Block-Anti-Circulant Unbalanced Oil and Vinegar

Alan Szepieniec and Bart Preneel

imec-COSIC KU Leuven, Belgium
first-name.last-name@esat.kuleuven.be

Abstract. We introduce a new technique for compressing the public keys of the UOV signature scheme that makes use of block-anti-circulant matrices. These matrices admit a compact representation as for every block, the remaining elements can be inferred from the first row. This space saving translates to the public key, which as a result of this technique can be shrunk by a small integer factor. We propose parameters sets that take into account several important attacks.

Keywords: multivariate quadratic, post-quantum, unbalanced oil and vinegar

1 Introduction

Unbalanced Oil and Vinegar (UOV) is one of the longest-standing multivariate quadratic (MQ) signature schemes [9]. While the signatures are rather small, the public keys tend to be huge — they scale with the *cube* of the security parameter. Two notable improvements address this drawback in part.

First, the compression technique due to Petzoldt *et al.* allows most of the public key to be set arbitrarily; the remaining part is then computed with the secret key [13]. Since the arbitrary first part can be the output of a pseudorandom generator, the public key can be compressed to a short seed and the uncompressible second part.

Second, the field lifting technique due to Beullens and Preneel defines the public key over $\mathbb{F}_2$ but solves the signature equation and produces a signature over an extension thereof [1]. As a result, the direct attack is more complex as it must be performed over a larger field; this allows a smaller number of equations for the same security level. At the same time, however, the public key admits a representation of just one bit for every polynomial coefficient as it was constructed that way.

We propose a third compression technique, relying on structured matrices to compactly represent objects of large size. In particular, the remaining rows of an anti-circulant matrix can be inferred from the first. Moreover, these matrices guarantee that $B^\mathsf{T}AB$ is anti-circulant if A and B are; this property lends naturally to constructions of MQ public keys, where the matrix representation of the ith component's quadratic form can be presented as $S^\mathsf{T}F_iS$. As a result, the public key consists of block-anti-circulant matrices if the matrices of the secret key are block-anti-circulant. It can therefore be represented compactly by the list of first rows of each component block.

The obvious question raised by this design concerns its impact on security. We analyze empirically the complexity of a direct algebraic attack. With respect to the UOV Reconciliation Attack [4], our analysis assumes pessimistically that a successful attack need only consider each block to be its own variable. Building on the insights gleaned from this empiricism and pessimistic analysis, we propose parameters for various security levels. Despite the conservative parameter choices, our compression technique achieves a notable size reduction of the public key.

2 Preliminaries

We use pythonic notation to slice submatrices from matrices: $A_{[i:j,k:l]}$ represents the $(j-i) \times (l-k)$ block of A whose upper left element has index (i,j), with indices starting as they should at zero. Furthermore we denote by $0_{[0:v,0:v]}$ the $v \times v$ zero matrix.

A square matrix A is *anti-cirulant*, and a square matrix B is *circulant*, if they are fully determined by their first rows $(a_0, a_1, \ldots, a_{\ell-1})$ and $(b_0, b_1, \ldots, b_{\ell-1})$ via

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{\ell-2} & a_{\ell-1} \\ a_1 & a_2 & \cdots & a_{\ell-1} & a_0 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{\ell-2} & a_{\ell-1} & \cdots & a_{\ell-4} & a_{\ell-3} \\ a_{\ell-1} & a_0 & \cdots & a_{\ell-3} & a_{\ell-2} \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} b_0 & b_1 & \cdots & b_{\ell-2} & b_{\ell-1} \\ b_{\ell-1} & b_0 & \cdots & b_{\ell-3} & b_{\ell-2} \\ \vdots & \vdots & & \vdots & \vdots \\ b_2 & b_3 & \cdots & b_0 & b_1 \\ b_1 & b_2 & \cdots & b_{\ell-1} & b_0 \end{pmatrix} . \quad (1)$$

Circulant matrices are multiplication matrices of elements of the quotient ring $R[x]/\langle x^\ell - 1\rangle$, where R is the base ring of the matrix. Denote by J the 90° degree rotation of the identity matrix, *i.e.*, with the ones on the perpendicular diagonal. Then left or right multiplication by J makes a circulant matrix anti-circulant and vice versa. We make use of the following lemmata.

Lemma 1. *Let A, B be anti-circulant matrices. Then AB is circulant.*

Proof. There must be elements $a, b \in R[x]/\langle x^\ell - 1\rangle$ with multiplication matrices M_a and M_b such that $M_a J = A$ and $JM_b = B$. Then $AB = M_a JJM_b = M_a M_b = M_{ab}$ is the multiplication matrix of the element $ab \in R[x]/\langle x^\ell - 1\rangle$ and thus circulant. □

Lemma 2. *Let A be circulant and B anti-circulant. Then AB and BA are anti-circulant.*

Proof. There must be elements $a, b, b' \in R[x]/\langle x^\ell - 1\rangle$ with multiplication matrices M_a, M_b and $M_{b'}$ such that $A = M_a$ and $B = M_b J = JM_{b'}$. Then $AB = M_a M_b J = M_{ab} J$ and $BA = JM_{b'} M_a = JM_{b'a}$ are anti-circulant. □

Lemma 3. *The sum of circulant matrices is circulant. The sum of anti-circulant matrices is anti-circulant.*

Proof. The sum of circulant matrices $\sum_i B_i$ corresponds to the sum of elements $b_i \in R[x]/\langle x^\ell - 1\rangle$ and thus results in the multiplication matrix $M_{\sum_i b_i} = \sum_i M_{b_i}$, which is circulant as well. The sum of anti-circulant matrices $\sum_i A_i = \sum_i JM_{a_i} = J\sum_i M_{a_i} = JM_{\sum_i a_i}$. □

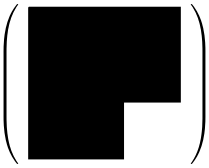
3 Multivariate Quadratic Signature Schemes

The public key in a hash-and-sign multivariate signature scheme is given by a list of m quadratic polynomials $\mathbf{P} \in (\mathbb{F}_q[x_0, \ldots, x_{n-1}]_{\leq 2})^m$ in n variables over a finite field $\mathbb{F}_q$. To verify a signature $\mathbf{s} \in \mathbb{F}_q^n$ on a document $d \in \{0,1\}^*$, the user evaluates $\mathbf{P}(\mathbf{s})$ and tests if it is equal to the hash $\mathsf{H}(d) \in \mathbb{F}_q^m$. To generate a signature, the signer uses the secret decomposition of the public key $\mathbf{P} = T \circ \mathbf{F} \circ S$ where T and S are affine and where $\mathbf{F}$ is also quadratic but easy to invert. With this decomposition, the signer can compute sequentially $\mathbf{h} = \mathsf{H}(d)$ and $\mathbf{y} = T^{-1}\mathbf{h}$, followed by sampling an inverse $\mathbf{x}$ under $\mathbf{F}$ (as there may be many), and finally $\mathbf{s} = S^{-1}\mathbf{x}$. The key challenge for the design of multivariate quadratic (MQ) schemes is how to find a quadratic map $\mathbf{F}$ that simultaneously admits efficient inverse sampling and is also hard to recover from $\mathbf{P} = T \circ \mathbf{F} \circ S$ for random and unknown affine transforms T, S.

3.1 Unbalanced Oil and Vinegar

The Unbalanced Oil and Vinegar (UOV) scheme answers this question by partitioning the variables of $\mathbf{F}$ into two sets: the *vinegar* variables $x_0, \ldots, x_{v-1}$ which are multiplied with each other and all other variables, and the *oil* variables $x_v, \ldots, x_{v+o-1}$ which do not mix with other oil variables. Phrased differently, every term that is quadratic in the oil variables has coefficient equal to zero. This gives rise to quadratic forms with the following matrix silhouette:

$$F^{(i)} =$$



$. \qquad (2)$

The black coefficients are chosen at random; the white coefficients are zero. The shape (2) anticipates the descriptor "unbalanced", as the number of vinegar variables is typically larger than the number of oil variables.

Since all the quadratic forms of $\mathbf{F}$ have the same silhouette, the transform T hides nothing and therefore it is set to the identity transform. For the present description we will drop linear and constant terms so that $\mathbf{F}$ can be described as $\mathbf{F}(\mathbf{x}) = (\mathbf{x}^\mathsf{T} F^{(i)} \mathbf{x})_{i=0}^{m-1}$ and $S \xleftarrow{\$} \mathsf{GL}_n(\mathbb{F}_q)$ with $n = o + v$ and $m = o$. Here and elsewhere we use the shorthand $\mathbf{x}^\mathsf{T} = (x_0, \ldots, x_{n-1})$.

To sign a document $d \in \{0,1\}^*$, the signer computes the hash $\mathbf{h} = \mathsf{H}(d)$ and selects a random assignment to the vinegar variables $\mathbf{x}_{[0:v]} \xleftarrow{\$} \mathbb{F}_q^v$. This produces a system of m equations of the form

$$\mathbf{x}_{[0:v]}^{\mathsf{T}} \left(F^{(i)}_{[0:v,v:(v+o)]} + F^{(i)\mathsf{T}}_{[v:(v+o),0:v]} \right) \mathbf{x}_{[v:(v+o)]} = h_i - \mathbf{x}_{[0:v]}^{\mathsf{T}} F^{(i)}_{[0:v,0:v]} \mathbf{x}_{[0:v]} \ , \tag{3}$$

which is linear in the $o = m$ oil variables $\mathbf{x}_{[v:(v+o)]}$. Solving this system completes $\mathbf{x}$ and from this inverse the user computes the signature $\mathsf{s} = S^{-1}\mathbf{x}$ straightforwardly.

3.2 Petzoldt's Compression Technique

Petzoldt's compression technique [13] rests on the observation that the composition with S is a *linear* action on the quadratic forms $F^{(i)}$. In particular, let $\overrightarrow{F^{(i)}}$ denote the row-vector of all $n(n+1)/2$ coefficients in accordance with any standard monomial order; then $\overrightarrow{P^{(i)}} = \overrightarrow{F^{(i)}} A$ for some matrix $A \in \mathbb{F}_q^{\frac{n(n+1)}{2} \times \frac{n(n+1)}{2}}$ whose coefficients are given by

$$A_{[\mathsf{mo}(i,j),\mathsf{mo}(r,s)]} = \begin{cases} S_{[r,i]}S_{[s,j]} + S_{[r,j]}S_{[s,i]} & \text{if} \quad i \neq j \\ S_{[r,i]}S_{[s,i]} & \text{otherwise} \ , \end{cases} \tag{4}$$

where $\mathsf{mo} : \mathbb{N}^2 \rightarrow \mathbb{N}$ sends the pair (i,j) to the index of the monomial $x_i x_j$ in the given monomial order.

As the $o(o+1)/2$ oil coefficients are zero, the $\overrightarrow{F^{(i)}}$ must live in a subspace of $\mathbb{F}_q^{n(n+1)/2}$ of dimension $n(n+1)/2 - o(o+1)/2$. As a result, the $\overrightarrow{P^{(i)}}$ must lie in a subspace of the same dimension. In particular, this means that the first $v(v+1)/2 + ov$ coefficients of every $\overrightarrow{P^{(i)}}$ can be set arbitrarily, after which the remaining $o(o+1)/2$ coefficients are fixed as a function of S.

The public key, represented as a Macaulay matrix whose rows are $\overrightarrow{P^{(i)}}$, is thus divisible into two blocks, of dimensions $m \times (v(v+1)/2 + vo)$, and $m \times o(o+1)/2$, respectively. The first block can be generated by a peudorandom generator, after which point the user can find the second only if he knows S. The public key can therefore be reduced to a short seed and the second block. Note that this size is independent of the number of vinegar variables.

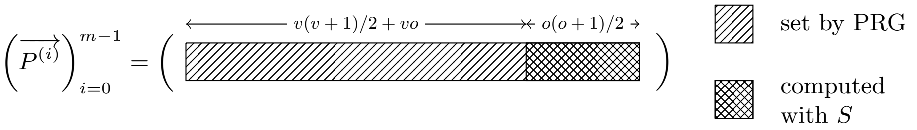


Fig. 1. Petzoldt's compression technique.

3.3 Field Lifting

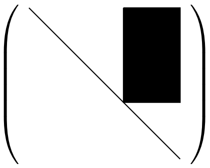
Field lifting is another method of compressing the public key, although in this case it comes at the cost of a larger signature [1]. The secret and public keys are defined over a small base field, typically $\mathbb{F}_2$. However, the hash function $\mathsf{H} : \{0,1\}^* \to \mathbb{F}_{2^r}^m$ maps to a vector of *extension field elements*, and the signature is generated —and verified— using arithmetic over the extension field.

This distinction allows the designer to ignore direct algebraic attacks performed over the base field. The number of equations needs only be large enough to guarantee the targeted level of security against a direct algebraic attack over the extension field. This number can be smaller as a result, which in turn leads to a much smaller public key. However, the base field must be taken into account for the UOV Reconciliation Attack [4], which solves an system of polynomial equations in order to recover the secret key from the public key. The complexity of this attack is accounted for by the increased number of vinegar variables. Since the field lifting technique is compatible with Petzoldt's technique, this increase does not affect the size of the public key. However, the signature size does grow as n is larger and as each component takes r bits to represent.

3.4 Irredundant *S*

It is always possible to find an equivalent secret key $(\mathbf{F}, S)$ for a given UOV public key, where S has the shape

$S =$



, (5)

where the white spaces are zero, the diagonal contains ones, and the nonzero block has dimensions $v \times o$. To see this, consider that only the rightmost o columns of S^{-1} —which has the same shape, just negate the rectangle— are capable of making the oil-oil coefficients of ${S^{-1}}^{\mathsf{T}} P^{(i)} S^{-1}$ equal to zero. Moreover, within the equivalence class of matrices S^{-1} with this property, it is always possible to choose one where the bottom right $o \times o$ block is the identity matrix.

The UOV Reconciliation Attack is a search for a matrix S of form (5) regardless of whether the public key was actually constructed with such an S. Therefore, one might as well choose S of this form from the onset. This has the benefit of accelerating key pair and signature generation [3].

4 Compression with Block-Anti-Circulant Matrices

Let $\ell \in \mathbb{N}$ denote the height (and width) of the blocks on block matrices; from now on we refer to this parameter as the *degree of circulancy.* A matrix is *block-anti-circulant* if every $\ell \times \ell$ block represents an anti-circulant matrix. Our compression technique arises from the following observation.

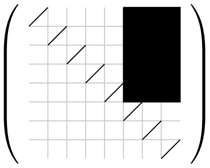
Theorem 1. *Let A, B, C be block-anti-circulant matrices with square blocks of height (and width) ℓ. Then ABC is block-anti-circulant for blocks of the same size.*

Proof. The $\ell \times \ell$ blocks of BC represent the sum of products of anti-circulant matrices. Via lemmata 1 and 3 one observes that these blocks are circulant. The $\ell \times \ell$ blocks of $A(BC)$ represent the sum of products of anti-circulant matrices with circulant ones. Via lemmata 2 and 3, one observes that these blocks are anti-circulant. The matrix ABC is thus block-anti-circulant. □

4.1 Description

Let $v = V \times \ell$, $o = O \times \ell$ and $N = O + V$. Observe that when S is chosen in the shape (5), it is not block-anti-ciculant; to remedy this, choose S in the following $\ell \times \ell$ block-anti-circulant shape:

$$S =$$



. (6)

Then choose $\ell \times \ell$ block-anti-circulant matrices $F^{(i)}$ in the shape of (2). One observes that the matrices $P^{(i)}$ are block-anti-circulant as well. These matrices can be represented by only the first row of every block. This requires only $N^2\ell$ elements per matrix as opposed to the highly redundant $n^2 = N^2\ell^2$ elements associated with an explicit representation.

Matrices that represent quadratic forms, such as $F^{(i)}$ and $P^{(i)}$, are invariant under addition of skew-symmetric matrices. Over odd-characteristic fields[1] one can therefore always choose $F^{(i)}$ and $P^{(i)}$ to be symmetric, even when they are block-anti-circulant (but not necessarily when they are (block-)circulant). This reduces the storage requirement to $N(N+1)\ell/2$ field elements, down from $n(n+1)/2$. For fields of even characteristic, upper-triangular matrix representatives of the quadratic forms are preferred, and in this case the same compression argument applies. However, this means that the $\ell \times \ell$ blocks on the diagonal must be either identity or zero matrices.

We depart from the Macaulay matrix representation of the public key $\mathbf{P}$ or of the secret map $\mathbf{F}$ traditionally used in Petzoldt's compression technique. Instead, both $\mathbf{P}$ and $\mathbf{F}$ are represented as lists of symmetric block-anti-circulant matrices. Nevertheless, Petzoldt's compression technique still applies. The pseudorandom generator is used to generate the first row of every $\ell \times \ell$ block in the upper-triangular part, except for the bottom-most $O \times (O+1)/2$ blocks which are computed using S. Figure 2 elaborates.

[1] We restrict focus to odd-characteristic fields because the use of even-characteristic fields induces a security degradation, as shown in Sect. 4.2.

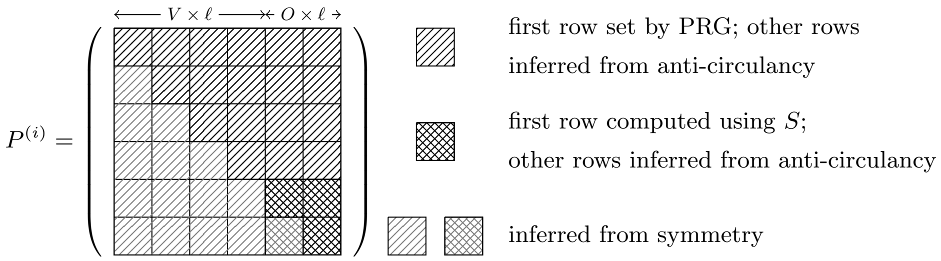

$V \times \ell$
$O \times \ell$
$P^{(i)} =$
first row set by PRG; other rows inferred from anti-circulancy
first row computed using S; other rows inferred from anti-circulancy
inferred from symmetry

Fig. 2. Petzoldt's compression technique with $\ell \times \ell$ block-anti-circulant matrices.

More explicitly, let $J_o^{\oplus}$ and $J_v^{\oplus}$ represent the $o \times o$ and $v \times v$ matrices that are zero everywhere except for the $\ell \times \ell$ blocks on the diagonals which are exactly J. Then form (6) is equivalent to $S = \left(\begin{array}{c|c} J_v^{\oplus} & S' \\ \hline 0_{[0:o,0:v]} & J_o^{\oplus} \end{array}\right)$ for some block-anti-circulant $v \times o$ matrix S'. The bottom right $o \times o$ block of $P^{(i)}$ is given by

$$P^{(i)}_{[v:n,v:n]} = {S'}^{\mathsf{T}} F^{(i)}_{[0:v,0:v]} S' + J_o^{\oplus} F^{(i)}_{[v:n,0:v]} S' + {S'}^{\mathsf{T}} F^{(i)}_{[0:v,v:n]} J_o^{\oplus} \ . \tag{7}$$

The nonzero blocks of $F^{(i)}$ are given by

$$F^{(i)}_{[0:v,0:v]} = J_v^{\oplus} P^{(i)}_{[0:v,0:v]} J_v^{\oplus} \tag{8}$$

$$F^{(i)}_{[0:v,v:n]} = -J_v^{\oplus} P^{(i)}_{[0:v,0:v]} J_v^{\oplus} S' J_o^{\oplus} + J_v^{\oplus} P^{(i)}_{[0:v,v:n]} J_o^{\oplus} \tag{9}$$

$$F^{(i)}_{[v:n,0:v]} = -J_o^{\oplus} {S'}^{\mathsf{T}} J_v^{\oplus} P^{(i)}_{[0:v,0:v]} J_v^{\oplus} + J_o^{\oplus} P^{(i)}_{[v:n,0:v]} J_v^{\oplus} \ . \tag{10}$$

Altogether, if Petzoldt's technique is used in conjunction with our block-anti-circulant compression, then the public key is given by $m\ell O(O+1)/2$ field elements and a short seed.

4.2 Security

This section evaluates to which extent the additional structure in the public key facilitates attacks; based on this analysis, we propose parameters later on. The following attacks are considered: Direct Algebraic Attack, Kipnis-Shamir Attack, and UOV Reconciliation Attack.

Direct Attack. A direct algebraic attack involves deploying Gröbner basis type algorithms [6,5,10,11] in order to solve for $\mathbf{s} \in \mathbb{F}_q$ the system of multivariate quadratic polynomial equations given by $\left(\mathbf{s}^{\mathsf{T}} P^{(i)} \mathbf{s}\right)_{i=0}^{m-1} = \mathbf{h}$, where $\mathbf{h} = \mathsf{H}(d) \in \mathbb{F}_q^m$ is the hash of a target document. The question is whether the introduction of the blockwise anti-circulant structure in order to compress the public key decreases the complexity of such an attack. We implemented the scheme with and without block-anti-circulant compression in Magma in order to test empirically whether this is the case.

In particular, we instantiate two systems of polynomials:

1. m equations in n variables without block-anti-circulant compression; this corresponds to $\ell = 1$.
2. m equations in $n = N \times \ell$ variables with block-anti-circulant compression; this corresponds to $\ell > 1$.

In both cases, the first $n - m$ variables were assigned random values that still guarantee that a solution exists. Figure 3 shows the running time of these attacks as a function of ℓ, for various values of (q, m), as performed by Magma's implementation of F_4 on an eight core 2.9 GHz machine. The plots suggest that over fields of even characteristic, block-anti-circulant matrices come with a security degradation proportional to the degree of circulancy. In contrast, the security of the same construction but over fields of odd characteristic seems largely unaffected by the degree of circulancy.

Given the correspondence between anti-circulant matrices and the ring $\frac{\mathbb{F}_q[x]}{\langle x^\ell - 1 \rangle}$, another natural question is whether arithmetic in this ring can help mount a direct attack. Solutions might be found in each component term of $\frac{\mathbb{F}_q[x]}{\langle x^\ell - 1 \rangle} \cong \frac{\mathbb{F}_q[x]}{\langle x - 1 \rangle} \oplus \frac{\mathbb{F}_q[x]}{\langle (x^\ell - 1)/(x-1) \rangle}$ before being joined together using the Chinese Remainder Theorem. However, finding even one such solution still requires solving a system of m equations in N variables; as a result the complexity of this task is already captured by Fig. 3.

Kipnis-Shamir Attack. The present proposal is not the first time circulant matrices have been considered in conjunction with UOV. Peng and Tang recently proposed choosing the secret quadratic forms $F^{(i)}$ to have a specific structure such that during signature generation, the coefficient matrix becomes circulant [12]. This embedded structure not only shrinks the secret key, but it also speeds up signature generation. However, Hashimoto shows that this scheme is vulnerable to a Kipnis-Shamir attack, despite the numbers of vinegar and oil variables being unbalanced [8].

The circulancy in the scheme of Peng and Tang arises as a result of recycling oil-vinegar coefficients across the quadratic forms $F^{(i)}$. The algebraic relation that describes this recycling, is exactly the algebraic property that gives rise to the attack. If the $F^{(i)}$ are chosen independently, the required relation does not hold and the attack fails — or rather, the attack works only with the exponential complexity $O(q^{v-o})$ of regular unbalanced oil and vinegar.

The $F^{(i)}$ in our construction do have structure, but do not have algebraic properties relating $F^{(i)}$ for various i. The coefficient matrix obtained while generating a signature does not have a circulant or block-anti-circulant structure. The attack can conceivably be performed over $\mathbb{F}_q[x]/\langle x^\ell - 1 \rangle$ and even over the constituent terms of this ring. The number V of vinegar *blocks* must be chosen accordingly, *i.e.*, such that the targeted security level is reached by q^{V-O}, or

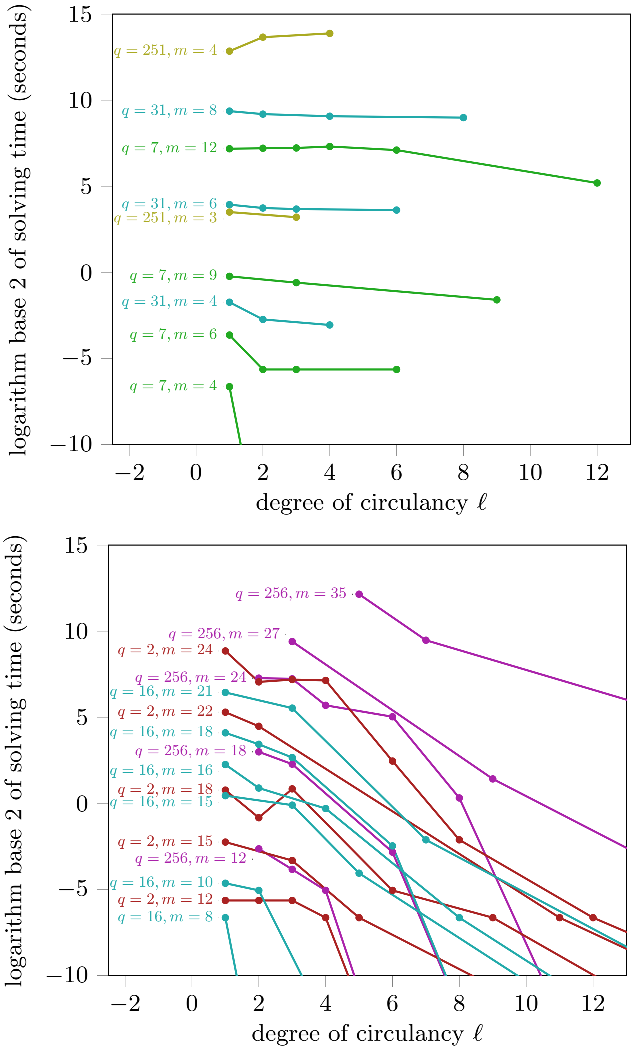


Fig. 3. Running time of direct algebraic attack for odd and even characteristic.

preferably by $q^{(V-O)/2}$ to account for a speedup on quantum computers due to Grover's algorithm [7].

UOV Reconciliation Attack. The UOV Reconciliation Attack [4] is an algebraic key recovery attack that mounts a search for the matrix S by treating its elements as variables and solving the system of equations obtained by equating $\left({S^{-1}}^{\mathsf{T}} P^{(i)} S^{-1}\right)_{[v:n,v:n]} = 0_{[0:o,0:o]}$ for all $i \in \{0, \ldots, m-1\}$. Ding *et al.* argue that the search can be decomposed into a series of steps of which the first dominates the complexity of the entire procedure [4]. This first step requires solving a system of m quadratic equations in v variables, originating from the number of polynomials, *i.e.*, m, and the number of unknowns in the rightmost column of S, *i.e.*, v. In the case of UOV where $v > m$ it is tempting to use a result by Thomae and Wolf showing how to reduce solving a system of m quadratic equations in $n = \alpha m$ variables to solving one of $m - \lfloor \alpha \rfloor + 1$ equations in as many variables [14]. However, Beullens and Preneel argue that this reduction does not apply to this first step of the UOV Reconciliation Attack because it finds an arbitrary solution and not necessarily one that is consistent with the other steps [1]. Instead, Beullens and Preneel estimate the complexity of this attack as strictly larger than that of solving a system of v equations in v variables.

With respect to our construction, we assume optimistically from the point of view of the attacker that an attack over the simplest constituent term of the ring $\frac{\mathbb{F}_q[x]}{\langle x^\ell - 1 \rangle} = \frac{\mathbb{F}_q[x]}{\langle x - 1 \rangle} \oplus \cdots$ suffices to break the scheme. In this case the attack represents a search for the $V \times O$ unknown ring elements of the matrix S. In particular, the last column of S has only $V = v/\ell$ unknowns. However, the number of equations m remains unaffected by this ring switch. Therefore, as long as $V \geq m$, the introduction of block-anti-circulant structure incurs no security degradation.

4.3 Parameters and Comparison

We advise against using fields of even characteristic in light of the poor resilience of our block-anti-circulant compression against direct algebraic attacks, as shown in Fig. 3. However, we note that using odd characteristic fields does not preclude using the field lifting technique of Beullens and Preneel, although it does make it less effective. Denote by r the extension degree, *i.e.*, the signature equation is defined over $\mathbb{F}_{q^r}$ instead of $\mathbb{F}_q$.

We estimate the complexity of algebraic system solving using the Wiedemann method [11] along with Groverized fixing of variables [2,1]. This makes for a complexity of

$$C_{m,n,k} = O\left(q^{k/2} \cdot \binom{n-k+2}{2} \binom{d_{reg}(k) + n - k}{n-k}^2\right) \quad , \tag{11}$$

where k is the number of variables that are quantumly guessed, and the degree of regularity d_{reg} is given by the degree of the first non-positive term in the formal power series expansion of

$$HS(z) = \frac{(1-z^2)^m}{1-z^n} \quad . \tag{12}$$

To obtain one concrete number, we take the minimum of $C_{m,n,k}$ over all k and pretend as though the constant hidden by the Landau notation is equal to 1.

Table 1 presents a selection of parameter sets designed to meet various target levels of post-quantum security, measured in terms of the base 2 logarithm of the best attack's complexity. For convenience, it also offers comparisons with variants of UOV, namely:

- LUOV — UOV with Petzoldt's compression technique and field lifting [1].
- PCT — UOV with Petzoldt's compression technique [13].
- Plain — Plain UOV with no compression [9].

Table 1. Proposed parameter sets and comparison to other variants of UOV.

scheme	parameters	$\|pk\|$	$\|sig\|$	sec. lvl.
Plain	$q = 256, v = 106, m = o = 53$	658.36 kB	159 bytes	128.85
PCT	$q = 256, v = 106, m = o = 53$	74.07 kB	159 bytes	128.85
LUOV	$q = 2, v = 296, m = o = 40, r = 68$	4.00 kB	2.79 kB	128.17
ours	$q = 7, V = 99, O = 7, \ell = 8, r = 7$	4.59 kB	2.17 kB	129.13
Plain	$q = 256, v = 164, m = o = 82$	2.38 MB	246 bytes	191.89
PCT	$q = 256, v = 164, m = o = 82$	272.5 kB	246 bytes	191.89
LUOV	$q = 2, v = 444, m = o = 60, r = 84$	13.40 kB	5.16 kB	190.00
ours	$q = 7, V = 145, O = 6, \ell = 16, r = 5$	11.81 kB	4.42 kB	192.54
Plain	$q = 256, v = 224, m = o = 112$	6.05 MB	336 bytes	256.50
PCT	$q = 256, v = 224, m = o = 112$	692.13 kB	336 bytes	256.50
LUOV	$q = 2, v = 600, m = o = 82, r = 90$	34.06 kB	7.49 kB	256.13
ours	$q = 7, V = 198, O = 9, \ell = 13, r = 5$	25.06 kB	4.93 kB	256.52

4.4 Implementation

A full working proof of concept implementation was developed in Sage. The direct attack timings were obtained from a Magma implementation that only generates block-anti-cyclic public keys but does not do compression of any kind. The security levels are estimated using a Sage script. All source code is available under the Community Research and Academic Programming License (CRAPL) from github: `https://github.com/aszepieniec/bacuov`.

5 Conclusion

We propose to introduce a block-anti-circulant structure into the secret and private keys of the UOV signature scheme. While the addition of structure may accelerate some attacks, we argue that it is possible to either offset this acceleration or block it entirely by choosing parameters appropriately. The resulting public key is smaller than the variant of UOV that uses only Petzoldt's compression trick by a factor ℓ which determines the block size. For typical values of this parameter, *i.e.* between 6 and 8, the resulting public keys are several tens of kilobytes in size for all security levels.

With respect the metric $|pk| + |sig|$, our scheme represents a marginal improvement over LUOV for the 128 bit security level. For higher security levels, though, this size difference increases noticeably. This increasing size differece provides empirical evidence of the improved scaling behavior promised by the insertion of an anti-circulant structure. Nevertheless, whether this smaller bandwidth requirement justifies the computational overhead associated with working over odd characteristic fields, is a question whose answer likely depends on the context. At any rate, the present construction provides the protocol designer with a greater flexibility in his choice of parameters, thus enabling him to better finetune the cryptosystem to the constraints of his problem.

An important question not answered by the present work, is the degree to which performance is affected as a consequence of increasing the parameter V to take into account attacks over the ring $\mathbb{F}_q[x]/\langle x^\ell + 1 \rangle$. While the number of variables $n = (V + O) \times \ell$ grows quite dramatically, and in turn generates huge quadratic form matrices $F^{(i)} \in \mathbb{F}_q^{n \times n}$, it should be noted that the arithmetic involving these matrices can in fact be accelerated, just like the attacks can, by working over $\mathbb{F}_q[x]/\langle x^\ell + 1 \rangle$ instead. The *effective number of variables* therefore *decreases* with respect to the other variants of UOV of the same security level, although these variables do take values from a larger ring. In contrast, the parameter o, which determines the complexity signature generation via the bottleneck of solving the $m \times o$ linear system, is increased only marginally. In the end, the litmus test for assessing performance is a low-level implementation to facilitate a comparison to competing schemes. We leave such an implementation to future work.

An interesting question is raised by our empirical results: why is there a significant security degradation associated with a larger degree of circulancy specifically for fields of characteristic two? We conjecture that this degradation is related to the impossibility of representing quadratic forms over an even characteristic field by symmetric matrices. As a result, a block-anti-circulant representation of such a quadratic form necessarily contains blocks of zeros on its diagonal, thus greatly reducing the number of nonzero coefficients.

References

1. Beullens, W., Preneel, B.: Field lifting for smaller UOV public keys. In: Patra, A., Smart, N.P. (eds.) INDOCRYPT 2017. LNCS, vol. 10698, pp. 227–246. Springer (2017)
2. Chen, M., Hülsing, A., Rijneveld, J., Samardjiska, S., Schwabe, P.: From 5-pass *MQ* -based identification to *MQ* -based signatures. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part II. LNCS, vol. 10032, pp. 135–165 (2016)
3. Czypek, P., Heyse, S., Thomae, E.: Efficient implementations of MQPKS on constrained devices. In: Prouff, E., Schaumont, P. (eds.) CHES 2012. LNCS, vol. 7428, pp. 374–389. Springer (2012)
4. Ding, J., Yang, B., Chen, C.O., Chen, M., Cheng, C.: New differential-algebraic attacks and reparametrization of rainbow. In: Bellovin, S.M., Gennaro, R., Keromytis, A.D., Yung, M. (eds.) ACNS 2008. LNCS, vol. 5037, pp. 242–257 (2008)
5. Faugère, J.C.: A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In: ISSAC 2002. pp. 75–83. ACM (2002)

6. Faugère, J.C.: A new efficient algorithm for computing Gröbner bases (F4). Journal of pure and applied algebra 139(1-3), 61–88 (1999)
7. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Miller, G.L. (ed.) ACM STOC 1996. pp. 212–219. ACM (1996)
8. Hashimoto, Y.: On the security of circulant uov/rainbow. IACR Cryptology ePrint Archive 2018, 947 (2018), https://eprint.iacr.org/2018/947
9. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. In: Stern, J. (ed.) EUROCRYPT '99. Lecture Notes in Computer Science, vol. 1592, pp. 206–222. Springer (1999)
10. Mohamed, M.S.E., Cabarcas, D., Ding, J., Buchmann, J.A., Bulygin, S.: MXL$_3$: An efficient algorithm for computing Gröbner bases of zero-dimensional ideals. In: Lee, D.H., Hong, S. (eds.) ICISC 2009. LNCS, vol. 5984, pp. 87–100. Springer (2009)
11. Mohamed, W.S.A., Ding, J., Kleinjung, T., Bulygin, S., Buchmann, J.: PWXL: A parallel Wiedemann-XL algorithm for solving polynomial equations over GF (2). In: Cid, C., Faugère, J. (eds.) Conference on Symbolic Computation and Cryptography. pp. 89–100 (2010)
12. Peng, Z., Tang, S.: Circulant UOV: a new UOV variant with shorter private key and faster signature generation. TIIS 12(3), 1376–1395 (2018)
13. Petzoldt, A., Buchmann, J.A.: A multivariate signature scheme with an almost cyclic public key. IACR Cryptology ePrint Archive 2009, 440 (2009), http://eprint.iacr.org/2009/440
14. Thomae, E., Wolf, C.: Solving underdetermined systems of multivariate quadratic equations revisited. In: Fischlin, M., Buchmann, J.A., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 156–171. Springer (2012)