JOURNAL OF FUNDAMENTAL MATHEMATICS
AND APPLICATIONS (JFMA) VOL. 8 NO. 1 (2025)
Available online at www.jfma.math.fsm.undip.ac.id

HPPCv: a Modification of HPPC Scheme with Vinegar Variables

Saifullah Ali[1*], Indah Emilia Wijayanti[1], Uha Isnaini[1]

[1] *Universitas Gadjah Mada*
Email: [1]saifullah.ali@mail.ugm.ac.id, [1]ind_wijayanti@ugm.ac.id, [1]isnainiuha@ugm.ac.id
*Corresponding author

Abstract. The Hidden Product of Polynomial Composition (HPPC) Digital Signature is multivariate-based cryptography using an HFE trapdoor. The HPPC scheme provides the technique for choosing the HFE central map. Its technique utilizes the product of the composition of two linearized polynomials. In this research, we proposed the modification of the HPPC scheme. We modify the HPPC scheme such that the scheme is based on HFEv. The linearized polynomial with vinegar variables will be chosen for constructing the central map. In our modification version, the public key becomes a system of polynomials of degree 4 and a map from $n + v$ to n-dimension vector space. For a final remark, Despite an increase in the polynomial degree, HPPCv maintains a computational cost similar to HPPC.

Keywords: PQC, HFEv, Finite Field, Matrix, MPKC

I. INTRODUCTION

Cryptography, which is widely used in real life for key encapsulation mechanisms, is based on RSA and ECC. These two systems use factorization problems and discrete logarithm problems respectively. In 1994, Peter Shor proposed an algorithm for quantum computers that could find efficiently the order of elements in [1]. Since Shor's Algorithm was proposed, the factorization and discrete logarithm problem would be solved effectively if the quantum computer existed. Therefore, in 2016, NIST started a competition to find a cryptosystem that remains secure even if a quantum computer is formed, called Post-Quantum Cryptography (PQC). There are five mathematical bases for PQC, i.e. lattice-based, code-based, hash-based, isogeny-based, and multivariate-based. In 2022, NIST announced the new cryptosystems for Key Encapsulation Mechanisms (KEM) and Digital Signature Algorithms (DSA) [2]. The new cryptosystems are ML-KEM [3] and ML-DSA [4] which are based on a lattice, SLH-DSA [5] which is based on hash, and a few alternative systems which are based on code. NIST continues the competition for DSA. They want to find an alternative system with other mathematical bases. One of them is multivariate-based cryptography, those are some digital signature schemes, such as 3WISE [6], DME-Sign [7], MAYO [8], PROV [9], QR-UOV [10], and SNOVA [11]. Among the proposed multivariate-based cryptography, Rodriguez introduces HPPC [12], which serves as the foundation of our modification.

Multivariate-based Cryptography was first introduced by Matsumoto and Imai in [13]. The idea is to hide a multivariate quadratic equation between two transformations. Patarin analyzes this scheme and the scheme is broken by using Groebner's bases in [14]. Then, he introduces the Hidden Field Equation (HFE), a trapdoor function for multivariate-based cryptography. A few years later, a new trapdoor function was introduced by Kipnis, Patarin, and Goubin in [15], called Unbalanced Oil and Vinegar (UOV). They also modify the HFE trapdoor function with

vinegar variables (HFEv). The HFEv trapdoor function is more secure than the HFE trapdoor function because of the vinegar variables which add perturbation to the central map stated by Wolf in his PhD thesis [16]. In 2016, Casanova, Faugere, Macario-Rat, Patarin, Perret, and Ryckeghem proposed GeMSS, the digital signature scheme that is based on the HFEv trapdoor function [17]. The HPPC uses vinegar variables but not in the central map and we find out that the HPPC scheme is more like HFE trapdoor than HFEv. In this paper, we present a modification of the HPPC scheme using vinegar variables. We use the idea of the multivariate quadratic problem modification with vinegar variables.

This paper is organized as follows. Section II. provides the necessary background on representing an element of the finite field to its matrix representation and multiplying two vector representations of the finite field elements using a tensor product. In Section III., the summary of the HPPC scheme will be presented. Section IV. presents the modification of the HPPC scheme with vinegar variables. Section V. contains some conclusions.

II. Prelimineries

In this section, we will summarize some background used in our paper. The finite field is widely used in our calculation. Based on [12], the computation will be computed in all representations of a finite field, i.e. polynomial, vector, and matrix. The tensor product is used to compute the multiplication of vector representation. It is also used to compute the matrix representation of the multiplication of two polynomials. The last is the background of multivariate public key cryptography (MPKC).

2.1. Finite Field

In this paper, the finite field of q elements and characteristic p will be denoted by $\mathbb{F}_q$ with $q = p^l$ for some $l \in \mathbb{Z}$. The n-th degree extension field of a finite field $\mathbb{F}_q$ will be denoted by $\mathbb{F}_{q^n}$. We will write the elements of the extension field $\mathbb{F}_{q^n}$ with capital letters, e.g. $X, Y \in \mathbb{F}_{q^n}$. Vectors will be written using bold letters, e.g. $\mathbf{v}$, and matrices using capital and bold letters, e.g. $\mathbf{M}$.

Finite fields are already well known for their polynomial representation and the corresponding vector [18, 19, 20]. Given irreducible polynomial $f(x)$ of degree n over $\mathbb{F}_q$ and let θ be the root of $f(x)$, then the vector space over $\mathbb{F}_q$ with the set $\{1, \theta, \ldots, \theta^{n-1}\}$ as its bases are the extension field of $\mathbb{F}_q$ and the coordinate vector of elements in $\mathbb{F}_{q^n}$ as its vector representation. In this paper, We use a matrix representation of a finite field. Matrix representation requires the companion matrix of the minimal polynomial $f(x)$, denoted by $\mathbf{C}_{f(x)}$. The companion matrix $\mathbf{C}_{f(x)}$ of minimal polynomial $f(x)$ can be the root of the minimal polynomial $f(x)$. So, the root θ in the bases can be replaced by the companion matrix of $f(x)$ [19].

Theorem 1 [19] Let $\mathbb{F}_{q^n}$ be the extension field over $\mathbb{F}_q$ and $\mathbf{C}_{f(x)}$ be the companion matrix of irreducible polynomial $f(x)$. There exist $n \times n$ matrix representation of each elements of $\mathbb{F}_{q^n}$. Furthermore, if $\mathbf{g} \in \mathbb{F}_q^n$ is the vector representation of element $G \in \mathbb{F}_{q^n}$, then

$$\mathbf{G} = (\mathbf{C}^0_{f(x)}\mathbf{g}, \ldots, \mathbf{C}^{n-1}_{f(x)}\mathbf{g})$$

is the matrix representation of G.

Proof. Let θ be a root of minimal polynomial $f(x)$. Consider the element $G \in \mathbb{F}_{q^n}$ in the form $G = g_0 + g_1\theta + \cdots + g_{n-1}\theta^{n-1}$ and its vector representation is $\mathbf{g} = (g_0, \ldots, g_{n-1})^T$. We know that matrix $\mathbf{C}_{f(x)}$ is a root of minimal polynomial $f(x)$. So we get the matrix representation of G which is $\mathbf{G} = g_0\mathbf{C}^0_{f(x)} + g_1\mathbf{C}_{f(x)} + \cdots + g_{n-1}\mathbf{C}^{n-1}_{f(x)}$. Furthermore, for each vector standard $\mathbf{e}_i$, we get that

$$\begin{aligned}
\mathbf{G}\mathbf{e}_i &= \left(g_0\mathbf{C}^0_{f(x)} + \cdots + g_{n-1}\mathbf{C}^{n-1}_{f(x)}\right)\mathbf{e}_i \\
&= \left(\mathbf{C}^0_{f(x)}\mathbf{e}_i, \ldots, \mathbf{C}^{n-1}_{f(x)}\mathbf{e}_i\right)\mathbf{g} \\
&= \left(\mathbf{C}^{i-1}_{f(x)}\mathbf{e}_1, \ldots, \mathbf{C}^{i-1}_{f(x)}\mathbf{e}_n\right)\mathbf{g} \\
&= \mathbf{C}^{i-1}_{f(x)}\mathbf{g}
\end{aligned}$$

for all $1 \leq i \leq n$. Therefore, we can compute the matrix representation of G as $\mathbf{G} = (\mathbf{G}\mathbf{e}_1, \ldots, \mathbf{G}\mathbf{e}_n) = \left(\mathbf{C}^0_{f(x)}\mathbf{g}, \ldots, \mathbf{C}^{n-1}_{f(x}\mathbf{g}\right)$. □

By Theorem 1, we can express every element of a finite field $\mathbb{F}_{q^n}$ into $n \times n$ matrix over $\mathbb{F}_q$ and compute the matrix representation using its vector representation.

Lemma 1 *Let $\mathbb{F}_{q^n}$ be a finite field. For each matrix representation $\mathbf{G}$ of element $G \in \mathbb{F}_{q^n}$, $\mathbf{G}\mathbf{e}_1 = \mathbf{g}$ be the vector representation of G.*

Proof. By Theorem 1, we can express the matrix representation of any element $G \in \mathbb{F}_{q^n}$ by

$$g_0\mathbf{C}^0_{f(x)} + g_1\mathbf{C}_{f(x)} + \cdots + g_{n-1}\mathbf{C}^{n-1}_{f(x)}.$$

We can conclude that

$$\begin{aligned}
\mathbf{G}\mathbf{e}_1 &= \left(g_0 + g_1\mathbf{C}_{f(x)} + \cdots + g_{n-1}\mathbf{C}^{n-1}_{f(x)}\right)\mathbf{e}_1 \\
&= g_0\mathbf{C}^0_{f(x)}\mathbf{e}_1 + g_1\mathbf{C}_{f(x)}\mathbf{e}_1 + \cdots + g_{n-1}\mathbf{C}^{n-1}_{f(x)}\mathbf{e}_1 \\
&= g_1\mathbf{e}_1 + \cdots + g_{n-1}\mathbf{e}_n = \mathbf{g}.
\end{aligned}$$

So, the first column of $\mathbf{G}$ is its vector representation. □

Lemma 1 give us the connection between matrix representation and vector representation. The following theorem is stated in [12], we complete the statement by proof.

Theorem 2 *Let $\mathbb{F}_{q^n}$ be a finite field. For any $G, S \in \mathbb{F}_{q^n}$ with $\mathbf{G}$ be a matrix representation of G and $\mathbf{s}$ be a vector representation of S, then $\mathbf{G}\mathbf{s} = \mathbf{r}$ where $\mathbf{r}$ is the vector representation of $R = GS$.*

Proof. By Lemma 1, We get that the vector representation of s is $\mathbf{S}\mathbf{e}_1 = \mathbf{s}$ and we can calculate the vector representation of multiplication GS as $\mathbf{G}\mathbf{s} = \mathbf{G}\mathbf{S}\mathbf{e}_1 = \mathbf{R}\mathbf{e}_1 = \mathbf{r}$. □

2.2. Tensor

In abstract algebra perspective, a tensor product of two vector spaces is a pair of vector space and bilinear maps that satisfies universal properties. The tensor product between linear transformation from each vector space becomes a linear transformation in a tensor product of two vector spaces [21] and it has a matrix representation. The matrix representation will be called the tensor or Kronecker product of matrices [22].

Definition 1 [23] Let $\mathbf{A}_{m_1\times n_1} = (a_{i,j})_{m_1\times n_1}$ and $\mathbf{B}_{m_1\times n_2}$ be two matrices over field $\mathbb{F}$. Tensor product of $\mathbf{A}$ and $\mathbf{B}$, denoted by $\mathbf{A}\otimes\mathbf{B}$, is a $m_1m_2 \times n_1n_2$ matrix of the form

$$\begin{pmatrix} a_{1,1}\mathbf{B} & a_{1,2}\mathbf{B} & \dots & a_{1,n_1}\mathbf{B} \\ a_{2,1}\mathbf{B} & a_{2,2}\mathbf{B} & \dots & a_{2,n_1}\mathbf{B} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m_1,1}\mathbf{B} & a_{m_1,2}\mathbf{B} & \dots & a_{m_1,n_1}\mathbf{B} \end{pmatrix}.$$

There is a property of a tensor product that is useful for computation. The property states that the product of two tensors is equal to the tensor of its matrices multiplication.

Theorem 3 [23] Given four matrices $\mathbf{A} \in \mathbb{F}^{m\times n}, \mathbf{B}\mathbb{F}^{s\times t}, \mathbf{C} \in \mathbb{F}^{n\times k}$, and $\mathbf{D} \in \mathbb{F}^{t\times l}$. We get the equality

$$(\mathbf{A}\otimes\mathbf{B})(\mathbf{C}\otimes\mathbf{D}) = (\mathbf{AC})\otimes(\mathbf{BD}).$$

Using a tensor, we can multiply two finite field elements in vector representation without expressing them in matrix representation. The following theorem is stated in [12], we give the complete proof of the statement.

Theorem 4 *Let $\mathbb{F}_{q^n}$ be a finite field with generator $f(x)$ and matrix $\boldsymbol{C}_{f(x)}$ be a companion matrix of $f(x)$. For any $\boldsymbol{g}, \boldsymbol{s} \in \mathbb{F}_q^n$ where $\boldsymbol{g}$ and $\boldsymbol{s}$ be a vector representation of element G and S respectively, then*

$$(\boldsymbol{C}^0_{f(x)}, \dots, \boldsymbol{C}^{n-1}_{f(x)})(\boldsymbol{g}\otimes\boldsymbol{s})$$

is a vector representation of GS.

Proof. Let $\mathbb{F}_{q^n}$ be an extension field over $\mathbb{F}_q$, θ be its primitive element, $f(x)$ be the minimal polynomial of θ, and $\mathbf{C}_{f(x)}$ be its companion matrix. For each $G, S \in \mathbb{F}_{q^n}$, we get

$$\begin{aligned}
&\left(\mathbf{C}^0_{f(x)}\mathbf{g}, \dots, \mathbf{C}^{n-1}_{f(x)}\mathbf{g}\right)\mathbf{s} \\
&= \mathbf{C}^0_{f(x)}\mathbf{g}s_0 + \dots + \mathbf{C}^{n-1}_{f(x)}\mathbf{g}s_{n-1} \\
&= \sum_{i=0}^{n-1} \mathbf{C}^i_{f(x)}(g_0s_i, \dots, g_{n-1}s_i)^T \\
&= \left(\sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1}\left(\mathbf{C}^i_{f(x)}\right)_{1,j+1} g_js_i\right), \dots, \sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1}\left(\mathbf{C}^i_{f(x)}\right)_{n,j+1} g_js_i\right)\right)^T
\end{aligned}$$

$$= \left(\sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} \left(\mathbf{C}_{f(x)}^{i} \right)_{1,j+1} g_i s_j \right), \ldots, \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} \left(\mathbf{C}_{f(x)}^{i} \right)_{n,j+1} g_i s_j \right) \right)^T$$
$$= \left(\mathbf{C}_{f(x)}^{0}, \ldots, \mathbf{C}_{f(x)}^{n-1} \right) (\mathbf{g} \otimes \mathbf{s})$$

where $\mathbf{g}$ and $\mathbf{s}$ are the vector representations of G and S, respectively. □

In Theorem 2, to find the vector representation of the multiplication of two elements, we have to represent one of them by matrix and the other one by vector. By Lemma 4, we can compute the multiplication of two vector representations just by using the tensor product of their vector representation and matrix companion.

2.3. Multivariate Quadratic and Its Modification

Given a system of m multivariate polynomials P_i with n variables $\mathcal{P}$ and each polynomial's degrees are $d \in \mathbb{N}$. Let $P_i(x_1, \ldots, x_n)$ be in the form

$$P_i(x_1, \ldots, x_n) = \sum_{\mathbf{a}_j \in \mathbb{N}_0^n} c_{i,j} t_{\mathbf{a}_j}$$

for all $1 \leq i \leq m$ where $c_{i,j} \in \mathbb{F}_q$. Multivariate quadratic problem is a hardness problem to find $(x'_1, \ldots, x'_n) \in \mathbb{F}_q^n$ such that satisfy

$$\begin{aligned} y_1 &= P_1(x'_1, \ldots, x'_n) \\ &\vdots \\ y_m &= P_m(x'_1, \ldots, x'_n) \end{aligned}$$

for a given $(y_1, \ldots, y_m) \in \mathbb{F}_q^m$ and a system $\mathcal{P} = (P_1, \ldots, P_m)$ where each degrees of P_i are $d = 2$. The family of all multivariate quadratic problems will be denoted by $\mathcal{MQ}(\mathbb{F}_q^n, \mathbb{F}_q^m)$. For cryptographic purposes, let $\mathcal{S}, \mathcal{T}$ be a pair of invertible affine maps and $\mathcal{P}' \in \mathcal{MQ}(\mathbb{F}_q^n, \mathbb{F}_q^m)$ be a central map. The public key of this multivariate-based cryptography is

$$\mathcal{P} = \mathcal{T} \circ \mathcal{P}' \circ \mathcal{S} \in \mathcal{MQ}(\mathbb{F}_q^n, \mathbb{F}_q^m).$$

We hide a multivariate quadratic system $\mathcal{P}'$ into a new multivariate quadratic system $\mathcal{P}$ using two affine/linear maps.

Patarin, in [14], made the HFE trapdoor function. The HFE trapdoor function utilizes univariate polynomials over the extension field to be the central maps. In [24, 25], there is a bijective function between the multivariate polynomial system of n variables over $\mathbb{F}_q$ and the univariate polynomial over $\mathbb{F}_q^n$. The HFE central map in the form

$$\mathcal{F}(x) = \sum_{i,j=0}^{q^i+q^j \leq D} C_{i,j} x^{q^i+q^j} + \sum_{k=0}^{q^k \leq D} B_k x^{q^k} + A$$

where $i, j, D \in \mathbb{N}, C_{i,j}, B_k, A \in \mathbb{F}_{q^n}$. By vinegar variables modification in [15], the HFEv

central map becomes

$$P_{z_1,\ldots,z_v}(x) = \sum_{0\leq i,j\leq n} C_{i,j}x^{q^i+q^j} + \sum_{k=0}^{n'-1} B_k(z_1,\ldots,z_v)x^{q^k} + A(z_1,\ldots,z_v)$$

where each $B_k : \mathbb{F}^v \to \mathbb{F}_{q^n}$ are a linear maps and $A_k : \mathbb{F}^v \to \mathbb{F}_{q^n}$ is a quadratic map. The HFEv central map has a solution if and only if the vinegar variables are fixed.

III. HPPC

The HPPC Scheme was introduced in [12], one of the participants in the NIST Digital Signature competition. The HPPC Scheme is based on the HFE trapdoor with matrix representation. This scheme proposed the construction of the HFE central map using two linearized polynomials $l_1(x)$ and $l_2(x)$ over $\mathbb{F}_{q^n}$ and computes $l_1(x) \cdot l_2(l_1(x))$ to be its central map. The idea is to use a matrix representation for HFE. We need to choose invertible matrix $\mathbf{L}_1$ and linearized polynomial $l_2(x)$ with matrix representation $\mathbf{L}_2$. The HPPC central map $l_1(x) \cdot l_2(l_1(x))$ could be computed by $\mathbf{M}(\mathbf{L}_1 \otimes \mathbf{L}_2\mathbf{L}_1)$ where $\mathbf{M} = \left(\mathbf{C}^0_{f(x)}, \ldots, \mathbf{C}^{n-1}_{f(x)}\right)$.

The HPPC scheme is multivariate-based cryptography. The HPPC central map will be hidden with two linear/affine maps $\mathbb{S}$ and $\mathbb{T}$. In this scheme, we will choose two affine map $\mathbf{S}, \mathbf{T} : \mathbb{F}_q^n \to \mathbb{F}_q^n$, an invertible matrix $\mathbf{L}_1$, and a linearized polynomial $l_2(x)$ to be its private key and compute

$$\mathcal{P} = \mathbf{TMF}(\mathbf{S} \otimes \mathbf{S})$$

with $\mathbf{F} = \mathbf{L}_1 \otimes \mathbf{L}_2\mathbf{L}_1$ to be its public key where $\mathbf{L}_2$ is the matrix representation of linearized polynomial $l_2(x)$. To get the trapdoor function $G(x)$, the HPPC scheme will compute

$$\begin{aligned}\mathcal{P}'(\mathbf{x}) &= \mathcal{P}(\mathbf{S}^{-1}\mathbf{L}_1^{-1}\mathbf{x}') \\ &= \mathbf{TM}(\mathbf{I}_n \otimes \mathbf{L}_2)(\mathbf{x}' \otimes \mathbf{x}').\end{aligned}$$

The product $\mathbf{M}(\mathbf{I}_n \otimes \mathbf{L}_2(x)$ is equal to the monic polynomial $G(x) = xl_2(x)$ over $\mathbb{F}_{q^n}$. The trapdoor of this scheme is the solution of $G(x) = Y$ for a given $Y \in \mathbb{F}_{q^n}$. This equation could be solved using Barlekamps Algorithm. The trapdoor of the HPPC scheme could be computed faster than the HFE scheme because the degree of $l_2(x)$ is much less than the HFE central map.

To sign a hash value of message $\mathcal{H}(m) := \mathbf{y}$, the HPPC scheme first selects a random $\mathbf{v} \in \mathbb{F}_q^v$, then write $\mathbf{y}' = \mathbf{y} - \mathbf{v}$. After that, use the invert map of $\mathbf{T}$ that is $\mathbf{z} = \mathbf{T}^{-1}\mathbf{y}'$ and express $\mathbf{z}$ by its polynomial representation Z. Then solve the univariate equation $xl_2(x) = Z$ over $\mathbb{F}_{q^n}$. Let X' be the solution of $xl_2(x) = Z$ and $\mathbf{x}'$ be its vector representation. The last step is computing $\mathbf{x} = \mathbf{S}^{-1}\mathbf{L}_1^{-1}\mathbf{x}'$. Then we get the sign of message m is $(\mathbf{x}, \mathbf{v})$. The verification process is computing $\mathcal{P}(\mathbf{x}) + \mathbf{v}$.

This scheme uses a vinegar vector $\mathbf{v}$ at the signing process. The vector $\mathbf{v}$ becomes a translation map at verification. The translation map at the end of the calculation utilizes the HFE trapdoor with affine map $\mathcal{T}$.

IV. HPPCv: The Modification of HPPC Using Vinegar Variables

In the HFEv, the central map HFEv with $n' = n + v$ is in the form

$$P_{z_1,\ldots,z_v}(x) = \sum_{0\leq i,j\leq n} C_{i,j}x^{q^i+q^j} + \sum_{k=0}^{n'-1} B_k(z_1,\ldots,z_v)x^{q^k} + A(z_1,\ldots,z_v)$$

where each $B_k : \mathbb{F}^v \to \mathbb{F}_{q^n}$ are a linear maps and $A_k : \mathbb{F}^v \to \mathbb{F}_{q^n}$ is a quadratic map. From the HFEv scheme, we made notes as follows:

1. The public key in HFEv is a map from $\mathbb{F}_q^{n+v}$ to $\mathbb{F}_q^n$,
2. The sign function is a map a map from $\mathbb{F}_q^n$ to $\mathbb{F}_q^{n+v}$,
3. The central maps are not unique depending on vinegar variables.

From the notes above and the construction of the HPPC scheme, we modify HPPC with vinegar modification satisfying the following conditions.

1. Matrix $\mathbf{L}_1$ be an invertible matrix and $l_2(x)$ be a linearized polynomial.
2. Polynomial $l_2'(x)$ must be monic that is the leading coefficient is 1.
3. The coefficient of monomial in $l_2'(x)$ with the least degree is quadratic map from $\mathbb{F}_q^v$ to $\mathbb{F}_{q^n}$.
4. The coefficient of other monomial in $l_2'(x)$ is linear map from $\mathbb{F}_q^v$ to $\mathbb{F}_{q^n}$.

So, we design the polynomial $l_2'(x)$ is in the form

$$l_2'(x) = l_{z_1,\ldots,z_v}(x) = x^{p^d} + \sum_{k=1}^{d-1} B_k(z_1,\ldots,z_v)x^{p^k} + A(z_1,\ldots,z_v)x$$

for $d \in \{1,\ldots,n\}$, $B_k(z_1,\ldots,z_v)$ is a linear map from $\mathbb{F}_q^v \to \mathbb{F}_{q^n}$ for all k, and $A(z_1,\ldots,z_v)$ is a quadratic map from $\mathbb{F}_q^v$ to $\mathbb{F}_{q^n}$.

Theorem 1 *Let $\mathbb{F}_{q^n}$ be a finite field. Given $Y \in \mathbb{F}_{q^n}$. If all the vinegar variables are set to 0 then the equation $xl_2'(x) = Y$ has a solution.*

Proof. If all the vinegar variables are set to 0, then we have $l_2'(x) = x^{p^d}$. In [19], a linearized polynomial $l(x)$ is a bijective function if and only if the solution of $l(x) = 0$ only $x = 0$ in $\mathbb{F}_{q^n}$. In our case, the linearized polynomial is $l_2'(x) = x^{p^d}$ and the solution of $x^{p^d} = 0$ only $x = 0$. We can conclude that $xl_2'(x)$ is a bijective function that is for any $Y \in \mathbb{F}_{q^n}$ there is $X \in \mathbb{F}_{q^n}$ such that $Xl_2'(X) = Y$. □

The chosen linearized polynomial $l_2'(x)$ has a matrix representation in $\mathbb{F}_q^{n\times n}$ with some entries in the form of the quadratic and linear map $\mathbb{F}_q^v \to \mathbb{F}_{q^n}$. By the chosen polynomial $l_2'(x)$, we can modify the HPPC scheme such that the public key becomes a map from $\mathbb{F}_q^{n+v}$ to $\mathbb{F}_q^n$.

Therefore, we can chose two invertible matrices $\mathbf{T}, \mathbf{S} \in \mathbb{F}_q^{n\times n}$, invertible matrix $\mathbf{L}_1 \in \mathbb{F}_q^{n\times n}$, and a polynomial $l_2'(x)$. We compute the public key

$$\mathcal{P}(\mathbf{x}) = \mathbf{TM}(\mathbf{L}_1 \otimes \mathbf{L}_2'\mathbf{L}_1)(\mathbf{S}\otimes\mathbf{S})(\mathbf{x}\otimes\mathbf{x})$$

where $\mathbf{L}_2'$ is a matrix representation of $l_2'(x)$. To get the trapdoor function, we compute

$$\mathbf{x} = \mathbf{S}^{-1}\mathbf{L}_1^{-1}\mathbf{x}' \tag{1}$$

where the vector $\mathbf{x}'$ is the vector representation of the solution $xl_2'(x) = Y$ for a given Y and a fixed vinegar variables. To create a signature for message m, we modify the HPPC scheme by doing the following steps.

1. Compute the hash value of message m by $\mathcal{H}(m); = \mathbf{y} \in \mathbb{F}_q^n$.
2. Compute $\mathbf{T}^{-1}\mathbf{y} := \mathbf{z}$ and express $\mathbf{z}$ as its polynomial representation $Z \in \mathbb{F}_{q^n}$.
3. Choose the vinegar variables randomly and substitute the vinegar variables to $l_{z_1,\ldots,z_v}(x)$. Now the polynomial $l_{z_1,\ldots,z_v}(x)$ becomes a polynomial with a fixed coefficient.
4. Solve the solution of $xl_{z_1,\ldots,z_v}(x) = Z$ by Barlekamp's Algorithm. If it has no solution, back to the last step.
5. Suppose the solution is X', that is $X'l_{z_1,\ldots,z_v}(X') = Z$, express X' as its vector representation. Then compute the vector $\mathbf{x} = \mathbf{S}^{-1}\mathbf{L}_1^{-1}\mathbf{x}'$.

Then the signature of message m is the vector $\mathbf{u} = (x_1,\ldots,x_n,z_1,\ldots,z_v)^T$ where the vector $(x_1,\ldots,x_n)^T = \mathbf{x}$. The signature value will become the vector in $\mathbb{F}_q^{n+v}$. Then, verification can be computed by evaluating the system $\mathcal{P}$ at vector $\mathbf{u}$, that is $\mathcal{P}(\mathbf{u})$. If $\mathcal{P}(\mathbf{u}) = \mathcal{H}(m)$ then it is valid, otherwise is not valid. We can check the calculation of the modification as follows.

$$\begin{aligned}
\mathcal{P}(\mathbf{x}) &= \mathbf{TM}(\mathbf{L}_1 \otimes \mathbf{L}_2'\mathbf{L}_1)(\mathbf{S}\otimes\mathbf{S})(\mathbf{x}\otimes\mathbf{x}) \\
&= \mathbf{TM}(\mathbf{L}_1 \otimes \mathbf{L}_2'\mathbf{L}_1)(\mathbf{S}\otimes\mathbf{S})(\mathbf{S}^{-1}\mathbf{L}_1^{-1}\mathbf{x}'\otimes\mathbf{S}^{-1}\mathbf{L}_1^{-1}\mathbf{x}') \text{ by Equation 1} \\
&= \mathbf{TM}(\mathbf{L}_1 \otimes \mathbf{L}_2'\mathbf{L}_1)(\mathbf{L}_1^{-1}\mathbf{x}'\otimes\mathbf{L}_1^{-1}\mathbf{x}') \\
&= \mathbf{TM}(\mathbf{I} \otimes \mathbf{L}_2')(\mathbf{x}'\otimes\mathbf{x}') \\
&= \mathbf{Ty} \text{ since } Y = X'l_2'(X')
\end{aligned}$$

The calculation above would correct for fixed vinegar variables and valid pair $(m, \mathcal{H}, \mathbf{u})$ where m is a message, $\mathcal{H}$ is a hash function, and $\mathbf{u}$ is a signature for m. This scheme uses parameters (n, d, v) where $n \in \mathbb{N}$ is the degree of the extension field over $\mathbb{F}_q$, $d < n$ where q^d is a degree of linearized polynomial $l_{z_1,\ldots,z_v}(x)$, and v is the number of vinegar variables. For the illustration, we made a toy example.

Example 1 We chose parameter $(n, d, v) = (4, 3, 2)$. Let $\mathbb{F}_{2^4}$ be an extension field of $\mathbb{F}_2$ generated by θ with primitive polynomial $f(x) = x^4 + x + 1$. The companion matrix of polynomial

$f(x)$ is matrix

$$\mathbf{C}_{f(x)} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

and matrix $\mathbf{M} = (\mathbf{C}^0_{f(x)}, \mathbf{C}^1_{f(x)}, \mathbf{C}^2_{f(x)}, \mathbf{C}^3_{f(x)})$. Given two invertible linear maps $\mathbf{T}, \mathbf{S} \in \mathbb{F}_2^{4\times 4}$ where

$$\mathbf{T} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix} \text{ and } \mathbf{S} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

invertible matrix $\mathbf{L}_1$ where

$$\mathbf{L}_1 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix},$$

and linearized polynomial

$$l_{z_1,z_2}(x) = x^8 + (z_1 + z_2\theta)x^4 + z_2x^2 + (z_1z_2 + z_1\theta^2)x$$

which has a matrix representation

$$\mathbf{L}_{z_1,z_2} = \begin{pmatrix} z_1z_2 + z_1 + z_2 + 1 & z_1 + 1 & z_2 & z_1 + z_2 \\ z_2 & z_1z_2 + z_1 + z_2 & z_1 + 1 & 1 \\ z_1 & 1 & z_1z_2 + z_1 & 0 \\ 0 & z_1 & z_2 & z_1z_2 + z_1 + 1 \end{pmatrix}.$$

The public key of this scheme is $\mathcal{P}(\mathbf{x}) = \mathbf{TM}(\mathbf{L}_1 \otimes \mathbf{L}_{z_1,z_2}\mathbf{L}_1)(\mathbf{S} \otimes \mathbf{S})(\mathbf{x} \otimes \mathbf{x})$. So, we get the map $\mathcal{P}(\mathbf{x})$ mapped from $\mathbb{F}_2^6$ to $\mathbb{F}_2^4$.

For signing a message m, we are doing the following steps.

1. Suppose the hash value of m is $\mathcal{H}(m) = (0, 1, 1, 1)^T := \mathbf{y}$,
2. Compute $\mathbf{z} := \mathbf{T}^{-1}\mathbf{y} = (1, 1, 0, 0)^T$ and the polynomial representation of $\mathbf{z}$ is $\theta^4 = 1 + \theta$.
3. Let the selected value for vinegar variables be $z_1 = 1$ and $z_2 = 0$. We get the polynomial $l_{1,0}(x) = x^8 + x^4 + \theta^2 x$.
4. By root finding, we get the solution of $xl_{1,0}(x) = Z$ is $X' = \theta^2$.
5. Express θ^2 as its vector representation, that is $\mathbf{x}' = (0, 0, 1, 0)^T$. Then, we get the vector $\mathbf{x} = \mathbf{S}^{-1}\mathbf{L}_1^{-1}\mathbf{x}' = (0, 0, 1, 1)^T$.

So, the signature of m is the vector $\mathbf{u} = (0, 0, 1, 1, 1, 0)^T$.

Table 1. Comparison between HPPC and HPPCv Parameters

Scheme	HPPC	HPPCv
Public key size	$\log_2 q \times \frac{n^3+n^2}{2}$	$\log_2 q \times n^3$
Private key size $(\mathbf{T}, \mathbf{S}, \mathbf{L}_1)$	$\log_2 q \times 3n^2$	$\log_2 q \times 3n^2$
Private key $l_2(x)$ degree	q^d	q^d
Public key degree	2	4

To verify the signature, we evaluate the map $\mathcal{P}$ at $\mathbf{u}$. We get $\mathcal{P}(\mathbf{u}) = (0, 1, 1, 1)^T = \mathcal{H}(m)$. We can conclude that the signature that was published is valid.

With this modification, the HPPCv public key has a degree higher than the original one. The public key system degrees are 4 with $n + v$ variables. However, the private keys are two linear maps $\mathbf{S}, \mathbf{T} \in \mathbb{F}_q^{n\times n}$, a invertible matrices $\mathbf{L}_1$, and a linearized polynomial $l_{z_1,\ldots,z_v}(x)$ over $\mathbb{F}_{q^n}$. For the comparison with HPPC's original scheme, see Table 1..

By Table 1., We modify the HPPC scheme such that the public key has a higher degree but has a similar public key size and computation cost by looking at the private key size. The modification increased the complexity of solving multivariate systems. Bouillaguet et al. compared the exhaustive search for polynomial systems and found that the higher the degree of polynomial, the longer the time takes to solve [26]. By [27], the complexity raises from $O(n^2 \cdot 2^{0.815n})$ bit operation to $O(n^2 \cdot 2^{0.9n})$ as the degree's changes from $d = 2$ into $d = 4$.

V. CONCLUSIONS AND FUTURE RESEARCH DIRECTION

The HPPC Scheme uses vinegar variables in their last affine map, which is in the translation. They did not utilize the dimensional changes. We modify the HPPC scheme using vinegar variables so that the scheme is based on the HFEv trapdoor. Our modification provides the key in terms of vinegar variables. The vinegar variables will affect the HPPCv public key, that is we will get some public keys from the selection of vinegar variables. The HPPCv public key complexity will be increased because we used to find a solution for a system of degree 4. Even though, the HPPCv center map is still a multivariate quadratic system. For the comparison, Table 1. shows that we can get a higher degree of public key even if we use the same private key size. This modification can be applied to be used for the post-quantum digital signature scheme, considering that this modification is still based on a multivariate problem. However, this modification could not match encryption because the equation in Theorem 1 is not injective.

For future research, We will analyze our modification with the known attack. With the analysis, we can check the security rate of our system. We compare the security between the modification and the original scheme. The future research direction also analyzes the HPPC Scheme with a modified attack.

ACKNOWLEDGEMENT

We would like to acknowledge the Indonesia Endowment Fund for Education (LPDP) Under the Ministry of Finance, Republik Indonesia, for its scholarship funding support.

REFERENCES

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[2] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, and D. Smith-Tone, "Status report on the third round of the NIST post-quantum cryptography standardization process," *Nist Pqc*, vol. 2022, no. 210, pp. 75–86, 2022.

[3] R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals-kyber," *NIST, Tech. Rep*, 2017.

[4] V. Lyubashevsky, L. Ducas, E. Kiltz, T. Lepoint, P. Schwabe, G. Seiler, D. Stehlé, and S. Bai, "Crystals-dilithium," *Algorithm Specifications and Supporting Documentation*, 2020.

[5] D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, and P. Schwabe, "The sphincs+ signature framework," in *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2019, pp. 2129–2146.

[6] B. G. Rodrıguez, "3wise: Cubic element-wise trapdoor based mpkc cryptosystem," *SUBMISSION TO NIST PQC*, 2023.

[7] I. Luengo and M. Avendaño, "Dme: Multivariate signature public key scheme," *SUBMISSION TO NIST PQC*, 2023.

[8] S. C. B. H. M. J. Ward Beullens, Fabio Campos, "Mayosubmitters," *SUBMISSION TO NIST PQC*, 2023.

[9] J.-C. Faugere, P.-A. Fouque, R. Larrieu, G. Macario-Rat, B. Minaud, and J. Patarin, "Prov: Provable unbalanced oil and vinegar specification v1. 0–06/01/2023," *SUBMISSION TO NIST PQC*, 2023.

[10] H. Furue, Y. Ikematsu, F. Hoshino, T. Takagi, K. Yasuda, T. Miyazawa, T. Saito, and A. Nagai, "Qr-uov," *Specification document of NIST PQC Standardization of Additional Digital Signature Scheme*, 2023.

[11] L.-C. Wang, C.-Y. Chou, J. Ding, Y.-L. Kuan, J. A. Leegwater, M.-S. Li, B.-S. Tseng, P.-E. Tseng, and C.-C. Wang, "A note on the snova security," *Cryptology ePrint Archive*, 2024.

[12] B. G. Rodriguez, "HPPC: Hidden Product of Polynomial Composition," *Nist Pqc*, pp. 1–30, 2023.

[13] T. Matsumoto and H. Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 330 LNCS, pp. 419–453, 1988.

[14] J. Patarin, "Hidden Field 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, 1996.

[15] A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced oil and vinegar signature schemes," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 1592, pp. 206–222, 1999.

[16] C. Wolf and B. Preneel, *Multivariate Quadratic Polynomials in Public Key Cryptography*, 2005, no. November. [Online]. Available: http://dblp.uni-trier.de/db/journals/iacr/iacr2005.html#WolfP05a

[17] A. Casanova, J.-C. Faug'ere, G. Macario-Rat, J. Patarin, L. Perret, and J. Ryckeghem, *GeMSS: A Great Multivariate Short Signature*, 2017. [Online]. Available: https://www-polsys.lip6.fr/Links/NIST/GeMSS_specification.pdf

[18] W. A. Adkins and S. H. Weintraub, *Algebra: An Approach via Module Theory*. Springer New York, 1995, vol. 79, no. 484.

[19] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed. Cambridge University Press, 1996, vol. 20.

[20] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed., 2004, vol. 4, no. 1.

[21] B. N. Cooperstein, *Advanced Linear Algebra*. Taylor & Francis, 1967.

[22] A. Graham, *Kronecker products and matrix calculus with applications*. Courier Dover Publications, 2018.

[23] W.-H. Steeb and T. K. Shi, *Matrix Calculus and Kronecker Product with Applications and C++ Programs*. World Scientific Publishing Co., 1997.

[24] A. Kipnis and A. Shamir, "Cryptanalysis of the HFE Public Key Cryptosystem," in *Advances in Cryptology, Proceedings of Crypto*, vol. 99, 1999, pp. 19–30.

[25] C. Wolf and B. Preneel, "Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations." *IACR Cryptology ePrint Archive*, vol. 2005, p. 77, 2005. [Online]. Available: http://dblp.uni-trier.de/db/journals/iacr/iacr2005.html#WolfP05

[26] C. Bouillaguet, H.-C. Chen, C.-M. Cheng, T. Chou, R. Niederhagen, A. Shamir, and B.-Y. Yang, "Fast exhaustive search for polynomial systems in," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2010, pp. 203–218.

[27] I. Dinur, "Cryptanalytic applications of the polynomial method for solving multivariate equation systems over gf (2)," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2021, pp. 374–403.