# Kipnis-Shamir Attack on Unbalanced Oil-Vinegar Scheme

Weiwei Cao[1], Lei Hu[1], Jintai Ding[2,3], and Zhijun Yin[2]

[1] State Key Laboratory of Information Security,
Graduate School of Chinese Academy of Sciences, Beijing 100049, China
[2] University of Cincinnati, OH 45221, USA
[3] South China University of Technology, Guangzhou 510640, China
{wwcao,hu}@is.ac.cn, jintai.ding@uc.edu, yinz@ohio.edu

**Abstract.** The public key of the Oil-Vinegar scheme consists of a set of $m$ quadratic equations in $m+n$ variables over a finite field $\mathbb{F}_q$. Kipnis and Shamir broke the balanced Oil-Vinegar scheme where $d = n-m = 0$ by finding equivalent keys of the cryptosytem. Later their method was extended by Kipnis et al to attack the unbalanced case where $0 < d < m$ and $d$ is small with a complexity of $O(q^{d-1}m^4)$. This method uses the matrices associated with the quadratic polynomials in the public key, which needs to be symmetric and invertible. In this paper, we give an optimized search method for Kipnis el al's attack. Moreover, for the case that the finite field is of characteristic 2, we find the situation becomes very subtle, which, however, was totally neglected in the original work of Kipnis et al. We show that the Kipnis-Shamir method does not work if the field characteristic is 2 and $d$ is a small odd number, and we fix the situation by proposing an alternative method and give an equivalent key recovery attack of complexity $O(q^{d+1}m^4)$. We also prove an important experimental observation by Ding et al for the Kipnis-Shamir attack on balanced Oil-Vinegar schemes in characteristic 2.

**Keywords:** multivariate public key cryptosystem, signature scheme, Oil-Vinegar scheme, Kipnis-Shamir attack.

## 1 Introduction

Public key cryptography (PKC) has opened a new era of cryptography since Diffie and Hellman presented their new idea in "New Directions in Cryptography" in 1976 [3]. The classic trapdoors of PKC are based on the difficulty of factorization of integers for RSA and discrete logarithm for ElGamal and ECC. However, with the arrival of quantum computer, these systems can be broken easily by quantum computer attacks [12]. Therefore, leading experts have joined forces to develop post-quantum cryptography including hash-based cryptography [2], code-based cryptography [9], lattice-based cryptography [7], and multivariate cryptography [4].

The public key of multivariate public key cryptosystems (MPKC) is a set of quadratic polynomials and its security relies on the difficulty of solving polynomial systems, which has been proved to be an NP-hard problem in general

F. Bao and J. Weng (Eds.): ISPEC 2011, LNCS 6672, pp. 168–180, 2011.

and has a potential to resist against quantum computer attack. MPKC has also become one of the promising alternatives for RSA due to its advantage on implementation on resource restricted devices. As compared with RSA, the computation in MPKC can be implemented very fast since it is operated on a small finite field [11].

For the merit of simple and fast implementation, multivariate public key cryptosystems attracts a lot of attention and has been a hot topic over the last few years. Amongst MPKC systems unbalanced Oil-Vinegar [10] is one of the most important signature schemes.

The Oil-Vinegar scheme is proposed by Patarin in 1997. Its trapdoor is a set of easy-to-invert quadratic polynomials in two kinds of variables: Oil and Vinegar variables over a finite field $\mathbb{F}_q$, which are called Oil-Vinegar polynomials. The public key is formed by composing the Oil-Vinegar polynomial and a linear transformation, and the latter is used to hide the special structure of the Oil-Vinegar polynomial. The trapdoor of the Oil-Vinegar scheme is highly efficient to invert but can be randomly produced, and therefore its public key polynomials are immune to structural attacks like differential attack [6] or linearization attack [5].

Let $m$ and $n$ be the numbers of the Oil and Vinegar variables respectively and let $n = m + d$. Kipnis and Shamir [8] analyzed the balanced Oil-Vinegar scheme where $d = 0$, and found an equivalent key attack with complexity of $O(m^4)$. Later, their method was extended to deal with the unbalanced case where $0 < d < m$ and $d$ is small with complexity of $O(q^{d-1}m^4)$ [1]. We find it can be refined by an optimized search method. However, it turns out that their attack does not really work in the case when the finite field is of characteristic 2 and $d$ is a small odd number, because they neglect a very important fact that the matrices they used in the attack must be symmetric and invertible.

In this paper, we fix the bug of their method in this case and give an equivalent key recovery attack. The complexity of the attack is $O(q^{d+1}m^4)$. In addition, we give a theoretical proof of the key observation in [4], which implies the Kipnis-Shamir attack needs modification in the even characteristic balanced Oil-Vinegar case and this motivates the present paper.

We organize the paper as follows. We describe the Oil-Vinegar scheme in Section 2. In Section 3, we will briefly review the Kipnis-Shamir attack on the Oil-Vinegar scheme [8]. In Section 4 we present a method to improve Kipnis et al's attack and a method to fix the attack on unbalanced Oil-Vinegar scheme when the field characteristic is two. A theoretical proof for the Ding et al's observation which is stated in Subsection 3.2 is given in Section 5. Finally, we concludes the paper in Section 6.

## 2 The Oil-Vinegar Scheme

Let $\mathbb{K} = \mathbb{F}_q$ be a finite field of $q$ elements, and $n$ and $m$ be two integers. Let $F$ be a set of $m$ quadratic polynomials in $n + m$ variables $x_1, \cdots, x_{n+m}$ over $\mathbb{K}$, and $S$ be an invertible $(n + m) \times (n + m)$ matrix over $\mathbb{K}$. Then a public key $P$ of the Oil-Vinegar scheme is a set of $m$ quadratic polynomials in the variables

$x = (x_1, \cdots, x_{n+m})$, which is formed by composing the mappings of $S$ and $F$: $P(x) = F(xS)$. The secret key is $S$ and $F$.

The quadratic polynomial map $F$ needs to be easy to invert, and to this goal, its each polynomial is specifically produced as a so-called Oil-Vinegar polynomials of the form

$$Q_k(x) = \sum_{1 \le i \le j \le n} {a_{ij}}^{(k)} x_i x_j + \sum_{1 \le i \le n, n+1 \le j \le n+m} b_{ij}^{(k)} x_i x_j + \text{affine terms}.$$

Here the variables are partitioned into two parts: $x_1, \cdots, x_n$ (called Vinegar variables) and $x_{n+1}, \cdots, x_{n+m}$ (called Oil variables), such that there are no quadratic terms in the Oil variables involved. Hence, when the Vinegar variables are taken values, then from the evaluation of $F$ one can easily find the value of the Oil variables by solving a linear system on them. The coefficients of $F$ need to be secret and not public.

The secret matrix $S$ is used to hide the Oil-Vinegar structure of $F$ to get a random-looking quadratic polynomial set $P$.

**Signature generation of the Oil-Vinegar scheme:** Let $u = (u_1, \cdots, u_m) \in \mathbb{K}^m$ be the message to be signed. Randomly choose $x_1, \cdots, x_n$ over $\mathbb{K}$ and solve the linear system on the Oil variables $x_{n+1}, \cdots, x_{n+m}$,

$$F(x_1, \cdots, x_n, x_{n+1}, \cdots, x_{n+m}) = (u_1, \cdots, u_m),$$

to get a value of the Oil variables $x_{n+1}, \cdots, x_{n+m}$. If this system has no solution (this happens with a negligible probability), try another tuple of $x_1, \cdots, x_n$. Then compute $(y_1, \cdots, y_{n+m}) = (x_1, \cdots, x_{n+m})S^{-1}$ to get the signature.

**Signature verification of the Oil-Vinegar scheme:** To verify whether a signature $(y'_1, \cdots, y'_{n+m})$ is valid for the message $(u_1, \cdots, u_m)$ or not, verify the equality $P(y'_1, \cdots, y'_{n+m}) = (u_1, \cdots, u_m)$ holds or not.

## 3 Kipnis-Shamir Attack on the Balanced Oil-Vinegar Scheme

An Oil-Vinegar scheme is called a balanced Oil-Vinegar scheme if $n = m$. Kipnis and Shamir introduced an equivalent key recovery attack on the balanced Oil-Vinegar scheme [8].

Let the same notation $S$ denote the linear mapping corresponding to the matrix $S$. We say a tuple of an Oil-Vinegar mapping $F'$ and an invertible matrix $S'$ to be an equivalent key of $(F, S)$ if the composition $P = F \circ S = F' \circ S'$ holds. Finding equivalent keys is essential to the Kipnis-Shamir attack and to our improvement in the next section.

### 3.1 Kipnis-Shamir Attack on Odd Characteristic Balanced Oil-Vinegar Scheme

Assume $\mathbb{K}$ is of odd characteristic. A homogeneous quadratic polynomial of the form $\sum_{1 \le i \le j \le n+m} a_{ij} x_i x_j$ can be written as $xUx^T$, where $x = (x_1, \cdots, x_{n+m})$, the

superscript $T$ denotes the transpose of vectors and matrices, $U$ is the symmetric matrix of order $n+m$ with $a_{ii}$ as its $(i,i)$ entry and $a_{ij}/2$ as its $(i,j)$ and $(j,i)$ entries for $i \neq j$. $U$ is called the associated symmetric matrix of the quadratic polynomial. If the polynomial is an Oil-Vinegar polynomial, then its associated matrix has the following special structure as

$$\begin{pmatrix} A & B \\ B^T & 0 \end{pmatrix}, \tag{1}$$

where $A$ is a symmetric matric of order $n$, $B$ is an $n \times m$ matrix.

Let $Q_i$ and $W_i$ denote the associated symmetric matrix of the homogeneous quadratic part of the $i$-th polynomial in $F$ and in $P$, respectively. Since $P(x) = F(xS)$, we have $W_i = SQ_iS^T$.

**Definition 1.** *Let $\mathcal{V}$ be the $n$-dimensional linear subspace of all vectors in $\mathbb{K}^{n+m}$ whose last $m$ entries are zeros, and $\mathcal{O}$ be the $m$-dimensional linear subspace of all vectors in $\mathbb{K}^{n+m}$ whose first $n$ entries are zeros.*

*The Oil space $\tilde{\mathcal{O}}$ is the image of $\mathcal{O}$ under the linear mapping by $S^{-1}$, and Vinegar space $\tilde{\mathcal{V}}$ is the image of $\mathcal{V}$ under the linear mapping by $S^T$.*

Obviously, we have

**Lemma 1.** *For each $i$, $Q_i$ maps $\mathcal{O}$ into $\mathcal{V}$, and for any two vectors $o$ and $o'$ in $\mathcal{O}$, $oQ_io'^T = 0$ holds.*

From $W_i = SQ_iS^T$, we have immediately the following

**Corollary 1.** *For each $i$, we have*
*(i) $W_i$ maps $\tilde{\mathcal{O}}$ into $\tilde{\mathcal{V}}$;*
*(ii) For any two vectors $o$ and $o'$ in $\tilde{\mathcal{O}}$, $oW_io'^T = 0$ holds.*

By Corollary 1, if we can recover the Oil space $\tilde{\mathcal{O}}$, then write the $m$ vectors of its one basis as the last $m$ rows of an invertible matrix $M$, then $P \circ M$ is again an Oil-Vinegar mapping since each of their corresponding associated matrix is $MW_iM^T$, which is of the form

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} S^{-1} S \begin{pmatrix} A & B \\ B^T & 0 \end{pmatrix} S^T (S^{-1})^T \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} = \begin{pmatrix} * & * \\ * & 0 \end{pmatrix}.$$

Hence, $(P \circ M, M^{-1})$ is an equivalent key of $(F, S)$, which can be used to arbitrarily forge a valid signature. Thus, recovering $\tilde{\mathcal{O}}$ is a key point for finding equivalent keys and breaking the scheme. The Kipnis-Shamir attack utilized the special structure of the associated symmetric matrices of the Oil-Vinegar polynomials to recover $\tilde{\mathcal{O}}$ [8].

Let $Q_i = \begin{pmatrix} A & B \\ B^T & 0 \end{pmatrix}$ and $B$ be invertible. Then $Q_i^{-1} = \begin{pmatrix} 0 & (B^T)^{-1} \\ B^{-1} & -B^{-1}A(B^T)^{-1} \end{pmatrix}$. So we can assume $Q_j^{-1} = \begin{pmatrix} 0 & D \\ D^T & C \end{pmatrix}$, where $A$ and $C$ are symmetric, and $B$ and $D$ are invertible matrices over $\mathbb{K}$ of order $m$. For any pair of an invertible

matrix $Q_j$ and a matrix $Q_i$, define $Q_{ij} = Q_i Q_j^{-1}$ and correspondingly define $W_{ij} = W_i W_j^{-1}$. Thus, $Q_{ij} = \begin{pmatrix} BD^T & AD + BC \\ 0 & B^T D \end{pmatrix}$. Since $W_{ij} = SQ_{ij}S^{-1}$ and $BD^T = B(B^T D)^T B^{-1}$, the characteristic polynomials of $Q_{ij}$ and $W_{ij}$ are the same and are the square of that of $BD^T$. Let $g_{ij}(x) = c_0 + c_1 x + \cdots + c_m x^m$ be the characteristic polynomial of $BD^T$ (it depends on $Q_i$ and $Q_j$). Then for operations on block upper-triangular matrices, we have

$$g_{ij}(Q_{ij}) = \begin{pmatrix} 0 & U \\ 0 & 0 \end{pmatrix}, \tag{2}$$

where $U$ is an $m \times m$ matrix with a complicated expression in terms of $A, B, C$ and $D$. $U$ is shown by computer experiment to be invertible with a probability almost to 1. If $U$ is invertible, then $\mathcal{O}$ is exactly the kernel space of $g_{ij}(Q_{ij})$. Correspondingly, $\tilde{\mathcal{O}} = \mathcal{O}S^{-1}$ is exactly the kernel space of $g_{ij}(W_{ij}) = Sg_{ij}(Q_{ij})S^{-1}$. Thus, to recover $\tilde{\mathcal{O}}$, we need only a pair of invertible $W_i$ and $W_j$ $(i \neq j)$, with the property that $\mathrm{rank}(g_{ij}(W_i W_j^{-1})) = m$ for the square root factor $g_{ij}(x)$ of the characteristic polynomial of $W_i W_j^{-1}$, and then compute the kernel space of $g_{ij}(W_i W_j^{-1})$ as $\tilde{\mathcal{O}}$.

### 3.2 Kipnis-Shamir Attack on Even Characteristic Balanced Oil-Vinegar Scheme

The point of the Kipnis-Shamir attack is to use the *invertible* and *symmetric* associated matrices of the public key polynomials to find the hidden Oil space. For the case that the field characteristic is 2, Ding et al [4] define the associated symmetric matrix of a quadratic polynomial $\sum_{1 \leq i \leq j \leq n+m} a_{ij} x_i x_j$ as the matrix with zero diagonal and with $a_{ij}$ as its $(i, j)$ and $(j, i)$ entries. However, it is pointed out in [4] when the field characteristic is 2, the corresponding $g_{ij}(Q_{ij}) = 0$ always holds by numerical experiment. In Section 5, we give a theoretical proof of this fact. Thus, Ding et al have to propose an alternative method to make the Kipnis-Shamir attack work. It depends on the existence of low degree factors (e.g., a linear factor) of the characteristic polynomial of $BD^T$ since the method needs to search an eigenspace of $W_{ij}$ to find an eigenvector to generate the whole Oil space under the action of $W_{ij}$, and the corresponding eigenvalue should be of low multiplicity in the characteristic polynomial to make the eigenspace as small as possible. Ding et al's modified method, of course, relies on the invertibility of associated symmetric matrices.

## 4 Improvement of Kipnis-Shamir Attack on Unbalanced Oil-Vinegar Scheme

### 4.1 Improvement on Odd Characteristic Unbalanced Scheme

Let $n = m + d$ and $d$ be small. By observing the fact that $\tilde{\mathcal{O}}$ is an invariant subspace of $W_{ij}$, Kipnis et al [1] extended the original idea of [8] and proved

that when $0 < d < m$ and $d$ is small, there exists a subspace of $\tilde{\mathcal{O}}$ as an invariant subspace of a $W_{ij}$ with a probability $\geq \frac{q-1}{q^{2d}-1}$, furthermore, the probability that a one-dimensional subspace of $\tilde{\mathcal{O}}$ is an invariant subspace of $W_{ij}$ is about $q^{-d}$. They then utilized these invariant subspaces of the Oil space to recover $\tilde{\mathcal{O}}$ in a complexity $O(q^{d-1}m^4)$. Here we call the attack as the extended Kipnis-Shamir attack.

**Optimized Search Method:** Below we give an optimized method for the search of independent vectors of the Oil space $\tilde{\mathcal{O}}$ in the extended Kipnis-Shamir attack. The point is as follows. Let $o$ be a vector in $\tilde{\mathcal{O}}$, $K_o$ denote the space of the solution vectors $x = (x_1, \cdots, x_{n+m})$ of the linear system $oW_i x^T = 0$ $(1 \leq i \leq m)$. By Corollary 1(ii), $K_o$ always contains the Oil space $\tilde{\mathcal{O}}$. Obviously, the dimension of $K_o$ is greater than or equal to $n$, and is $n$ for most randomly chosen $o$.

Let $o_1 = o$. To decrease the space $K_{o_1}$ to find out $\tilde{\mathcal{O}}$, we need another vector $o_2$ in $\tilde{\mathcal{O}}$ and calculate $K_{o_1} \bigcap K_{o_2}$. If $o_1$ and $o_2$ are linearly independent, then $K_{o_1} \bigcap K_{o_2}$ obviously be more close to the desired Oil space. This $o_2$ may have been found yet in a previous step of the extended Kipnis-Shamir attack, otherwise, we can try a randomly chosen vector $o_2$ in $K_{o_1}$ and test whether the system $o_1 W_i o_2^T = 0$ $(1 \leq i \leq m)$ holds or not, if not, this $o_2$ is not in $\tilde{\mathcal{O}}$ by Corollary 1(ii), and if the test holds, this $o_2$ is generally in the Oil space. The probability of a successful try is generally $q^m/q^n = q^{-d}$. Continue this process, we take a third vector in $\tilde{\mathcal{O}}$, which is found in the previous steps of the extended Kipnis-Shamir attack or is taken from $K_{o_1} \bigcap K_{o_2}$, and calculate $K_{o_1} \bigcap K_{o_2} \bigcap K_{o_3}$, and take an $o_4$ and so on until we find out $K_{o_1} \bigcap \cdots \bigcap K_{o_t}$ is of dimension $m$, which must be the desired Oil space. Our experiment shows $t = 2$ is enough to recover the Oil space.

Using the above optimized search method, an improved extended Kipnis-Shamir attack is given as follows:

1. Produce the associated symmetric matrices $W_1, \cdots, W_m$ for the homogeneous quadratic parts of the $m$ public key polynomials. Let $\Gamma$ be the empty set.
2. Randomly choose two different matrices from the linear combinations of $W_1, \cdots, W_m$, and one of them is invertible. Still denote them by $W_i$ and $W_j$ ($W_j$ is inverible). Calculate $W_{ij} = W_i W_j^{-1}$.
3. Compute the characteristic polynomial of $W_{ij}$ and find its linear factors with multiplicity 1. Denote such factors by $h(x)$. Compute each kernel of the corresponding $h(W_{ij})$.
4. For vectors in the kernels in Step 3, use $oW_i o^T = 0$ $(1 \leq i \leq m)$ to test out the vectors that belong to $\tilde{\mathcal{O}}$. Choose linearly independent vectors among them and append them to the set $\Gamma$.
5. If $\Gamma$ is empty or contains only an element, go back to Step 2.
6. If necessary, find more vectors $o_3, \cdots, o_t$. Calculate $K_{o_1} \bigcap \cdots \bigcap K_{o_t}$ to find out the Oil space $\tilde{\mathcal{O}}$.
7. Write arbitrarily a basis of $\tilde{\mathcal{O}}$ into the last $m$ rows of an invertible matrix $M$. Then $P \circ M$ is an Oil-Vinegar map and $(P \circ M, M^{-1})$ is an equivalent private key.

Steps 1-4 are a part of phases of the extended Kipnis-Shamir attack, the complexity is at most $O(q^{d-1}m^4)$. Step 6 is linear algebra computation, its complexity is at most $O(m^4)$.

### 4.2 Kipnis-Shamir Attack on Even Characteristic Unbalanced Scheme

When the field characteristic is 2 and $d$ is a small odd number, both the original and modified Kipnis-Shamir attacks [1] [4] do not work since in this case, $n+m = 2m+d$ is an odd number but any symmetric matrix with zero diagonal over a characteristic two field must have an even rank, which means it is definitely not invertible.

To fix the problem, our strategy is to let the associated matrices still be symmetric but with nonzero diagonals.

Let $W_1, \cdots, W_m$ be the associated symmetric matrices of the public key polynomials as in Subsection 3.2. Let $W_i' = W_i + D$, $1 \leq i \leq m$, where $D$ is the matrix with almost full zero entries except the $(1,1)$ entry is 1. Now we use $W_1', \cdots, W_m'$ as the associated symmetric matrices of the public key polynomials. Denote $Q_i' = S^{-1}W_i'S^{-1^T}$. Since $W_i = SQ_iS^T$, then $Q_i' = Q_i + S^{-1}DS^{-1^T}$.

It is easy to see $\text{rank}(D) = 1$ and $\text{rank}(S^{-1}DS^{-1^T}) = 1$. Let $r$ denote any nonzero row of $S^{-1}DS^{-1^T}$.

**Definition 2.** *Let $\mathcal{V}'$ be the linear space spanned by $\mathcal{V}$ and $r$ and $\tilde{\mathcal{V}}'$ be the image space of $\mathcal{V}'$ by $S^T$.*

It is easy to see that the dimensions of $\mathcal{V}'$ and $\tilde{\mathcal{V}}'$ are the same and are generally equal to $n+1$.

**Lemma 2.** *For each $i$, $Q_i'$ maps $\mathcal{O}$ to a subspace of $\mathcal{V}'$ and $W_i'$ maps $\tilde{\mathcal{O}}$ to a subspace of $\tilde{\mathcal{V}}'$.*

*Proof.* Since $Q_i' = Q_i + S^{-1}DS^{-1^T}$, by Lemma 1, $Q_i$ maps $\mathcal{O}$ to a subspace $\mathcal{V}$ and $S^{-1}DS^{-1^T}$ maps $\mathcal{O}$ to the one-dimensional subspace spanned by $r$, thus $Q_i'$ maps $\mathcal{O}$ to a subspace of $\mathcal{V}'$. The last statement follows from the first one by $W_i' = SQ_i'S^T$. □

**Definition 3.** *For any $Q_i'$ and any invertible $Q_j'$, define $Q_{ij}' = Q_i'Q_j'^{-1}$. Correspondingly, for any $W_i'$ and any invertible $W_j'$ define $W_{ij}' = W_i'W_j'^{-1}$.*

It is easy to see that $W_{ij}' = SQ_{ij}'S^{-1}$. To prove that $W_{ij}'$ has a nontrivial one-dimensional invariant subspace belonging to $\tilde{\mathcal{O}}$ with a non-negligible probability, we use the following lemma.

**Lemma 3.** *(Lemma 3.2.4 in [4]) Let $\varphi : \mathbb{K}^{n+m} \to \mathbb{K}^{n+m}$ be a randomly chosen invertible $\mathbb{K}$-linear map such that: (i) There exist two subspaces $A$ and $B$ in $\mathbb{K}^{n+m}$ such that the dimension of $A$ is $n$, and the dimension of $B$ is $m$ and $B \subset A$; (ii) $\varphi(B) \subset A$. Then the probability that $\varphi$ has a nontrivial one-dimensional invariant subspace in $B$ is no less than $q^{m-n}$.*

By Lemma 3, we have

**Theorem 1.** *The probability that $W'_{ij}$ has a nontrivial one-dimensional invariant subspace in $\tilde{\mathcal{O}}$ is about $\frac{1}{q^{d+1}}$.*

*Proof.* Since $W'_{ij} = SQ'_{ij}S^{-1}$ and $\tilde{\mathcal{O}}$ is the image of $\mathcal{O}$ by $S^{-1}$, then we only need to show the probability that $Q'_{ij}$ has a nontrivial one-dimensional subspace in $\mathcal{O}$ is no less than $\frac{1}{q^{d+1}}$. By Lemma 2, $Q'_i$ and $Q'_j$ respectively map $\mathcal{O}$ to two subspaces of $\mathcal{V}'$. The dimension of the intersection of these two subspaces is at least $m+m-(n+1) = m-d-1$. Let $B$ be the inverse-image of the intersection by $Q'^{-1}_i$, $A = \mathcal{O}$ and $\varphi = Q'_{ij}$. Then the statement follows by Lemma 3. □

By Theorem 1, we use the kernel of linear factors of the characteristic polynomial of $W'_{ij}$ to recover one-dimensional subspaces of $\tilde{\mathcal{O}}$. Similarly as the attack stated in Subsection 4.1, the whole attack is as follows:

1. Produce the associated symmetric matrices $W_1, \cdots, W_m$ and $W'_1, \cdots, W'_m$ for the homogeneous quadratic parts of the $m$ public key polynomials. Let $\Gamma$ be the empty set.
2. Randomly choose two different matrices from the linear combinations of $W'_1, \cdots, W'_m$, and one of them is invertible. Still denote them by $W'_i$ and $W'_j$ ($W'_j$ is inverible). Calculate $W'_{ij} = W'_i W'^{-1}_j$.
3. Compute the characteristic polynomial of $W'_{ij}$ and find its linear factors with multiplicity 1. Denote such factors by $h(x)$. Compute each kernel of the corresponding $h(W'_{ij})$.
4. For vectors in the kernels in Step 3, use $oW_i o^T = 0$ $(1 \leq i \leq m)$ to test out the vectors that belong to $\tilde{\mathcal{O}}$. Choose linearly independent vectors among them and append them to the set $\Gamma$.
5. If $\Gamma$ is empty or contains only an element, go back to Step 2. If $\Gamma$ contains more than 2 elements, go to Step 6.
6. Use the optimized search method on $\Gamma$ as in Subsection 4.1 to find out the Oil space $\tilde{\mathcal{O}}$.
7. Write arbitrarily a basis of $\tilde{\mathcal{O}}$ into the last $m$ rows of an invertible matrix $M$. Then $P \circ M$ is an Oil-Vinegar map and $(P \circ M, M^{-1})$ is an equivalent private key.

The complexity depends on Steps 2–5. By Theorem 1, Step 5 succeeds in finding a vector of $\tilde{\mathcal{O}}$ with a probability with no less than $\frac{1}{q^{d+1}}$, then the complexity of Steps 2–5 is about $O(q^{d+1}m^4)$. Thus, the complexity of the above attack is $O(q^{d+1}m^4)$.

## 5 Proof of the Fact that $g_{ij}(Q_{ij}) = 0$

Here we use the terminology of sequence of matrices to theoretically prove the experimental observation $g_{ij}(Q_{ij}) = 0$ in Subsection 3.2 holds. When $\mathbb{K}$ is of characteristic two, by the definition of associated symmetric matrices described

in Subsection 3.2, we can get $Q_{ij} = \begin{pmatrix} BD^T & AD+BC \\ 0 & B^TD \end{pmatrix}$. Here $A$ and $C$ are symmetric matrices with zero diagonals of order $m$ and $B$ and $D$ are random matrices of order $m$. Again since $BD^T = B(B^TD)^TB^{-1}$, the characteristic polynomials of $Q_{ij}$ and $W_{ij}$ are the square of that of $BD^T$. Let $g_{ij}(x) = c_0 + c_1x + \cdots + c_mx^m$ be the characteristic polynomial of $BD^T$ (it depends on $Q_i$ and $Q_j$). Then for operations on block upper-triangular matrices, we also have

$$g_{ij}(Q_{ij}) = \begin{pmatrix} 0 & U \\ 0 & 0 \end{pmatrix}$$

To prove $g_{ij}(Q_{ij}) = 0$ we need to prove $U = 0$. If one wishes, $U$ can be expressed as

$$U = \sum_{i=1}^{m} c_i \sum_{j=0}^{i-1} \left( (BD^T)^{i-1-j} A (DB^T)^j D + B(D^TB)^{i-1-j} C (B^TD)^j \right).$$

But this expression is hard to be used to prove $U = 0$.

Let $\mathbf{S} = (M_0, M_1, M_2, \cdots)$ be an infinite sequence of $n \times m$ matrices over a field $\mathbb{K}$. Define a left shift operation $x$ on $\mathbf{S}$ as $x\mathbf{S} = (M_1, M_2, M_3, \cdots)$ and an operation of left multiplication by an $n \times n$ matrix $A$ as $A\mathbf{S} = (AM_0, AM_1, AM_2, \cdots)$. Clearly, these two operations are commutative, that is, $A(x\mathbf{S}) = x(A\mathbf{S})$. Naturally define the action of a monomial on $\mathbf{S}$ as $x^2\mathbf{S} = x(x\mathbf{S})$, $x^3\mathbf{S} = x(x^2\mathbf{S})$, $\cdots$, and the action of a polynomial $f(x) = a_kx^k + a_{k-1}x^{k-1} + \cdots + a_0$ on $\mathbf{S}$ as $f(x)\mathbf{S} = a_kx^k\mathbf{S} + a_{k-1}x^{k-1}\mathbf{S} + \cdots + a_0\mathbf{S}$. There are the following simple facts: (1) If $(x-A)\mathbf{S} = \mathbf{0}$ is the full zero-matrix sequence, then $\mathbf{S} = (U, AU, A^2U, A^3U, \cdots)$ for some $n \times m$ matrix $U$; and (2) If $f(x)$ is the characteristic polynomial of an $n \times n$ matrix $A$ and $\mathbf{S} = (I, A, A^2, A^3, \cdots)$, then $f(x)\mathbf{S} = \mathbf{0}$.

Let $A, M$ and $B$ be respectively $n \times n$, $n \times m$ and $m \times m$ matrices, for a block matrix $Q = \begin{pmatrix} A & M \\ 0 & B \end{pmatrix}$, the sequence $\mathbf{S}_{A,B;M}$ of the upper-right matrices of $Q^i$ $(i = 0, 1, 2, \cdots)$ is

$$(0, M, AM + MB, A^2M + AMB + MB^2, \cdots, \sum_{j=0}^{i-1} A^{i-1-j} M B^j, \cdots). \tag{3}$$

For fixed $A$ and $B$, $\mathbf{S}_{A,B;M}$ is linear on $M$, that is,

$$\mathbf{S}_{A,B;M+M'} = \mathbf{S}_{A,B;M} + \mathbf{S}_{A,B;M'}.$$

Let $\mathbf{S} = \mathbf{S}_{A,B;M}$. Clearly,

$$(x - A)\mathbf{S} = M(I, B, B^2, B^3, \cdots).$$

Let $g(x)$ be the characteristic polynomial of $B$ and acting with it on the both sides of the above equality, we have

$$(x - A)(g(x)\mathbf{S}) = g(x)((x - A)\mathbf{S}) = M(g(x)(I, B, B^2, B^3, \cdots)) = M\mathbf{0} = \mathbf{0}.$$

By the fact mentioned above, there exists an $n \times m$ matrix $U$ such that

$$g(x)\mathbf{S} = (U, AU, A^2U, A^3U, \cdots). \tag{4}$$

Further, assume $f(x)$ is the characteristic polynomial of $A$, then

$$f(x)g(x)\mathbf{S} = \mathbf{0}. \tag{5}$$

This equality is of course obvious by applying the Hamilton-Cayley theorem to $Q$.

Below we always assume $M$ is an *alternate matrix*, i.e., a skew-symmetric square matrix (namely $M^T = -M$) with zero diagonal. This is equivalent to say that $M$ is exactly a skew-symmetric matrix if the underlying field is of odd characteristic or $M$ is a symmetric square matrix with zero diagonal if the underlying field is of even characteristic.

**Lemma 4.** *Let $A$ and $M$ be two $n \times n$ matrices, and $M = (m_{ij})_{1 \le i,j \le n}$ be alternate.*

*(i) Assume* $A = \begin{pmatrix} \lambda & 0 & 0 & \cdots & 0 \\ 1 & \lambda & 0 & \cdots & 0 \\ 0 & 1 & \lambda & \cdots & 0 \\ & & \cdots & & \\ 0 & 0 & \cdots & 1 & \lambda \end{pmatrix}$ *is a Jordan matrix. If $AM$ is an alternate matrix, then $M = 0$.*

*(ii) Each entry of the matric sequence $\mathbf{S}_{A,A^T;M}$ is an alternate matrix.*

*(iii) Assume $f(x)$ is the characteristic polynomial of $A$ and* $Q = \begin{pmatrix} A & M \\ 0 & A^T \end{pmatrix}$. *Then $f(Q) = 0$.*

*Proof.* (i) For any $2 \le i \le n$, the $(i,i)$-entry of $AM$ is zero, that is, $m_{i-1,i} + \lambda m_{i,i} = 0$. Hence, $-m_{i,i-1} = m_{i-1,i} = 0$ since $m_{i,i} = 0$. For any $3 \le i \le n$, the sum of the $(i-1,i)$- and the $(i,i-1)$-entries of $AM$ is zero, that is, $m_{i-2,i} + \lambda m_{i-1,i} + m_{i-1,i-1} + \lambda m_{i,i-1} = 0$. Hence, $-m_{i,i-2} = m_{i-2,i} = 0$ since $m_{i-1,i} = m_{i-1,i-1} = m_{i,i-1} = 0$. Similarly, for any $4 \le i \le n$, since the sum of the $(i-2,i)$- and the $(i,i-2)$-entries of $AM$ is zero, we have $m_{i-3,i} + \lambda m_{i-2,i} + m_{i-1,i-2} + \lambda m_{i,i-2} = 0$ and $-m_{i,i-3} = m_{i-3,i} = 0$. This process can be continued until all entries of $M$ are proved to be zero.

(ii) We can easily check $\sum_{j=0}^{i-1} A^{i-1-j} M (A^T)^j$ is skew-symmetric by the fact $M^T = -M$ and $(A^{i-1-j} M (A^T)^j)^T = -A^j M (A^T)^{i-1-j}$. If $2j \ne i-1$, each entry in the diagonal of $A^{i-1-j} M (A^T)^j) + A^j M (A^T)^{i-1-j} = -(A^j M (A^T)^{i-1-j})^T + A^j M (A^T)^{i-1-j}$ is of course zero. For $2j = i-1$, let $A^j = P = (p_{ij})_{1 \le i,j \le n}$. Then the $(k,k)$-entry of $A^{i-1-j} M (A^T)^j) = PMP^T$ is

$$\sum_{1 \le i,j \le n} p_{ki} m_{ij} p_{kj} = (\sum_{i<j} + \sum_{j<i}) p_{ki} m_{ij} p_{kj} = \sum_{i<j} p_{ki} (m_{ij} + m_{ji}) p_{kj} = 0.$$

Thus, each diagonal entry of $\sum_{j=0}^{i-1} A^{i-1-j} M (A^T)^j$ is zero.

(iii) The statement is equivalent to say that $f(x)\mathbf{S}_{A,A^T;M} = \mathbf{0}$. We prove this in the following three steps.

(iii.a) The claim is true for any Jordan matrix $A$. By (3),

$$f(x)\mathbf{S}_{A,A^T;M} = (U, AU, A^2U, A^3U, \cdots)$$

for some matrix $U$. By (ii), $U$ and $AU$ are alternate matrices. By (i), $U = 0$.

(iii.b) The claim is true for any block diagonal matrix with Jordan matrices as its block submatrices. Let $r \geq 2$, $A_1, \cdots, A_r$ be Jordan matrices, and $A = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_r \end{pmatrix}$. Let $\begin{pmatrix} A & M \\ 0 & A^T \end{pmatrix}^i = \begin{pmatrix} A^i & M_i \\ 0 & (A^i)^T \end{pmatrix}$. Block $M$ as $(M_{kl})_{1\leq k,l\leq r}$ and block $M_i$ as $(M_{kl}^{(i)})_{1\leq k,l\leq r}$ according to the block way of $A$. Then $M_{kl}^{(i)}$ is exactly the $i$-th entry of the matrix sequence $\mathbf{S}_{A_k,A_l^T;M_{kl}}$. Suppose $f_k(x)$ be the characteristic polynomial of $A_k$ and $f(x) = f_1(x)\cdots f_r(x)$ be the characteristic polynomial of $A$. Since $f_k(x)f_l(x)\mathbf{S}_{A_k,A_l^T;M_{kl}} = \mathbf{0}$, for $k \neq l$, we have $f(x)\mathbf{S}_{A_k,A_l^T;M_{kl}} = \mathbf{0}$. For $k = l$, by (iii.a), $f_k(x)\mathbf{S}_{A_k,A_k^T;M_{kk}} = \mathbf{0}$, and hence, $f(x)\mathbf{S}_{A_k,A_k^T;M_{kk}} = \mathbf{0}$. Thus, for any $k$ and $l$, we always have $f(x)\mathbf{S}_{A_k,A_l^T;M_{kl}} = \mathbf{0}$. Therefore, $f(x)\mathbf{S}_{A,A^T;M} = \mathbf{0}$.

(iii.c) The claim is true for any matrix $A$. By linear algebra, there exists an invertible matrix $V$ (maybe over an extension of the ground field) such that $VAV^{-1}$ is a block diagonal matrix with Jordan matrices as its block submatrices. Since

$$\begin{pmatrix} A & M \\ 0 & A^T \end{pmatrix} = \begin{pmatrix} V^{-1} & 0 \\ 0 & V^T \end{pmatrix} \begin{pmatrix} VAV^{-1} & VMV^T \\ 0 & (V^T)^{-1}A^TV^T \end{pmatrix} \begin{pmatrix} V^{-1} & 0 \\ 0 & V^T \end{pmatrix}^{-1}$$

and $VMV^T$ is skew-symmetric and with zero diagonal by the same proof as for (ii), let $Q' = \begin{pmatrix} VAV^{-1} & VMV^T \\ 0 & (V^T)^{-1}A^TV^T \end{pmatrix}$ and $P = \begin{pmatrix} V^{-1} & 0 \\ 0 & V^T \end{pmatrix}$, then by (iii.b), $f(Q') = 0$. Hence, $f(Q) = Pf(Q')P^{-1} = 0$. □

**Theorem 2.** *Let $A, B, C, D$ be four $m \times m$ matrices, $B$ and $D$ be invertible, and $A$ and $C$ be alternate matrices. Let $g(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ be the characteristic polynomial of $BD^T$ and $Q = \begin{pmatrix} BD^T & AD + BC \\ 0 & B^TD \end{pmatrix}$. Then $g(Q) = Q^m + a_{m-1}Q^{m-1} + \cdots + a_1Q + a_0I = 0$.*

*Proof.* By the linearity of $\mathbf{S}_{A,B;M}$ on $M$, we only need to show the statement for the case $C = 0$ and the case $A = 0$. Note that

$$\begin{pmatrix} BD^T & AD \\ 0 & B^TD \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & D^{-1} \end{pmatrix} \begin{pmatrix} BD^T & A \\ 0 & DB^T \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & D \end{pmatrix}$$

and

$$\begin{pmatrix} BD^T & BC \\ 0 & B^TD \end{pmatrix} = \begin{pmatrix} B & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} D^TB & C \\ 0 & B^TD \end{pmatrix} \begin{pmatrix} B^{-1} & 0 \\ 0 & I \end{pmatrix},$$

By Lemma 3(iii), the matrices $\begin{pmatrix} BD^T & A \\ 0 & B^T D \end{pmatrix}$ and $\begin{pmatrix} BD^T & C \\ 0 & B^T D \end{pmatrix}$ satisfy $g(x)$. Then the theorem follows by the linearity mentioned above. □

## 6 Conclusion

In this paper, we give a method to improve the extended Kipnis-Shamir attack on the unbalanced Oil-Vinegar Scheme when the difference of the numbers of the Vinegar variables and the Oil variables is small. Moreover, by modifying the associated symmetric matrices of quadratic polynomials in the public key, we propose a method to remedy the extended Kipnis-Shamir attack for the unbalanced Oil-Vinegar scheme in the case that the field characteristic is 2 and the difference of the numbers of the Vinegar and Oil variables is odd. In addition, we give a theoretical proof for the experimental observation which results in that Kipnis-Shamir attack needs to be modified as in [4].

**Acknowledgement.** The authors would like to thank Prof. Dingfeng Ye for pointing out us a clue for the theoretical proof in Section 5. The work of the first two authors were supported by the Natural Science Foundation of China (NSFC) under grants 61070172 and 10990011, the National 863 Program of China (2006AA01Z416) and the National Basic Research Program of China (2007CB311201). The work of the third author would like to thank partial support of NSF and NSFC grant 60973131.

## References

1. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil & vinegar signature schemes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 206–222. Springer, Heidelberg (1999)
2. Buchmann, J., Dahmen, E., Szydlo, M.: Hash-based digital signature schemes, 1st edn. Springer, Berlin (2009)
3. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Transactions on Information Theory 22, 644–654 (1976)
4. Ding, J., Gower, J., Schmidt, D.: Multivariate public keycryptosystems. In: The 9th International Workshop on Theory and Practice in Public Key Cryptography, PKC 2006, pp. 80–84. Springer, Heidelberg (2006)
5. Ding, J., Hu, L., Nie, X., Li, J., Wagner, J.: High order linearization equation (HOLE) attack on multivariate public key cryptosystems. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 233–248. Springer, Heidelberg (2007)
6. Dubois, V., Fouque, P.-A., Shamir, A., Stern, J.: Practical cryptanalysis of SFLASH. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 1–12. Springer, Heidelberg (2007)
7. Goldreich, O., Goldwasser, S., Halevi, S.: Public-key cryptosystems from lattice reduction problems. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 112–131. Springer, Heidelberg (1997)
8. Kipnis, A., Shamir, A.: Cryptanalysis of the oil & vinegar signature scheme. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 257–267. Springer, Heidelberg (1998)

9. McEliece, R.: A public-key cryptosystem based on algebraic coding theory. Deep Space Network Progress Report 42-44, Jet Propulsion Laboratory, California Institute of Technology, pp. 104–113 (1978)
10. Patarin, J.: The oil and vinegar signature scheme. Presented at the Dagstuhl Workshop on Cryptography (1997)
11. Patarin, J., Courtois, N.T., Goubin, L.: FLASH, a fast multivariate signature algorithm. In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 298–307. Springer, Heidelberg (2001)
12. Shor, P.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing 26(5), 1484–1509 (1997)