

# Cryptanalysis of the Oil & Vinegar Signature Scheme

Aviad Kipnis<sup>1</sup> and Adi Shamir<sup>2</sup>

<sup>1</sup> NDS Technologies, Israel

<sup>2</sup> Dept. of Applied Math, Weizmann Institute, Israel

**Abstract.** Several multivariate algebraic signature schemes had been proposed in recent years, but most of them had been broken by exploiting the fact that their secret trapdoors are low rank algebraic structures. One of the few remaining variants is Patarin's "Oil & Vinegar" scheme, which is based on a system of  $n$  quadratic forms in  $2n$  variables of two flavors ( $n$  "oil" variables and  $n$  "vinegar" variables). The security of the scheme depends on the difficulty of distinguishing between the two types, and does not seem to be susceptible to known low rank attacks. In this paper we describe two novel algebraic attacks which can efficiently separate the oil and vinegar variables, and thus forge arbitrary signatures.

## 1 Introduction

The problem of developing secure digital signature schemes had been extensively investigated over the last 20 years. The longest surviving and best known of these schemes is the RSA signature scheme, in which the verification condition for a message  $m$ , signature  $x$ , and public key  $(e, n)$  is the single algebraic equation  $x^e = m \pmod{n}$  of degree  $e$  in the single variable  $x$ . Its security is based on the difficulty of solving such an equation modulo a large  $n$  with unknown factorization.

A natural extension of this algebraic approach is to consider several simultaneous equations in several variables. Let  $M = (m_1, \dots, m_k)$  and  $X = (x_1, \dots, x_t)$  be vectors representing the message and signature, respectively. The signature is said to be valid if:

$$\begin{aligned}G_1(x_1, \dots, x_t) &= m_1 \\G_2(x_1, \dots, x_t) &= m_2 \\&\vdots \\G_k(x_1, \dots, x_t) &= m_k\end{aligned}$$

where the  $G_i$  are multivariate polynomials published by the signer as his public's key.

The designer of the signature scheme can now take one of two routes:

1. He can use a small (=constant) number of variables over a large algebraic domain such as  $\mathcal{F}_n$ , and base its security on the difficulty of factoring  $n$ . Compared to the RSA scheme, he hopes to get the same security but higher performance.

2. He can use a large (=security parameter) number of variables over a small algebraic domain. The problem of solving systems of polynomial equations is NP-complete even when all the equations are of degree 2 and the algebraic domain is the two-element field  $\mathcal{F}_2$ . Compared to the RSA scheme, he hopes to get higher security *and* higher performance.

Unfortunately, almost all these schemes were broken shortly after their introduction. For example, the Ong-Schnorr-Shamir [OSS] scheme (which belongs to the first type) was broken by Pollard and Schnorr [PS], the Matsumoto and Imai scheme [MI] (which belongs to the second type) was broken by Patarin [P1], and Shamir's birational permutation scheme [S] (which belongs to the second type) was broken by Coppersmith Stern and Vaudenay [CSV].

About two years ago, Patarin tried to revive the second approach by introducing several new signature schemes which seemed to be immune to all the known types of algebraic attacks. The "oil & vinegar" signature scheme [P2] was described as the simplest, while the "hidden field equations" [P3] was described as the most secure, and a \$1000 prize was offered for its cryptanalysis. The only partial attack found so far against any of these schemes (based on private communication with Patarin, January 1998) is due to Coppersmith, who broke a cubic variant of the oil & vinegar scheme, but not the original quadratic version.

In this paper we describe two novel algebraic attacks which can break the original "Oil & Vinegar" scheme in a matter of seconds for all reasonable choices of the security parameter. The first attack linearizes certain quadratic equations which distinguish between the oil and vinegar variables, while the second attack analyses the characteristic polynomials of certain matrices to find two eigenspaces generated by the two types of variables. The attacks extract from the public key an algebraic structure which is equivalent to (but not necessarily equal to) the legitimate signer's secret key, and after this short precomputation the forger can use the signer's efficient algorithm to generate signatures for arbitrary messages.

## 2 A Simplified Oil & Vinegar Scheme

In this section we introduce a homogeneous variant of the Oil & Vinegar scheme, which makes the description and analysis of our attacks simpler. In section 4 we show that essentially the same attack can be applied to the original non-homogeneous Oil & Vinegar scheme.

Let  $M = (m_1, \dots, m_k)$  be a message consisting of  $k$  elements from a finite field  $\mathcal{F}$  of order  $q$ .  $X = (x_1, \dots, x_{2k})$  consisting of  $2k$  elements from  $\mathcal{F}$  is a valid signature of  $M$  if it satisfies  $G(X) = M$  where  $G(X) : \mathcal{F}^{2k} \rightarrow \mathcal{F}^k$  is the signer's public key. The mapping  $G$  can be written as  $G(X) = (G_1(X), G_2(X), \dots, G_k(X))$  where each  $G_e(X)$  is a homogeneous quadratic form of  $2k$  variables  $X = (x_1, \dots, x_{2k})$  over  $\mathcal{F}$ , i.e., a sum of monomials of the form  $c_{ij}x_i x_j$ . Such a quadratic form can be described by the product  $X^t G_e X$  in which  $G_e$  is a  $2k \times 2k$  matrix,  $X$  is a column vector, and  $X^t$  is  $X$  transposed.

Each message  $M$  has approximately  $q^k$  possible signatures, but finding any one of them is apparently difficult due to the nonlinearity of the equations. The legitimate signer can solve these equations and compute  $X$  by exploiting the secret structure of  $G$ , defined by the following construction:

Let  $A$  be a randomly chosen nonsingular  $2k \times 2k$  matrix over  $\mathcal{F}$ , and let  $Y = (y_1, \dots, y_{2k})$  be a new set of  $2k$  variables defined by  $Y = AX$ . Let  $F = (F_1, \dots, F_k)$  be a vector of  $k$  random matrices of size  $2k \times 2k$  in which the top left  $k \times k$  submatrix is zero:

$$F_e = \begin{pmatrix} 0 & B_1 \\ B_2 & B_3 \end{pmatrix}$$

Define the quadratic forms  $F_e(Y)$  for  $e = 1, \dots, k$  in the usual way as  $Y^t F_e Y$ , and derive the equivalent quadratic forms  $G_e(X)$  after the linear change of variables  $Y = AX$  as the products  $X^t \cdot A^t \cdot F_e \cdot A \cdot X$ . Publish their coefficients (i.e., the entries of the triple products  $A^t \cdot F_e \cdot A$ ) as the public signature verification key.

The signer's secret key is the matrix  $A$  which translates between the public  $X$  and secret  $Y$  variables. In terms of the  $Y$  variables, the quadratic forms are  $Y^t \cdot F_e \cdot Y$ . The fact that  $F_e$  has a top left quarter of zeroes implies that in any monomial of the form  $c_{ij} y_i y_j$  at most one of  $i, j$  can be in the range  $[1, k]$ , and thus all the variables from the first half of  $Y$  (which we call the *oil* variables) occur linearly in the quadratic forms, while all the variables from the second half of  $Y$  (which we call the *vinegar* variables) can occur either linearly or quadratically in the quadratic forms. However, when translated into quadratic forms in terms of the  $X$  variables, the distinction disappears and all the  $2k$  variables in  $X$  seem to multiply each other in all possible combinations with random looking coefficients.

To sign a given message  $M = (m_1, \dots, m_k)$ , the legitimate signer uses the following simple algorithm:

1. Assign random values to all the vinegar variables  $(y_{k+1}, \dots, y_{2k})$ .
2. Simplify the quadratic equations defined by  $Y^t \cdot F_e \cdot Y = m_e$ . The resultant equations are linear and contain only oil variables.
3. Solve the system of  $k$  linear equations in  $k$  variables. If it is singular, return to step 1 (this can be shown to happen with a probability smaller than some constant which depends on the choice of  $F$ ).
4. Map the  $Y$  solution to an  $X$  solution via  $X = A^{-1}Y$ .
5. Provide  $X$  as a signature of  $M$ .

To forge a signature for message  $M$ , the forger has to find  $2k$  values for the variables in  $X$  satisfying the  $k$  random looking quadratic equations  $G_i(X) = m_i$ . In the next section we show that it is possible to break the scheme by recovering the oil variables.

### 3 Cryptanalysis of the Oil & Vinegar Signature Scheme

#### 3.1 The Cryptanalytic Approach

**Definition 1.** *The oil subspace of the  $Y$  space is the set of all vectors in  $\mathcal{F}^{2k}$  whose second half contain only zeroes. The oil subspace of the  $X$  space is the preimage by  $A$  of all vectors in  $\mathcal{F}^{2k}$  whose second half contain only zeroes.*

**Definition 2.** *The vinegar subspace of the  $Y$  space is the set of all vectors in  $\mathcal{F}^{2k}$  whose first half contain only zeroes. The vinegar subspace of the  $X$  space is the preimage by  $A$  of all vectors in  $\mathcal{F}^{2k}$  whose first half contain only zeroes.*

The notions of oil and vinegar subspaces will often be used without referring to the  $X$  or  $Y$  spaces, and the meaning will be clear from the context. Since  $A$  is nonsingular, each one of these subspaces has dimension  $k$ , and the  $X$  and  $Y$  spaces can be viewed as direct sums of their oil and vinegar subspaces.

An important property of the oil space is:

**Lemma 3.** *All the published quadratic forms  $G_1(X)..G_k(X)$  over  $\mathcal{F}^{2k}$  are identically zero on the oil subspace  $V$  of  $X$ .*

*Proof:* In each monomial in  $Y^t F_e Y$  there can be at most one oil variable. By our simplifying homogeneous assumption, the Oil & Vinegar scheme cannot contain linear monomials, and thus each monomial contains at least one vinegar variable. Since any  $X \in V$  corresponds to a  $Y$  in which all the vinegar variables are zero, the quadratic form is identically zero on  $V$ .  $\square$

The set of  $X$  vectors which make a particular  $G_e(X)$  zero is usually a strict superset of the oil subset, but the intersection of sufficiently many of these sets is likely to be exactly the oil subspace. However, this is not an effective characterization of the oil subspace, since we can't find the zero sets of quadratic forms with many variables by an efficient algorithm.

The next observation is that each matrix  $G_e$  can be considered not only as a quadratic form, but also as a linear mapping over the  $X$  space. One technical problem is that quadratic forms and linear mappings behave differently under the linear change of variables  $Y = AX$ : If  $B$  is the matrix of a quadratic form, it is changed by a congruence relation to  $A^t B A$ , while if  $B$  is the matrix of a linear mapping, it is changed by a similarity relation to  $A^{-1} B A$ .

To overcome this problem, we consider products of matrices of the form  $B^{-1} C$ . If  $B$  and  $C$  are quadratic forms and  $A$  is a linear change of variables, then the new  $B$  and  $C$  are  $A^t B A$  and  $A^t C A$ , respectively, and thus the new  $B^{-1} C$  is  $A^{-1} B^{-1} A^{t-1} A^t C A = A^{-1} B^{-1} C A$ , which is  $B^{-1} C$  changed by a similarity relation, as desired.

We first characterize the behaviours of the  $F_e$ 's as linear mappings over the  $Y$  space:

**Lemma 4.** *If  $F_i$  and  $F_j$  are nonsingular, then  $F_j$  maps the oil space onto the vinegar space,  $F_i^{-1}$  maps the vinegar space onto the oil space, and  $F_i^{-1} F_j$  maps the oil space onto itself.*

**Proof:**  $F_j$  has a top left quarter of zeroes. When it is multiplied by a column vector whose second half is zero, the result is a column vector whose first half is zero, and thus  $F_j$  maps the oil subspace into the vinegar subspace. If  $F_j$  is nonsingular, it maps a subspace of dimension  $k$  to a subspace of dimension  $k$ , and thus  $F_j$  maps the oil subspace onto the vinegar subspace. Since all the vinegar subspace is in the range of this mapping,  $F_i^{-1}$  maps the vinegar subspace back onto the oil subspace, and  $F_i^{-1}F_j$  maps the oil subspace onto itself.  $\square$

When we change  $Y$  to  $X$ ,  $F_e$  is changed to  $G_e$  as a quadratic form, but not as a linear mapping. However,  $F_{ij} = F_i^{-1}F_j$  is changed to  $G_{ij} = G_i^{-1}G_j$  as a linear mapping, and thus for any  $i, j$ ,  $G_{ij}$  maps the oil subspace of the  $X$  space onto itself.

**Remark:** There is a subtle point for fields  $\mathcal{F}$  of characteristic 2, since  $0+0 = 1+1 = 0$ , and thus the symmetric matrix representation of their quadratic forms does not always exist, and is not always unique. In particular, the party that chooses the signature key can change the top left quarter of  $F_e$  from zero to any symmetric matrix with zeroes on the diagonal, and then compute  $G_e$  in the usual way as  $A^t F_e A$ . As quadratic forms, all these matrices are equivalent, but as linear mappings they behave very differently, and in particular any attack based on a search for these zeroes in  $F_e$  will be foiled by such a modification. The simplest way to overcome this countermeasure was proposed by Coppersmith (private communication): replace each published  $G_e$  by  $G'_e = G_e + G_e^t$ . As a quadratic form over  $X$ ,  $X^t G'_e X$  is uninteresting since it is identically zero, but as a linear mapping it is equal to  $A^t (F_e + F_e^t) A$ , which has the desired form (a matrix  $F_e + F_e^t$  with a top left quarter of zeroes, under congruence relation). Since our attack only considers the behaviour of the given matrices as linear mappings, we can apply it even when the field has characteristic 2 and the  $F_e$  matrices are intentionally modified.

**Definition 5.** Assume that all the  $G_e$  matrices are nonsingular (eliminate those which are not). Define  $T$  as the closure of all the matrices  $G_{ij} = G_i^{-1}G_j$  under addition, multiplication, and multiplication by a constant from  $\mathcal{F}$ .

Note that if the  $F_e$  and  $A$  are chosen at random, at least a constant fraction of the  $G_e$  matrices are nonsingular, and thus there are quadratically many  $G_{ij}$  matrices. Their closure  $T$  is even richer, and contains all the polynomials in all the nonsingular  $G_{ij}$  (note that these matrices need not commute, and thus the monomials in these polynomials contain all the different orders in which they can be multiplied, and not just their multiplicity).

**Definition 6.** A linear subspace  $U$  is an eigenspace of matrix  $B$  if  $B$  maps  $U$  into itself.  $U$  is a common eigenspace of a set of matrices if it is an eigenspace of each one of them.

**Remark:** If  $B$  is nonsingular then it maps the eigenspace onto itself. Any eigenvector of  $B$  defines an eigenspace of dimension one. If  $B$  has several eigenvectors then the space spanned by any subset of eigenvectors is also an eigenspace. If  $B$  has a complete set of eigenvectors corresponding to distinct eigenvalues,

then all the eigenspaces of  $B$  are of this form. However,  $B$  can have nontrivial eigenspaces even when it has no eigenvectors at all, and thus the concept of eigenspaces is a strict generalization of the concept of eigenvectors. Random matrices often have only the trivial eigenspaces of the zero vector and the whole space, and several random matrices are very unlikely to have a common non-trivial eigenspace.

We can thus provide a strong characterization of the oil subspace:

**Theorem 7.** *The oil subspace  $V$  of the  $X$  space is a common eigenspace of all the matrices in  $T$ .*

**Proof:** We have already shown that  $V$  is a common eigenspace of all the  $G_{ij}$  matrices. Since this property is preserved by the operations of addition, multiplication, and multiplication by a constant,  $V$  is a common eigenspace of their closure  $T$ .  $\square$

## 4 Finding Common Eigenspaces

In this section we describe two efficient methods for finding a common eigenspace of a sufficiently rich set of matrices. The first method is a linearization heuristic which is expected to succeed with high probability. The second method is based on a simple relationship between eigenspaces and characteristic polynomials of matrices, and can be rigorously analysed.

### 4.1 The Linearization Method

In this method we first derive a large number of quadratic equations in a small number of variables. We linearize it by replacing the product of any two variables by a new variable, getting linear equations in a quadratic number of variables. If the original number of quadratic equations is quadratic in the number of variables, we hope to get a uniquely solvable system of linear equations. The values of the original variables can now be derived by analysing the values of their pairwise products.

To find the quadratic equations, choose a basis  $T_1, \dots, T_n$  for the closure  $T$  of the  $G_{ij}$  matrices. We cannot formally prove a lower bound on  $n$ , but there are strong heuristic arguments why  $n$  is expected to be  $\theta(k^2)$ . Let  $R = (r_1, \dots, r_{2k})$  be a vector of formal variables denoting some vector in the oil subspace of  $X$ . Consider the collection of column vectors  $T_1R, \dots, T_nR$  in which each entry is a formal linear combination of  $r_i$  variables with known coefficients, and arrange them in a  $2k \times n$  matrix  $M$ . Since the oil space is a common subspace of rank  $k$  of all the  $T_j$  matrices, the column rank of  $M$  cannot exceed  $k$  for any choice of  $R$  in the oil subspace  $V$ . Consequently, the row rank of  $M$  cannot exceed  $k$  as well, and thus there is a linear relationship between the first  $k + 1$  rows of  $M$ . Let  $S = (s_1, \dots, s_{k+1})$  be the coefficients of this linear relationship (without loss of generality, we can assume that  $s_{k+1}$  is 1). For each one of the  $n$  columns of  $M$ ,

we can thus express the relationship as a quadratic equation in the variables of  $R$  and  $S$ .

We can now solve this system of equations by the linearization method, replacing each product of variables  $r_i s_j$  by a new variable  $z_{ij}$ . Unfortunately, the  $r_i$  and  $s_j$  solution is not unique (any vector in the oil space can give rise to a different linear combination of the rows), and thus there is a non-trivial subspace of solutions for the linearized variables  $z_{ij}$ . A randomly chosen solution in this subspace is unlikely to correspond to a consistent product of  $r_i$  variables and  $s_j$  variables. To overcome this problem, we add random (nonhomogeneous) linear equations relating the  $2k$  variables  $r_i$ , and use them to eliminate some of the  $r_i$  variables from the quadratic equations before we linearize them. When sufficiently many random linear equations are added, we expect that the vector  $R$  in the oil subspace will become uniquely defined (as the intersection of a linear subspace and an affine subspace of half dimension), and thus we will not get parasitic  $z_{ij}$  solutions which do not correspond to products of  $r_i$  and  $s_j$  variables. We may have to try several collections of random equations of different sizes, but the method is expected to succeed since our characterization of the oil subspace leads to an extremely overdefined system of equations.

## 4.2 The Characteristic Polynomial Method

In this section we exploit interesting relations between eigenspaces and characteristic polynomials.

Let  $P(x)$  be the characteristic polynomial of an  $n \times n$  matrix  $B$ . By the Caley-Hamilton theorem,  $P(B)$  is the zero matrix. We now consider the matrices obtained by substituting  $B$  into other polynomials.

**Lemma 8.** *For any polynomial  $P'(x)$ ,  $\text{kernel}(P'(B))$  is an eigenspace of  $B$ .*

*Proof:* If  $Z \in \text{kernel}(P'(B))$  then  $P'(B)Z = 0$  by definition.  $B$  commutes with any power of  $B$ , and thus with any polynomial in  $B$  such as  $P'(B)$ . Consequently,  $P'(B) \cdot BZ = B \cdot P'(B)Z = 0$ . This proves that  $B$  maps the kernel of  $P'(B)$  into itself.  $\square$

The converse of this lemma is not true, in the sense that some eigenspaces of  $B$  are not definable as the kernel of any polynomial in  $B$ . Consider, for example, the identity matrix  $B = I$ . Since all the powers of  $B$  are  $I$ , the only singular polynomial in  $B$  is the zero matrix, whose kernel is the whole space. On the other hand, any linear subspace is an eigenspace of  $B$ .

For any matrix  $B$  and vector  $Z$  there exists a minimal nonzero polynomial  $P'(x)$  such that  $(P'(B))$  maps  $Z$  to zero ( $P'$  is defined by the smallest linear relationship between the vectors  $B^i Z$ ). If this  $P'(x)$  does not divide the characteristic polynomial  $P(x)$  of  $B$ , there are two polynomials  $D(x)$  and  $E(x)$  such that  $D(x)P'(x) + E(x)P(x) = P''(x)$  where  $P''(x) = \text{gcd}(P'(x), P(x))$  whose degree is strictly smaller than that of  $P'(x)$ . When  $B$  is substituted for  $x$  and the resultant matrix is applied to  $Z$ , we get a lower degree polynomial which maps  $Z$  to zero, in contradiction to the minimality of  $P'(x)$ .

The definition can be extended from a single vector  $Z$  to any linear subspace  $V$ , and the minimal polynomial of  $V$  (with respect to  $B$ ) is the least common multiple of the minimal polynomials of all the vectors  $Z \in V$ , which is also a divisor of the characteristic polynomial  $P(x)$  of  $B$ .

The following case is of special interest:

**Theorem 9.** *If the characteristic polynomial  $P(x)$  of  $B$  is irreducible, then the only eigenspaces of  $B$  are  $\{0\}$  and the whole space.*

*Proof:* Let  $Z$  be any nonzero vector in the eigenspace  $V$ . The minimal polynomial of  $Z$  is a divisor of  $P(x)$ . Since  $P(x)$  is irreducible, it can only be  $P(x)$  itself. Since the minimal polynomial of  $Z$  is of full degree  $n$ , the vectors  $Z, BZ, B^2Z, \dots, B^{n-1}Z$  are  $n$  linearly independent vectors. However,  $Z \in V$  and  $V$  is an eigenspace of  $B$ , and thus all these vectors are also in  $V$ . Consequently,  $V$  has full dimension  $n$ , and contains the whole space.  $\square$

We cannot use this simple characterization of eigenspaces to search for the nil subspace of matrices in  $T$ , since the characteristic polynomials of these matrices are always reducible polynomials. To see this, consider any two matrices  $F_i$  and  $F_j$  of size  $2k \times 2k$  whose top left quarter is zero. It is easy to show that the product  $F_{ij} = F_i^{-1}F_j$  has the form:

$$F_{ij} = \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix}$$

and the sum, product, and constant multiples of such matrices have the same form. The characteristic polynomial of any matrix of this form is the product of the characteristic polynomials of  $B_1$  and  $B_3$ , which are of degrees  $k$  each. The characteristic polynomial is not changed by a similarity transformation, and thus the characteristic polynomials of all the matrices in  $T$  can be expressed as the products of two  $k$  degree polynomials.

We are thus led to consider the next simplest case, in which the characteristic polynomial  $P(x)$  of  $B$  factors into two distinct irreducible factors  $P(x) = P_1(X) \cdot P_2(X)$ . Define  $B_1 = P_1(B)$ ,  $B_2 = P_2(B)$ ,  $K_1 = \text{kernel}(B_1)$ , and  $K_2 = \text{kernel}(B_2)$ . Then the following is true:

1.  $\text{range}(B_1) \subseteq K_2$  and  $\text{range}(B_2) \subseteq K_1$ .
2.  $K_1 \cap K_2 = \{0\}$  (the zero vector).
3.  $\dim(K_1) + \dim(K_2) = 2k$ .
4. The space can be represented as a direct sum of  $K_1$  and  $K_2$ .
5. The only eigenspaces of  $B$  are  $\{0\}$ ,  $K_1$ ,  $K_2$ , and the whole space.

The intuitive reason for the last part is that any vector  $Z$  in an eigenspace  $V$  can be decomposed into its  $K_1$  and  $K_2$  components, which behave independently of each other. If only one of the components is nonzero, repeated application of  $B$  to  $Z$  spans the corresponding  $K_i$  by the irreducibility of  $P_i$ . If both components are nonzero, the minimal polynomial of  $Z$  is the least common multiple of the two minimal polynomials, which is the whole  $P(x)$  since  $P_1(x)$  and  $P_2(x)$  are distinct and thus relatively prime. These statements will be formally proved in the full version of the paper.

*Remark:* It is possible to extend the complete characterization of the eigenspaces to arbitrary matrices by analysing their Jordan normal forms, but the results are more complicated and the characterization becomes useless when there are too many possible eigenspaces.

We know that the oil subspace is a common eigenspace of dimension  $k$  of all the matrices in  $T$ . The characteristic polynomial of any such matrix factors into two polynomials of degree  $k$ , but each one of these polynomials can often be factored further into smaller degree polynomials. In particular, if the characteristic polynomial factors completely into  $2k$  linear terms, there are exponentially many ways to multiply  $k$  of them to get the  $k$  degree polynomial defining the oil space. However, if  $T$  contains some matrix  $B$  whose characteristic polynomial  $P(x)$  can be factored into two distinct irreducible factors  $P_1(x)$  and  $P_2(x)$  of degree  $k$ , then the oil subspace we want to find is easy to compute either as the kernel of  $P_1(B)$  or as the kernel of  $P_2(B)$ .

The characteristic polynomial and the kernel of a given matrix can be found in polynomial time, and its complete factorization over a finite field can be found in random polynomial time. To find a usable  $B$ , we randomly sample matrices in  $T$ . What is left to be shown is that with a sufficiently high probability, the characteristic polynomials of these matrices factor into a pair of distinct irreducible factors. An easy counting argument shows that random  $k$  degree polynomials are irreducible with probability about  $1/k$ , and thus a quadratic number of random polynomials almost certainly contains polynomials of the desired form. However, the characteristic polynomials of random matrices may be non-uniformly distributed. We overcome this difficulty by proving:

**Theorem 10.** *There is a set  $B$  of matrices such that:*

1.  *$B$  contains at least a constant fraction of all the matrices*
2. *The characteristic polynomials of matrices in  $B$  are uniformly distributed.*

The proof will be given in the full version of the paper, and then applied to our case in which the characteristic polynomials of all the matrices in  $T$  are known to factor into two polynomials of degree  $k$ , but are somewhat unlikely to factor further into lower degree factors.

We can thus conclude that for a randomly chosen public key in the oil & vinegar signature scheme, we can find its oil subspace with high probability by a random polynomial time algorithm.

## 5 Completing the Attack

Let  $V$  be the common oil eigenspace of all the  $T$  matrices, found by one of the two methods described in the previous section. We define a new basis  $(y_1, \dots, y_{2k})$  in which the vectors  $y_1, \dots, y_k$  span the oil subspace and  $y_{k+1}, \dots, y_{2k}$  complete it into a basis for the  $2k$  dimensional space. This basis is not unique, but it is related to the original basis used by the legitimate signer via some linear transformation which maps the oil subspace onto itself. For any such basis, all the given quadratic forms  $G_e$  become linear in the first half of their variables,

because this is true when the original basis is used, and remains true under any linear transformation which preserves the oil subspace. Consequently, the forger can use the same efficient algorithm used by the signer to generate forged signatures for arbitrary messages, even though he cannot reconstruct an identical secret key.

To complete our attack on the original oil & vinegar signature scheme, we have to consider the differences between the original the simplified versions. The only significant difference is that in Patarin's original scheme, the quadratic forms  $F_e$  can contain linear and constant terms, and the mapping  $A$  is affine rather than linear. The resultant  $G_e$  forms are not necessarily homogeneous, and we have to modify our definitions of the oil and vinegar domains since they become affine rather than linear subspaces. However, all the modifications affect only the linear and constant terms in each  $G_e$ , which are clearly distinguishable from the quadratic terms in the published forms. We can thus apply the attack described so far to the homogeneous quadratic parts of the published forms, find the homogeneous linear part of the mapping  $A$ , and add the linear and constant parts of the  $G_e$  only when we actually solve the resultant system of linear equations in the oil variables. More details on this point will be provided in the full version of this paper.

## Acknowledgements

We would like to thank Don Coppersmith, Victor Halperin, Anthony Joseph, Jacques Patarin, Ran Raz and Jacques Stern for many fruitful discussions and improvement ideas.

## References

- CSV. D. Coppersmith, J. Stern and S. Vaudenay, *The Security of the Birational Permutation Signature Scheme*, Journal of Cryptology, 1997, pp. 207-221. [258](#)
- MI. T. Matsumoto and H. Imai, *Public Quadratic Polynomial Tuples for Efficient Signature Verification and Message Encryption*, Eurocrypt 88, Springer Verlag, pp.419-453. [258](#)
- OSS. H. Ong, C. P. Schnorr, and A. Shamir *A Fast Signature Scheme Based on Quadratic Equations*, Proc. 16-th ACM Symp. Theory of Computation, 1984, pp. 208-216. [258](#)
- P1. J.Patarin, *Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt 88*, Crypto 95, Springer Verlag, pp.248-261. [258](#)
- P2. J. Patarin, *The Oil and Vinegar Algorithm for Signatures*, presented at the Dagstuhl Workshop on Cryptography, September 97. [258](#)
- P3. J.Patarin, *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms*, Eurocrypt 96, Springer Verlag, pp.33-48.

- PS. J. M. Pollard and C. P. Schnorr, *An Efficient Solution of the Congruence  $x^2 + ky^2 = m \pmod{n}$* , IEEE Trans. Information Theory, vol. IT-33, no. 5, 1987, pp. 702-709. 258 258
- S. A. Shamir *Efficient Signature Schemes Based on Birational Permutations*, Crypto 93, Springer Verlag, pp.1-12. 258