smallmatrix} 1 & 2 \\ 2 & 2 \end{smallmatrix}\right), B = \left(\begin{smallmatrix} x_1+x_{10} \\ 2x_5+1 \end{smallmatrix}\right), C = \left(\begin{smallmatrix} 1 & 1 \end{smallmatrix}\right) E = \left(\begin{smallmatrix} 2 \end{smallmatrix}\right).$$

Therefore, $D = CA^{-1}B + E = x_5 + 1$.

Then,

$$M = \left(\begin{smallmatrix} 1 & 2 & x_1+x_10 \\ 2 & 2 & 2x_5+1 \\ 1 & 1 & x_5+1 \end{smallmatrix}\right)$$

and $M^{-1} = \left(\begin{smallmatrix} 2 & 2x_1+2x_5+2x_{10}+2 & 2x_1+2x_5+2x_{10}+1 \\ 1 & x_1+2x_5+x_{10}+2 & x_1+2x_5+x_{10}+1 \\ 0 & 2 & 2 \end{smallmatrix}\right)$

Let $P_1 = 2x_4 + x_9, P_2 = 2x_1 + 1, P_3 = x_7 + x_{11}, P_4 = x_8 + 2, P_5 = 2x_{12} + 1, P_6 = 2x_5 + 1, P_7 = x_3 + 2x_6, P_8 = 2x_{10} + x_1$, and $P_9 = x_2 + 2$.

$P_1' = x_5 + 1, P_2' = x_2, P_3' = x_1 + x_5, P_4' = 2x_6 + 1, P_5' = x_{12} + 2, P_6' = x_{10}, P_7' = x_3 + x_9, P_8' = x_7 + x_{10}$, and $P_9' = 2x_4$.

We obtain

$$P = \begin{pmatrix} 2x_4x_5+2x_4+x_5x_9+x_9 & 2x_1x_2+x_2 & x_1x_7+x_1x_{11}+x_5x_7+x_5x_{11} \\ 2x_6x_8+x_6+x_8+2 & 2x_{12}^2+2x_{12}+2 & 2x_5x_{10}+x_{10} \\ x_3^2+2x_3x_6+x_3x_9+2x_6x_9 & x_1x_7+x_1x_{10}+2x_7x_{10}+2x_{10}^2 & 2x_2x_4+x_4 \end{pmatrix}.$$

Hence,

$$H = MP = \begin{pmatrix} f_1 & f_2 & f_3 \\ f_4 & f_5 & f_6 \\ f_7 & f_8 & f_9 \end{pmatrix},$$

where

$f_1 = x_1x_3^2 + 2x_1x_3x_6 + x_1x_3x_9 + 2x_1x_6x_9 + x_3^2x_{10} + 2x_3x_6x_{10} + x_3x_9x_10 + 2x_4x_5 + 2x_4 + x_5x_9 + x_6x_8 + 2x_6x_9x_{10} + 2x_6 + 2x_8 + x_9 + 1$,

$f_2 = x_1^2x_7 + x_1^2x_{10} + 2x_1x_2 + x_2 + 2x_7x_{10}^2 + 2x_{10}^3 + x_{12}^2 + x_{12} + 1$,

$f_3 = 2x_1x_2x_4 + x_1x_4 + x_1x_7 + x_1x_{11} + 2x_2x_4x_{10} + x_4x_{10} + x_5x_7 + x_5x_{10} + x_5x_{11} + 2x_{10}$,

$f_4 = 2x_3^2x_5 + x_3^2 + x_3x_5x_6 + 2x_3x_5x_9 + 2x_3x_6 + x_3x_9 + x_4x_5 + x_4 + x_5x_6x_9 + 2x_5x_9 + x_6x_8 + 2x_6x_9 + 2x_6 + 2x_8 + 2x_9 + 1$,

$f_5 = x_1x_2 + 2x_1x_5x_7 + 2x_1x_5x_{10} + x_1x_7 + x_1x_{10} + 2x_2 + x_5x_7x_{10} + x_5x_{10}^2 + 2x_7x_{10} + 2x_{10}^2 + x_{12}^2 + x_{12} + 1$,

$f_6 = 2x_1x_7 + 2x_1x_{11} + x_2x_4x_5 + 2x_2x_4 + 2x_4x_5 + x_4 + 2x_5x_7 + x_5x_{10} + 2x_5x_{11} + 2x_{10}$,

$f_7 = x_3^2x_5 + x_3^2 + 2x_3x_5x_6 + x_3x_5x_9 + 2x_3x_6 + x_3x_9 + 2x_4x_5 + 2x_4 + 2x_5x_6x_9 + x_5x_9 + 2x_6x_8 + 2x_6x_9 + x_6 + x_8 + x_9 + 2$,

$f_8 = 2x_1x_2 + x_1x_5x_7 + x_1x_5x_{10} + x_1x_7 + x_1x_{10} + x_2 + 2x_5x_7x_{10} + 2x_5x_{10}^2 + 2x_7x_{10} + 2x_{10}^2 + 2x_{12}^2 + 2x_{12} + 2$, and

$f_9 = x_1x_7 + x_1x_{11} + 2x_2x_4x_5 + 2x_2x_4 + x_4x_5 + x_4 + x_5x_7 + 2x_5x_{10} + x_5x_{11} + x_{10}$.

Now, we have

$$\mathcal{F}(x_1, \cdots, x_{18}) = (f_1(x_1, \cdots, x_{18}), \cdots, f_9(x_1, \cdots, x_{18})).$$

The Public Key is:

1 $\mathbb{F}_3$.

2 $f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9$.

The Private Key is:

$$P = \begin{pmatrix} 2x_4x_5+2x_4+x_5x_9+x_9 & 2x_1x_2+x_2 & x_1x_7+x_1x_{11}+x_5x_7+x_5x_{11} \\ 2x_6x_8+x_6+x_8+2 & 2x_{12}^2+2x_{12}+2 & 2x_5x_{10}+x_{10} \\ x_3^2+2x_3x_6+x_3x_9+2x_6x_9 & x_1x_7+x_1x_{10}+2x_7x_{10}+2x_{10}^2 & 2x_2x_4+x_4 \end{pmatrix} \text{ and}$$

$$M = \begin{pmatrix} 1 & 2 & x_1{+}x_10 \\ 2 & 2 & 2x_5{+}1 \\ 1 & 1 & x_5{+}1 \end{pmatrix}.$$

Now, assume that Alice wants to sign the document $y = (1, 0, 1, 1, 2, 0, 1, 1, 2)$. She substitutes y in H and gets $H = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 2 & 0 \\ 1 & 1 & 2 \end{pmatrix}$. As $H = MP$, she gets $P = M^{-1}H$; that is,

$$\begin{pmatrix} 2x_4x_5{+}2x_4{+}x_5x_9{+}x_9 & 2x_1x_2{+}x_2 & x_1x_7{+}x_1x_{11}{+}x_5x_7{+}x_5x_{11} \\ 2x_6x_8{+}x_6{+}x_8{+}2 & 2x_{12}^2{+}2x_{12}{+}2 & 2x_5x_{10}{+}x_{10} \\ x_3^2{+}2x_3x_6{+}x_3x_9{+}2x_6x_9 & x_1x_7{+}x_1x_{10}{+}2x_7x_{10}{+}2x_{10}^2 & 2x_2x_4{+}x_4 \end{pmatrix} =$$

$$\begin{pmatrix} 2x_1^2{+}x_1x_{10}{+}2x_1x_{17}{+}2x_{10}^2{+}2x_{10}x_{17}{+}2x_{17}^2 & x_1^2{+}2x_1x_{10}{+}x_1x_{17}{+}x_1{+}x_{10}^2{+}x_{10}x_{17}{+}x_{10}{+}x_{17}^2{+}2x_{17} & x_1{+}x_{10}{+}2x_{17} \\ x_1{+}x_{10}{+}2x_{17}{+}1 & 2x_1{+}2x_{10}{+}x_{17}{+}1 & 2 \\ x_1{+}x_{10}{+}2x_{17}{+}2 & 2x_1{+}2x_{10}{+}x_{17} & 2 \end{pmatrix}.$$

Finally, to find the signature, Alice assigns a fixed value to the polynomials P'_i, as follows: $P'_1 = 2, P'_2 = 2, P'_3 = 1, P'_4 = 2, P'_5 = 2, P'_6 = 1, P'_7 = 1, P'_8 = 0$ and $P'_9 = 1$.
Then, she then solves the linear system and obtains the singature

$$x = (0, 2, 0, 2, 1, 2, 2, 0, 1, 1, 1, 0).$$

Alice sends the signed document to Bob, who can verify it by checking

$$\mathcal{F}(0, 2, 0, 2, 1, 2, 2, 0, 1, 1, 1, 0) = (1, 0, 1, 1, 2, 0, 1, 1, 2)$$

and accepts the document.

4. Security Analysis

Further analysis of the security, as well as the choice of parameters and the efficiency of our new scheme, will be left for future work. We give, here, some observations that make us believe that our new proposed scheme has good security, if the parameters are carefully chosen.

In the separation attacks introduced by Kipnis and Shamir [8], the Oil variables and Vinegar variables must be separated to forge arbitrary signatures. Its improvement by Kipnis, Patarin, and Goubin to attack the UOV scheme [2] proposes finding some hidden invariant subspaces from the public polynomials that will allow for separation of the Oil variables and Vinegar variables and forging an arbitrary signature.

The Rainbow Band Separation attack and its generalization [1, 1] need to use the missing cross-terms of the variables to find an equivalent set of keys, in order to forge an arbitrary signature.
Therefore, none of these attacks pose a real security threat to our new proposed scheme, due to its structural design whihc focuses on polynomials, rather than variables.

For the MinRank attack, an attacker needs to find a non-trivial linear combination of matrices with minimal rank associated with the components of the set of public polynomials. After finding these low-rank linear combinations, the linear map $\mathcal{L}_2$ can be recovered and, therefore, the secret key of the scheme is exposed. For the High-Rank Attack, the attacker tries to find linear combinations corresponding to variables with minimum appearances in the central map to recover the linear map $\mathcal{L}_1$ and, subsequently, the secret key of the scheme as well.
however, as in the previous cases, the structural design of the new scheme uses a product of randomly chosen affine linear polynomials and, hence, the entries of the matrix P are random multivariate quadratic polynomials. This guarantees that the rank of any non-trivial linear combination of matrices associated with the public polynomials will be close to n. Furthermore, as all variables appear in each of the central polynomials approximately the same number of times, neither of the two rank attacks can be used against our new scheme.
Considering the above arguments, we can conclude that the most likely successful attack against our new scheme must be a direct attack and, so, we can choose the parameters accordingly to guarantee acceptable security, due to the following observation: Let us assume that an attacker wants to solve the equation $(y_1, y_2, \ldots, y_m) = \bar{\mathcal{F}}(x_1, x_2, \ldots, x_n)$ to find the signature $x_1, x_2, \ldots, x_n$ of the message $y_1, y_2, \ldots, y_m$. Assume that an oracle O gives the attacker the values $(\bar{y}_1, \bar{y}_2, \ldots, \bar{y}_n)$ (without knowing $\mathcal{L}_2$, one of the secret keys) and they can obtain the matrix

$$H = \begin{pmatrix} \bar{y}_1 & \bar{y}_2 & \cdots & \bar{y}_s \\ \bar{y}_{s+1} & \bar{y}_{s+2} & \cdots & \bar{y}_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{y}_{(s-1)s+1} & \bar{y}_{(s-1)s+2} & \cdots & \bar{y}_{s^2} \end{pmatrix}.$$

At this point, the attacker still needs to find a way to get the entries of the matrices M^{-1}. Even if they succeed in finding the entries of the matrix $M^{-1}H$ without knowing M^{-1} explicitly, to be able to forge a signature, they will still need to solve the system $P = M^{-1}H$, which is a system of multivariate quadratic equations with randomly chosen coefficients.

5. Conclusion

We have proposed a new multivariate signature scheme whose central map is obtained from the multiplication of matrices with random multivariate polynomials as entries. This implies that the central map is composed of cubic polynomials which are the sum of the products of completely randomly chosen affine linear polynomials, with no specific form. Multiplication from the left by the block matrix M causes any tentative factorization of the polynomials in the central matrix extremely difficult. Due to its structural design, the only feasible attack against this new scheme is the direct attack, and we conjecture that its security can be reduced to the NP-hard problem of solving a non-linear system of equations. Finally, we need to mention that this paper focuses more on the design and the theoretical approach of the scheme, and further study to establish the provable security, determine secure parameters, and analyze the efficiency of the proposed scheme will be the object of future research.

6. Acknowledgements

The first author was supported by the Emirate Foundation through grant 21S021.

7. References

References

[1] Matsumoto T, Imai H. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption[C]. Advances in Cryptology-EUROCRYPT'88. Springer Berlin Heidelberg, 1988: 419-453.

[2] Gary M R, Johnson D S. Computers and Intractability: A Guide to the Theory of NP-completeness[J]. 1979

[3] Shor P.,: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on computing, 26(5): 1484-1509, 1997.

[4] Courtois N., Goubin L. Cryptanalysis of the TTM cryptosystem. Advances in Cryptology-ASIACRYPT'00, Lecture Notes in Computer Science, vol. 1976, pp.44-57. Springer, Berlin (2000).

[5] Ding J, Ren A, Tao C. Embedded Surface Attack on Multivariate Public Key Cryptosystems from Diophantine Equations[C]. Information Security and Cryptology. Springer Berlin Heidelberg, 2013: 122-136.

[6] Ding J., Hodges T.J.: Inverting HFE systems is quasi-polynomial for all fields. In: Rogaway P. (ed.) CRYPTO 2011, Lecture Notes in Computer Science, vol. 6841, pp. 724-742. Springer, Berlin (2011).

[7] Kipnis A., Shamir A.: Cryptanalysis of the HFE public key cryptosystem by relinearization. In: Advances in Cryptology-CRYPTO'99, Lecture Notes in Computer Science, vol. 1666, pp. 19-30. Springer, Berlin (1999)

[8] Kipnis A., Shamir A.: Crypranalysis of the Oil and Vinegar Signature Scheme. In: Stern, J. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp, 257-267. Springer, Heidelberg (1998)

[9] Olivier B., Henri G. Cryptanalysis of Rainbow. SCN 2006, LNCS 4116, pp. 336-347. Springer Berlin Heidelberg, 2006.

[10] Patarin J. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88[M]. Advances in Cryptology-CRYPTO'95. Springer Berlin Heidelberg, 1995: 248-261.

[11] Thomae E. A Generalization of the Rainbow Band Separation Attack and its Applications to Multivariate Schemes[R]. IACR Cryptology ePrint Archive, 2012.

[12] Ding, Jintai, Zheng Zhang, Joshua Deaton, Kurt Schmidt, and F. Vishakha. "New attacks on lifted unbalanced oil vinegar." In The 2nd NIST PQC Standardization Conference. 2019.

[13] Ding J., Schmidt D., Werner F. Algebraic attack on HFE revisited. In: Information Security, Lecture Notes in Computer Science, vol. 5222, pp.215-227. Springer, Berlin (2008).

[14] Faugère J.C.: A new efficient algorithm for computing Gröbner bases (F4). J. Pure Appl. Algebra 139, 61-88(1999).

[15] Faugère J.C.: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation ISSAC, pp.75-83. ACM Press (2002).

[16] Mohamed M S E, Cabarcas D, Ding J, et al. MXL3: An efficient algorithm for computing Gröbner bases of zero-dimensional ideals[M]. Information, Security and Cryptology-ICISC 2009. Springer Berlin Heidelberg, 2010: 87-100.

[17] Mohamed M S E, Mohamed W S A E, Ding J, et al. MXL2: Solving polynomial equations over GF(2) using an improved mutant strategy[M]. Post-Quantum Cryptography. Springer Berlin Heidelberg, 2008: 203-215.

[18] Ding, J., Zhang, Z., Deaton, J., Schmidt, K., Vishakha, F.: New attacks on lifted unbalanced oil vinegar. In: The 2nd NIST PQC Standardization Conference (2019)

[19] Tao, C., Diene, A., Tang, S., Ding, J.: Simple Matrix Scheme for Encryption. In: Gaborit, P. (ed.) PQCrypto 2013. LNCS, vol. 7932, pp. 231–242. Springer, Heidelberg (2013)

[20] Ding J, Schmidt D., Rainbow, a new multivariable polynomial signature scheme[C]. Applied Cryptography and Network Security. Springer Berlin Heidelberg, 2005: 164-175.

[21] Ding J., Yang B.Y., Chen C.H.O., Chen M.S., Cheng C.M.: New Differential-Algebraic Attacks and Reparametrization of Rainbow. In: Bellovin S.M., Gennaro R., Keromytis A.D., Yung M. (ed.) ACNS 2008. LNCS, vol. 5037, pp. 242-257. Springer, Heidelberg (2008)

[22] Ding J., Petzoldt, A., Current state of multivariate cryptography. IEEE Security and Privacy, 2017 - ieeexplore.ieee.org, 15(4):28–36, 2017.

[23] Ding, J., Petzoldt, A., and Wang,: The Cubic Simple Matrix Encryption Scheme. In Mosca, M. (ed.), Post-Quantum Cryptography, Lecture

doi:10.20944/preprints202004.0392.v1

Notes in Computer Science, 8772, pp. 76–87. Springer International Publishing. 2014

[24] Patarin J.: The Oil and Vinegar Signature Scheme, presented at the Dagstuhl Workshop on Cryptography, September 1997 (transparencies).

[25] Kipnis A., Patarin J., Goubin L., Unbalance Oil and Vinegar Signature Scheme. In: J. Stern, (ed.) EUROCRYPT 1999, LNCS, vol. 1592, pp. 206-222. Springer, Heidelberg (1999)

[26] Patarin J.: Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In: Advances in Cryptology-EUROCRYPT '96, Lecture Notes in Computer Science, vol. 1070, pp. 33-48. Springer, Berlin (1996).

[27] Patarin, J., Courtois, N., Goubin, L. Quartz, 128-bit long digital signatures. In Naccache, D., ed. CT-RSA. Volume 2020 of Lecture Notes in Computer Science., Springer (2001) 282–297

[28] Petzoldt A., Chen M.S., Yang B.Y., Tao C. , Ding J. : Design Principles for HFEv- based Signature Schemes. ASIACRYPT 2015 - Part 1, LNCS vol. 9452, pp. 311-334. Springer, 2015.