An Asymptotically Optimal Structural Attack on the ABC Multivariate Encryption Scheme

Dustin Moody[1], Ray Perlner[1], and Daniel Smith-Tone[1,2]

[1] National Institute of Standards and Technology,
Gaithersburg, Maryland, USA
[2] Department of Mathematics, University of Louisville,
Louisville, Kentucky, USA
{dustin.moody,ray.perlner,daniel.smith}@nist.gov

Abstract. Historically, multivariate public key cryptography has been less than successful at offering encryption schemes which are both secure and efficient. At PQCRYPTO '13 in Limoges, Tao, Diene, Tang, and Ding introduced a promising new multivariate encryption algorithm based on a fundamentally new idea: hiding the structure of a large matrix algebra over a finite field. We present an attack based on subspace differential invariants inherent to this methodology. The attack is a structural key recovery attack which is asymptotically optimal among all known attacks (including algebraic attacks) on the original scheme and its generalizations.

Keywords: multivariate public key cryptography, differential, invariant, encryption.

1   Introduction

In the mid 1990s, Peter Shor developed efficient algorithms for factoring and computing discrete logarithms with quantum computers [1]. Since that time, the state-of-the-art of quantum computing has changed significantly, indicating that large scale quantum computing may become an eventual reality. In the years since Shor's discovery, there has emerged a rapidly growing community dedicated to the task of constructing algorithms resistant to cryptanalysis with quantum computers.

Multivariate Public Key Cryptography(MPKC) is one among a few serious candidates to have risen to prominence as post-quantum options. The appeal of MPKC is due to several factors. The fundamental problem of solving a system of quadratic equations is known to be NP-hard, and so in the worst case, solving a system of generic quadratic equations is unfeasible for a classical computer; neither is there any indication that the task is easier in the quantum computing paradigm. Furthermore, experience indicates that this problem is hard even in the average case; thus multivariate cryptosystems at least have a chance of being difficult to break. Secondly, multivariate cryptosystems are often very efficient,

see [2–4]. Finally, such cryptosystems can be very amenable to the user demands, with multiple parameters hidden within the system which can be altered by the user to achieve different performance goals.

Though MPKC has a turbulent history with many schemes failing against only a few attack techniques, there are still some entirely usable and trustworthy quantum-resistant multivariate signature schemes. Specifically, UOV [5], HFE- [6], and HFEv- [7] are noteworthy in this regard. Moreover, some of these schemes have optimizations which have strong theoretical support or have stood unbroken in the literature for some time. Specifically, UOV has a cyclic variant [8] which reduces the key size dramatically, and QUARTZ, an HFEv- scheme, has had its parameters tweaked [9] due to greater confidence in the complexity of algebraically solving the underlying system of equations [10].

Where MPKC has failed more directly has been encryption. There is a striking lack of reliable multivariate encryption schemes in the literature. Many attempts, see [11, 12] for example, have been shown to be weak based on rank or differential weaknesses. The most recent and promising attempt, by Tao et al., see [13], uses a fundamentally new structure for the derivation of an encryption system. Specifically, the scheme masks matrix multiplication to generate a system of structured quadratic equations.

In this article, we present a structural attack which is the asymptotically optimal attack on this matrix encryption scheme, having a complexity on the order of q^{s+4}, where s is the dimension of the matrices in the scheme. This technique uses a differential invariant property of the core map to perform a key recovery attack. We reevaluate some of the security analysis from the original ABC specification and conclude that this attack is asymptotically optimal among structural attacks. In fact, the attack uses a property which uniquely distinguishes the isomorphism class of the core map from that of a random collection of formulae. This attack asymptotically defeats algebraic attacks as well, though falling short of the benchmark established by generic algebraic attacks for the original parameters. This result supports the security claims of the designers (modulo decryption failure).

The paper is organized as follows. In the next section, we present the structure of the original ABC encryption scheme. The following section reviews some of the previous cryptanalyses of the scheme, and clarifies some of the previous attacks. In the subsequent section, we recall differential invariants. The differential invariant structure of the ABC scheme is then presented and the effect of this structure on minrank calculations is derived. In the following section, the complexity of the full attack is calculated and compared to the complexity of other valid structural attacks. Finally, we review these results and discuss the implications for the practical security of the ABC scheme.

2   The ABC Matrix Encryption Scheme

In [13], Tao et al. introduce the ABC Matrix encryption scheme. For the simplicity of the exposition, we will analyze the original scheme noting that all results carry over exactly as stated to the updated version, see [14].

The scheme depends on an initial parameter $s \in \mathbb{N}$. The public key consists of $n = s^2$, variables taking values in a fixed finite field $k = \mathbb{F}_q$, and $m = 2s^2$ equations. The system utilizes the butterfly construction, creating a private collection of formulae Q, and deriving a public key P by composing two invertible linear transformations $U \in GL_n(k)$ and $T \in GL_m(k)$, so that $P = T \circ Q \circ U$. What makes the system unique is the derivation of the map Q. For ease of analysis later, we will denote plaintext by $\bar{x} = (x_1, \dots, x_n) \in k^n$, ciphertext by $\bar{y} = (y_1, \dots, y_m) \in k^m$, and the input and output of Q by $\bar{u} = (u_1, \dots, u_n) = U(x_1, \dots, x_n) \in k^n$ and $\bar{v} = (v_1, \dots, v_m) = T^{-1}(y_1, \dots, y_m) \in k^m$, respectively. The construction begins by defining three $s \times s$ matrices A, B, and C. Specifically, we have:

$$
A = \begin{bmatrix} u_1 & u_2 & \cdots & u_s \\ u_{s+1} & u_{s+2} & \cdots & u_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ u_{s^2-s+1} & u_{s^2-s+2} & \cdots & u_{s^2} \end{bmatrix}, B = \begin{bmatrix} b_1 & b_2 & \cdots & b_s \\ b_{s+1} & b_{s+2} & \cdots & b_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ b_{s^2-s+1} & b_{s^2-s+2} & \cdots & b_{s^2} \end{bmatrix},
$$

and

$$
C = \begin{bmatrix} c_1 & c_2 & \cdots & c_s \\ c_{s+1} & c_{s+2} & \cdots & c_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ c_{s^2-s+1} & c_{s^2-s+2} & \cdots & c_{s^2} \end{bmatrix}.
$$

Here the b_i and c_i are linear combinations of the u_i chosen independently and uniformly at random from the collection of all possible k-linear combinations of the u_i.

Next, the $s \times s$ matrices $E_1 = AB$ and $E_2 = AC$ are constructed. Since all of A, B, and C are linear in u_i, E_1 and E_2 are quadratic in the u_i. Finally, setting $Q_{(l-1)s^2+(i-1)s+j}$ to be the (i,j)th element of E_l, we have the private key T, Q, U and the public key $P = T \circ Q \circ U$.

Encryption with this system is standard: given a plaintext $(x_1, \dots, x_n)$, compute $(y_1, \dots, y_m) = P(x_1, \dots, x_n)$. Decryption is somewhat more complicated.

To decrypt, one inverts each of the private maps in turn: apply T^{-1}, invert Q, and apply U^{-1}. To "invert" Q, one assumes that A is invertible, and forms a matrix

$$
A^{-1} = \begin{bmatrix} w_1 & w_2 & \cdots & w_s \\ w_{s+1} & w_{s+2} & \cdots & w_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ w_{s^2-s+1} & w_{s^2-s+2} & \cdots & w_{s^2} \end{bmatrix},
$$

where the w_i are indeterminants. Then using the relations $A^{-1}E_1 = B$ and $A^{-1}E_2 = C$, we have $m = 2s^2$ linear equations in $2n = 2s^2$ unknowns w_i and u_i.

(We note here that it would be more correct to say $A^{-1}(\bar{u})E_1(\bar{u}) = B(\bar{u})$ and $A^{-1}(\bar{u})E_2(\bar{u}) = C(\bar{u})$, since the values of these matrices depend on $\bar{u}$.) Using, for example, Gaussian elimination one can eliminate all of the variables w_i and most of the u_i. The resulting relations can be substituted back into $E_1(\bar{u})$ and $E_2(\bar{u})$ to obtain a large system of equations in very few variables which can be solved efficiently in a variety of ways.

In [14], the scheme is revised, replacing the square matrices A, B, and C with matrices of dimension $s \times r$, $r \times u$, and $r \times v$, respectively, where $r < s$. In addition, the matrix A consists of random linear forms just as B and C in the improved scheme. The public key is constructed in the exact same way, and encryption is performed by evaluating the public polynomials at the plaintext. Decryption is analogous to the original scheme, except now, since A is $s \times r$, only a left inverse of A on k^r is needed, so the matrix W, a left inverse, is $r \times s$ such that $WA = I_r$, the $r \times r$ identity matrix. Such a W plays the role of A^{-1} in the decryption, and decryption proceeds as above.

3   Security Claims, Revisions, and Corrections

3.1   Decryption Failure

In [13], it was claimed in error that the probability of decryption failure in the ABC scheme is very small, depending specifically on the probability that $dim(ker(A)) \leq 2$. This mistake was corrected in [14], revealing that the probability is approximately q^{-1}, where $|k| = q$. Also in [14], the scheme was generalized so that decryption can be accomplished as long as A (reparametrized as an $s \times r$ matrix) merely has a left inverse as a function on k^r, which occurs with high probability, roughly $1 - q^{r-s-1}$ when $s > r$.

3.2   HOLEs Attack

In [13], HOLEs attack analysis against the scheme was presented. Consider the equation

$$BE_1^{-1}E_2 = C. \tag{1}$$

For $B, C, E_1, E_2 \in M_s(k)$, we can consider the characteristic polynomial $f(x) = x^s + a_{s-1}x^{s-1} + \cdots + a_1x + a_0$ of E_1, and then we have that $E_1(-E_1^{s-1} - a_{s-1}E_1^{s-2} + \cdots - a_1I) = det(E_1)I$ by the Cayley-Hamilton theorem. In fact, the set of all polynomials evaluating to this scalar matrix at E_1 is $a_0 + \langle min_k(E_1) \rangle$, where $min_k(E_1)$ is the minimal polynomial of E_1. Let $xg(x) \in a_0 + \langle min_k(E_1) \rangle$ be a polynomial of smallest degree with constant coefficient zero. Since $det(E_1)I$ is a scalar matrix, it is in the center of $GL_s(k)$, and so multiplying equation (1) on the left by $-E_1g(E_1) = det(E_1)I$, we obtain

$$Bg(E_1)E_2 = det(E_1)C. \tag{2}$$

In this equation, g clearly depends on E_1, which for the purposes of the HOLEs attack is a function of $\bar{y}$. Thus to create a similar relation for plaintext/ciphertext

pairs requires us to consider $B(\bar{x}), C(\bar{x}) \in M_s(k[x_1, \ldots, x_n])$ & $E_1(\bar{y}), E_2(\bar{y}) \in M_s(k[y_1, \ldots, y_m])$, where $k[\cdot, \ldots, \cdot]$ is a polynomial ring in the indeterminants $x_1, \ldots, x_n$ and $y_1, \ldots, y_m$, respectively. Then by the invertibility of T we have that the minimal polynomial of $E_1(\bar{y})$ is equal to the characteristic polynomial. Thus there is a polynomial $g(z) \in k(y_1 \ldots, y_m)[z]$ of degree $s - 1$ (specifically $(-min_{k(y_1, \ldots, y_m)}(E_1(\bar{y})) + det(E_1(\bar{y})))/z$) such that $zg(z) = det(E_1(\bar{y}))$. Clearly, if $E_1(\bar{y})$ is singular then equation (1) is invalid; however, equation (2) still holds since

$$Bg(E_1)E_2 = Bg(AB)AC = BAg(BA)C = 0,$$

with the last equality due to the fact that the characteristic polynomials of AB and BA are identical. We may then obtain the relation (2). Notice that if U and T are linear as in the original description of the scheme then this equation is homogeneous of degree $s + 1$, specifically:

$$\sum_{i=1}^{n} \sum_{j_1, \ldots, j_s=1}^{m} \alpha_{i, j_1, \ldots, j_s} x_i y_{j_1} \cdots y_{j_s} = 0. \tag{3}$$

Even in this more manageable situation, the complexity of finding a nontrivial solution is immense. First, the adversary must generate $O(n\binom{m}{s}) = O(s^2\binom{2s^2}{s})$ plaintext/ciphertext pairs, and then solve a system of roughly $s^2\binom{2s^2}{s}$ equations in $s^2\binom{2s^2}{s}$ variables. The complexity of this operation is roughly $(s^2\binom{2s^2}{s})^\omega$ where $\omega = 2.3766$ operations. In the more realistic scenario of having a nonhomogeneous system, the analysis in [13] indicates that the complexity of the HOLEs attack is $O((s^2\binom{2s^s+s}{s}) + 2s^2 + 1)^\omega)$.

Remark 1. It is important to note that the HOLEs attack fails in the generalization [14] because the matrices are no longer square.

3.3 Rank Attacks

Rank attacks use linear maps associated with the public key to detect abnormal behavior. In the context of the ABC scheme, we may look at the associated quadratic forms of the public and private keys, or more or less equivalently, at the differentials of these maps. The MinRank attack searches for maps of low rank when viewed as matrices. We will discuss the MinRank attack in greater detail as well as a variant of the high rank attack not considered in [13] in Sections 5 and 6. The dual rank attack searches for a small subspace of the plaintext space which is in the kernel of a large subspace of the span of the maps.

In [13], it was stated that the task of finding a subspace of dimension $n - 2s$ of the associated quadratic forms which share a common nonzero element in their kernels is of complexity $O(n^6 q^{2s})$. This claim is overcautious. Given an element Q_0 in the first row of either $E_1(\bar{u})$ or $E_2(\bar{u})$, the formula is derived from the product of the first row of $A(\bar{u})$ and some column of $B(\bar{u})$ or $C(\bar{u})$ respectively. Since these columns are independent of one another and follow the

uniform distribution on the set of all column vectors (the joint distribution is inherited from the i.i.d. entries of B and C), Q_0 has rank $2s$ with near certainty. Since Q_0 has a matrix representation in the block form:

$$Q_0 = \left[\begin{array}{c|ccc} R_1 & R_2 & \cdots & R_s \\ \hline R_{s+1} & & & \\ \vdots & & 0 & \\ R_{2s-1} & & & \end{array}\right],$$

where each R_i is an $s \times s$ matrix, any element $\bar{z}$ in the kernel of Q_0 has an s-dimensional leading block of zeros with probability $\prod_{j=0}^{s-1} \frac{q^{s^2}-q^j}{q^{s^2}}$ which is *extremely* close to one. The first s rows of Q_0 put a further s constraints on $\bar{z}$. Given that the condition of being in the kernel of s such maps *of the same structure* results in an expected solution space of dimension 0, it is clear that there is no nontrivial element in the kernel of any large subspace of the span of the associated matrices. Thus the dual rank attack is nonexistent for the ABC scheme.

3.4 Algebraic Attacks

Based on an analysis of the degree of regularity for the ABC scheme the designers computed a degree of regularity $d_{reg} = 9$, and given the formula from [15] they estimated the complexity of the algebraic attack to be approximately

$$\binom{n + d_{reg}}{d_{reg}}^{2.3766} = \binom{73}{9}^{2.3766} \approx 2^{86}.$$

4 Subspace Differential Invariants

Let $f : k^n \to k^m$ be an arbitrary fixed function on k^n. Consider the differential $Df(a,x) = f(a+x) - f(a) - f(x) + f(0)$. We can express the differential as an n-tuple of differential coordinate forms in the following way: $[Df(a,x)]_i = a^T Df_i x$, where Df_i is a symmetric matrix representation of the action on the ith coordinate of the bilinear differential.

In [16], the following definition of a differential invariant was provided:

Definition 1. *A differential invariant of a map $f : k^n \to k^m$ is a subspace $V \subseteq k^n$ with the property that there exists a $W \subseteq k^n$ of dimension at most $dim(V)$ for which simultaneously $AV \subseteq W$ for all $A \in Span_i(Df_i)$.*

The motivation for the definition is to capture the behaviour of a nonlinear function which acts linearly on a subspace.

We note that any simultaneous invariant of all $Span_i(Df_i)$ satisfies the above definition, as well as invariants in the balanced oil and vinegar primitive, which are found in the product of an element and the inverse of another element in

$Span_i(Df_i)$. A differential invariant is thus a more general construct than a simultaneous invariant among all differential coordinate forms.

A natural generalization of the notion of a differential invariant is a subspace differential invariant.

Definition 2. *A subspace differential invariant of a map $f : k^n \rightarrow k^m$ with respect to a subspace $X \subseteq k^m$ is a subspace $V \subseteq k^n$ with the property that there exists a $W \subseteq k^n$ of dimension at most $dim(V)$ such that simultaneously $AV \subseteq W$ for all $A = \sum_{i=1}^m x_i Df_i$ where $(x_1, \ldots, x_m) \in X$, i.e. $A \in Span_X(Df_i)$.*

While the motivation for the differential invariant is to detect the linear action of a function on a subspace, the motivation for the subspace differential invariant is to detect the linear action of a subspace of the span of the public polynomials on a subspace of the plaintext space.

5   The Differential Invariant Structure of the ABC scheme

5.1   Prototypical Band-Spaces

Each component of the central $Q(\bar{u}) = E_1(\bar{u})||E_2(\bar{u})$ map may be written as:

$$Q_{(i-1)s+j} = \sum_{l=1}^{s} u_{(i-1)s+l}b_{(l-1)s+j}, \tag{4}$$

for the E_1 equations, and likewise, for the E_2 equations:

$$Q_{s^2+(i-1)s+j} = \sum_{l=1}^{s} u_{(i-1)s+l}c_{(l-1)s+j} \tag{5}$$

where i and j run from 1 to s.

Note that these $2s^2$ component equations may be grouped into s sets, indexed by i, of $2s$ equations. In particular note that the only quadratic monomials contained in $Q_{(i-1)s+j}$ and $Q_{s^2+(i-1)s+j}$ are those involving at least one factor of the variables $u_{(i-1)s+1}, \ldots, u_{(i-1)s+s}$. Moreover, since the coefficients of the linear polynomials $b_r(u)$ and $c_r(u)$ are uniformly random and independent, the nonzero coefficents are uniformly random and independent within each set of $2s$ equations.

Definition 3. *The ith band-space of maps $\mathcal{B}_i$ is the $2s$-dimensional space of quadratic forms given by*

$$\mathcal{B}_i = Span\{Q_{(i-1)s+1}, Q_{(i-1)s+2}, \ldots, Q_{is}, Q_{s^2+(i-1)s+1}, Q_{s^2+(i-1)s+2}, \ldots, Q_{s^2+is}\}.$$

In particular, the ith band-space is the span of the maps in the private key derived from the product of the ith row of A with the columns of B and C.

Any map Q_0 in the ith band-space has a differential in block form:

$$DQ_0 = \begin{bmatrix} 0 & R_1 & 0 \\ \hline R_1^T & R_2 & R_3 \\ \hline 0 & R_3^T & 0 \end{bmatrix} \tag{6}$$

having a band of nonzero values restricted to the ith s-dimensional block column and ith S-dimensional block row, hence the name. Notice that any vector $\bar{u}$ of the form:

$$(u_1, \ldots, u_{(i-1)s}, 0, \ldots, 0, u_{is+1}, \ldots, u_{s^2})^T$$

is mapped to a vector $\bar{v}$ of the form:

$$(0, \ldots, 0, v_{(i-1)s+1}, \ldots, v_{is-1}, 0, \ldots, 0)^T$$

by the differential of any map in $\mathcal{B}_i$. Therefore, the space of all such $\bar{u}$ is a subspace differential invariant of Q with respect to $\mathcal{B}_i$.

5.2   Generalized Band-Spaces

A critical observation is that the band-spaces associated with the rows of A are not the only band-spaces corresponding to a subspace differential invariant.

Definition 4. *Fix an arbitrary vector v in the rowspace of A, i.e. $v = \sum_{d=1}^{s} \lambda_d A_d$ where A_d is the dth row of A. The $2s$-dimensional space of quadratic forms $\mathcal{B}_v$ given by the span of the columns of vB and vC is called the* generalized band-space generated by v.

Theorem 1. *There is a subspace $V \subseteq k^n$ which is a subspace differential invariant with respect to $\mathcal{B}_v$ for all v in the rowspace of A. Moreover, $rank(DQ) \leq 2s$ for all $Q \in \mathcal{B}_v$.*

Proof. We prove the result for $v = \lambda_1 A_1 + \lambda_2 A_2$, an arbitrary linear combination of the first two rows of A. The general result follows from an analogous argument.

Any quadratic form in $\mathcal{B}_v$ is a linear combination of the columns of vB and vC, $Q_0 = \sum_{l=1}^{s} \gamma_l vB_l + \sum_{l=1}^{s} \delta_l vC_l$. This quantity can be rewritten as $Q_0 = v(\sum_{l=1}^{s} \gamma_l B_l + \sum_{l=1}^{s} \delta_l C_l)$. Since each of the entries of B and C are independent and random linear combinations in the coefficients of $\bar{u}$, each entry of the linear combination of the column vectors is itself a fixed but arbitrary such linear combination. Expressing the ith entry in this column vector as $\sum_{j=1}^{s^2} \zeta_{i,j} u_j$, and using the fact that $v = [\lambda_1 u_1 + \lambda_2 u_{s+1}, \lambda_1 u_2 + \lambda_2 u_{s+2}, \ldots, \lambda_1 u_s + \lambda_2 u_{2s}]$ we obtain:

$$Q_0 = v(\sum_{l=1}^{s} \gamma_l B_l + \sum_{l=1}^{s} \delta_l C_l)$$

$$= \sum_{i=1}^{s} (\lambda_1 u_i + \lambda_2 u_{s+i}) \sum_{j=1}^{s^2} \zeta_{i,j} u_j \qquad (7)$$

$$= \sum_{i=1}^{s} \sum_{j=1}^{s^2} (\lambda_1 \zeta_{i,j} u_i u_j + \lambda_2 \zeta_{i,j} u_{s+i} u_j).$$

Let M be the $s^2 \times s^2$ matrix obtained from this sum by setting the (i,j)th entry equal to the coefficient of $u_i u_j$, the $(s+i,j)$th entry equal to the coefficient of $u_{s+i} u_j$, and all other entries zero:

$$M = \begin{bmatrix} \lambda_1 \zeta_{1,1} & \lambda_1 \zeta_{1,2} & \cdots & \lambda_1 \zeta_{1,s^2} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1 \zeta_{s,1} & \lambda_1 \zeta_{s,2} & \cdots & \lambda_1 \zeta_{s,s^2} \\ \lambda_2 \zeta_{1,1} & \lambda_2 \zeta_{1,2} & \cdots & \lambda_2 \zeta_{1,s^2} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_2 \zeta_{s,1} & \lambda_2 \zeta_{s,2} & \cdots & \lambda_2 \zeta_{s,s^2} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

Notice that the differential of Q_0 is exactly the sum of M and M^T: $DQ_0 = M + M^T$. Since M has rank at most s, M^T has rank at most s. Thus by the subadditivity of rank, the rank of DQ_0 is at most $2s$. By the randomness of the coefficients of B and C the rank of DQ_0 is $2s$ with overwhelming probability (roughly q^{s-s^2-1}).

Consider performing column operations on M^T. In particular, consider operations such as subtracting $\lambda_2 \lambda_1^{-1}$ times column 1 from column $s+1$. It is clear that these operations can be used to eliminate the entries in columns $s+1$ through $2s$ of M^T. Let R be the matrix representing these column operations. Then $M^T R$ only has nonzero entries in the first s columns. Similarly, $R^T M$ only has nonzero entries in the first s rows.

Finally, consider the action $R^T DQ_0 R$. By distributivity we have $R^T DQ_0 R = R^T M R + R^T M^T R$, and by associativity, we have $(R^T M)R + R^T(M^T R)$. In the first summand column operations are performed on a matrix with nonzero entries in only the first s rows, resulting in a matrix with entries in only the top s rows. The second summand is the transpose of the first. Therefore, we see that $R^T DQ_0 R$ has the form:

$$R^T D Q_0 R = \left[\begin{array}{c|c} D_1 & D_2 \\ \hline D_2^T & 0 \end{array}\right],$$

where D_1 is $s \times s$ and D_2 is $s \times s^2 - s$. Thus $R^T D Q_0 R$ maps the subspace V' consisting of column vectors with the first s entries zero to its orthogonal complement. Consequently DQ_0 maps RV' to an s dimensional space. Further, notice that the row and column operations depend only on v, and not on the fixed but arbitrary $Q_0 \in \mathcal{B}_v$. Therefore DQ maps RV' to an s dimensional space for all $Q \in \mathcal{B}_v$. Thus RV' is a subspace differential invariant with respect to $\mathcal{B}_v$.

Remark 2. *We note that a subspace differential invariant V with respect to a generalized band-space $\mathcal{B}_v$ is special in that V, of dimension $s^2 - s$, is mapped to a subspace W of dimension s by any differential of a band-space map. Thus, given two such subspace differential invariants, V and V' with respect to $\mathcal{B}_v$ and $\mathcal{B}_{v'}$, we can find another subspace differential invariant $V \cap V'$ with respect to $Span(\mathcal{B}_v, \mathcal{B}_{v'})$. In this manner we can generate subspace differential invariants with respect to spaces containing differentials of even full rank. In particular, if one manages to find a linear combination of the public differentials which is of rank $s^2 - 2s$, the kernel reveals some information about the structure of the scheme. Given the invariant structure of the ABC scheme, this task amounts to finding a linear combination that avoids any equation derived from a $\frac{s+2}{2}$ dimensional subspace of the rowspace of A.*

This technique forms the foundation of a high rank version of a differential invariant attack. The complexity of recovering such a map is on the order of $q^{3s/2}$, and more information is still needed to constitute a full attack; therefore, we conclude that the ABC scheme is safe from the high rank side.

6 The Effect of Invariant Structure on the Complexity of MinRank

The Minrank attack searches for a low rank linear combination of m $n \times n$ bilinear forms over $k = \mathbb{F}_q$, $B_1, \ldots, B_m$. In the case of Ding's ABC scheme, $m = 2s^2$, $n = s^2$, and the B_i maps are the public differentials DP_i. The attack proceeds by randomly choosing $\lceil \frac{m}{n} \rceil$ vectors, x_k, setting

$$\left(\sum_{i=1}^{m} \bar{t}_i DP_i \right) x_k = 0 \tag{8}$$

and solving for the $\bar{t}_i$. The attack succeeds when all of the x_k are in the kernel of the target map. Simple rank analysis suggests that the probability of success per iteration is $q^{-r\lceil \frac{m}{n} \rceil}$ where r is the rank of the target map. In the case of the

ABC scheme, the target maps are those within a band space, which typically have rank $2s$. Therefore, if we consider the rank of the target maps alone, we should expect a complexity on the order of q^{4s}. A more careful rank analysis reveals that the kernels of the band-space maps are interlinked in the sense given in [17]. Computing via a crawling process as described in [17], we see that the best estimate from a rank perspective has expected complexity roughly q^{2s}, since there are roughly sq^{2s} such kernels. However, the actual complexity of this process is on the order of q^s, due to the subspace differential invariant structure, as will be demonstrated in this section. To emphasize the advantage the differential invariant structure provides, we note that the recovery of maps of rank $r = 2s$ is accomplished with this attack in time roughly $q^{r/2}$.

This demonstation proceeds by defining the "band kernel", an $s^2 - s$ dimensional subspace of k^{s^2}, corresponding to each generalized band-space, $\mathcal{B}_v$. We then show that with probability q^{-1}, if x_1 and x_2 fall within band kernel j, then they are both in the kernel of some band-space differential

$$DQ = \sum_{Q_i \in \mathcal{A}_j} \tau_i DQ_i,$$

where the Q_i in the sum form a basis $\mathcal{A}_v$ of the band-space generated by v, $\mathcal{B}_v$.

Definition 5. *Let $u_1 \ldots u_{s^2}$ be the components of $U\bar{x}$ and fix an arbitrary vector v in the rowspace of A, i.e. $v = \sum_{d=1}^{s} \lambda_d A_d$ where A_d is the dth row of A. An s^2 dimensional vector, $\bar{x}$ is in the band kernel generated by v iff $\sum_{d=1}^{s} \lambda_d u_{ds+k} = 0$ for $k = 1 \ldots s$.*

Theorem 2. *If x_1 and x_2 fall within band kernel generated by v, then they are both in the kernel of some generalized band-space differential $DQ = \sum_{Q_i \in \mathcal{B}_v} \tau_i DQ_i$ with probability approximately q^{-1}.*

Proof. A DQ meeting the above condition exists iff there is a nontrivial solution to the following system of equations

$$\sum_{Q_i \in \mathcal{B}_v} \tau_i DQ_i x_1{}^T = 0$$

$$\sum_{Q_i \in \mathcal{B}_v} \tau_i DQ_i x_2{}^T = 0 \tag{9}$$

Expressed in a basis where the first s basis vectors are chosen to be outside the band kernel, and the remaining $s^2 - s$ basis vectors are chosen from within the band kernel, the band-space differentials take the form:

$$DQ_i = \begin{bmatrix} S_i & R_i \\ \hline R_i^T & 0 \end{bmatrix} \tag{10}$$

where R_i is a random $s \times s^2 - s$ matrix and S_i is a random symmetric $s \times s$ matrix. Likewise x_1 and x_2 take the form $(0| \, x_k \,)$. Thus removing the redundant degrees of freedom we have the system of $2s$ equations in $2s$ variables:

$$
\begin{aligned}
\sum_{i=1}^{2s} \tau_i R_i x_1{}^T &= 0 \\
\sum_{i=1}^{2s} \tau_i R_i x_2{}^T &= 0
\end{aligned}
\tag{11}
$$

This has a nontrivial solution precicely when the following matrix is singular:

$$
\left[
\begin{array}{c}
\begin{matrix} | & | & & | \\ R_1 x_1{}^T & R_2 x_1{}^T & \ldots & R_{2s} x_1{}^T \\ | & | & & | \end{matrix} \\
\hline
\begin{matrix} | & | & & | \\ R_1 x_2{}^T & R_2 x_2{}^T & \ldots & R_{2s} x_2{}^T \\ | & | & & | \end{matrix}
\end{array}
\right]
\tag{12}
$$

As the R_i are random and independent, this is simply a random matrix over $k = \mathbb{F}_q$, which is singular with probability approximately q^{-1}, for practical parameters.

The band space differentials DQ_i for the private maps $Q_i \in \mathcal{B}_v$ generate a subspace of the space generated by public differentials DP_i, the solutions $\sum_{Q_i \in \mathcal{B}_v} \tau_i DQ_i$ of equation (9) form a subspace of the solutions $\sum_{i=1}^{2s^2} \bar{t}_i DP_i$ of equation (8). The condition on x_1 for membership in the band kernel of $\mathcal{B}_v$ for some v is that the matrix A, formed as in equation (13) from the components $u_1 \ldots u_{s^2}$ of $U x_1$, is singular.

$$
A = \begin{bmatrix}
u_1 & u_2 & \cdots & u_s \\
u_{s+1} & u_{s+2} & \cdots & u_{2s} \\
\vdots & \vdots & \ddots & \vdots \\
u_{s^2-s+1} & u_{s^2-s+2} & \cdots & u_{s^2}
\end{bmatrix}
\tag{13}
$$

This occurs with probability approximately q^{-1}. Given x_1 is in some band kernel, x_2 has a probability of q^{-s} of being chosen within the same band kernel. Given that x_1 and x_2 are in the same band kernel, the probability that they are in the kernel of the same band-space map is q^{-1}. Thus, a generalized band space map may be found among the solutions of equation (8) with probability $q^{-(s+2)}$.

Equation (8) is a system of $2s^2$ equations in $2s^2$ variables, one might expect it to generally have a 0-dimensional space of solutions. There are, however, linear dependencies among the equations, due to the fact that the DQ_i are symmetric matrices. In odd characteristic, the only linear dependency is $x_1 DQ_i x_2{}^T - x_2 DQ_i x_1{}^T = 0$, thus we should expect a 1-dimensional space of solutions. However, in even characteristic there are two more linear dependencies:

$x_1 DQ_i x_1{}^T = 0$ and $x_2 DQ_i x_2{}^T = 0$. Thus, in even characteristic, we expect a 3-dimensional solution space for equation (8). Finding the expected 1-dimensional space of band-space solutions in this 3-dimensional space costs $q^2 + q + 1$ rank operations, which in turn cost $(s^2)^3$ field operations. Thus the total cost of finding a band-space map using MinRank is approximately $q^{s+4}s^6$ for even characteristic and $q^{s+2}s^6$ for odd characteristic.

We ran a series of experiments to determine the number of trials required for randomly selected x_1 and x_2 to lie in the kernel of a differential of rank $2s$. The experiments were performed using toy examples of the scheme with $q = 3, 5$ and $s = 4, 5, 6, 7, 8$. In each of these cases the data support the theoretical complexity of $O(q^{s+2})$.

7   Complexity of Invariant Attack

While the detection of a low rank map in the space generated by the public differentials already constitutes a distinguisher from a random system of equations, it still falls short of a full key extraction. However, once two low rank differentials, DQ_1 and DQ_2, from the same generalized band space are found, the attacker can use similar methods to those used to attack balanced oil and vinegar. Recall that oil and vinegar can be broken by computing a product matrix $M = M_1^{-1}M_2$ and searching for large invariant subspaces. One complication arises, however which is that neither DQ_1 nor DQ_2 will be invertible, only having rank $2s$. This can be overcome by simply restricting DQ_1 and DQ_2 to act on random $2s$ dimensional subspace, W, of k^n. As long as the restrictions $DQ_1(W), DQ_2(W)$ are full rank in W, then $DQ_1(W)^{-1}DQ_2(W)$ will have an s dimensional invariant subspace, whose generators are also generators of the band kernel associated with DQ_1 and DQ_2.

Note that once we've found DQ_1 in $\mathcal{B}_v$, finding DQ_2 is approximately q times less costly. Since DQ_1 is known to contain in its kernel two vectors x_1 and x_2 from the band kernel generated by v, we simply need to find a rank $2s$ map, DQ_2, in the space of public differentials, whose kernel contains x_1 and another vector x_3. With overwhelming probability the only way this will occur is if x_3 is in the band kernel generated by v and DQ_2 is in $\mathcal{B}_v$.

Given bases for s independent band kernels generated by $v_1, \ldots, v_s$ we can reconstruct a private key of the same structure as that of the original ABC scheme, which has the same public differentials as the instance we are attacking. To see this, first note that there exists a U' for which the generalized band spaces $\mathcal{B}_{v_1} \ldots \mathcal{B}_{v_s}$ take the form of ordinary band spaces (i.e. for which $(U'^{-1})^T DQ U'^{-1}$ takes the form given in equation (6) when DQ is in $\mathcal{B}_{v_i}$.) U' is simply given by $U' = VU$, where V obeys

$$A(Vu) = \begin{bmatrix} v_1(u) \\ v_2(u) \\ \vdots \\ v_s(u) \end{bmatrix}.$$

Moreover there exists a B' C' and T' corresponding to U', that will give the same public key as U, B, C and T. These are given by:

$$B'(Vu) = B(u) \; i.e. \; B'(u') = B(V^{-1}u')$$
$$C'(Vu) = C(u) \; i.e. \; C'(u') = C(V^{-1}u')$$
$$T'(e_1', e_2') = T(V^{-1}e_1', V^{-1}e_2').$$

Thus, there exists an ABC private key, whose prototypical band spaces are equal to the generalized band spaces found by our attack. The task then remains to find it, or something equivalent. First note that the elements of row j of $A(U'x)$, which we will denote as $\bar{A}_j(U'x)$, are are in the band kernel generated by v_i for all $i \neq j$. The intersection of the band kernels generated by $v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_s$ is readily computable, given what we already have, and it has dimension s, and is therefore identical to the space generated by the elements of $\bar{A}_j(U'x)$.

This allows us to compute a map U'' which mostly mimics the action of U'. Specifically U'' only differs from U' by mixing the elements within the rows of the matrix A. i.e. $\bar{A}_j(U''x) = \Omega_j \bar{A}_j(U'x)$, where Ω_j is a nonsingular linear operator on s variables. U'' may also be extended into a full private key, U'', B'', C'', T'' for the target public key. The choice of B'' and C'' is straightforward:

$$B''(u'') = B'(U'U''^{-1}u'')$$
$$C''(u'') = C'(U'U''^{-1}u'')$$

All that remains is the choice of T''. To demonstrate that a choice is possible note that

$$\bar{A}_j(U''x)B''(U''x) = [\Omega_j \bar{A}_j(U'x)]B''(U''x)$$
$$= \Omega_j[\bar{A}_j(U'x)B''(U''x)]$$
$$= \Omega_j(\bar{A}_j(U'x)B'(U'x))$$

And similarly:

$$\bar{A}_j(U''x)C''(U''x) = \Omega_j(\bar{A}_j(U'x)C'(U'x)).$$

Thus, the components of $E'(U'x) = (A(U'x)B'(U'x), A(U'x)C'(U'x))$ are linearly related to the components of $E''(U''x) = (A(U''x)B''(U''x), A(U''x)C''(U''x))$ by the invertible maps Ω_j. There therefore exists an invertible T'' such that $T''E''(U''x) = T'E'(U'x) = TE(Ux)$.

All that remains is to solve for T'', B'', and C'', given our U''. This can be done by solving linear equations in the coefficients of B'', C'' and T''^{-1}:

$$D_k(A(x)B''(x), A(x)C''(x)) = \sum_l T_{kl}''^{-1}(U''^{-1})^T Dy_l(x)U''^{-1}$$

where the y_l are the components of the public map $TE(Ux)$.

The primary cost of the attack involves finding the s independent band kernels. Thus, the cost of a full private key extraction is $q^{s+4}s^7$ for even characteristic and $q^{s+2}s^7$ for odd characteristic.

Remark 3. The full key recovery attack for the improved ABC scheme of [14] (using an $s \times r$ A and n variables) requires $sq^{r+4}n^3$ operations for even characteristic and $sq^{r+2}n^3$ operations for odd characteristic.

8   Conclusion

The ABC scheme offers a promising new idea for the development of multivariate encryption schemes. Although the original presentation of the scheme contained errors— most significantly in the estimated probability of decryption failure— the scheme is easily generalized to nonsquare matrices and these anomalies are inconsequential in this context. In particular, the HOLEs attack is nonexistent when A, B, and C are replaced with rectangular matrices.

The attack outlined in this article exploits the subspace differential invariant structure inherent to the ABC methodology. The attack method works both for the original scheme and when applied to the updated scheme. With the original parameters, the attack is asymptotically the most efficient structural attack, with bit complexity scaling linearly with s, the square root of the number of variables. In the improved scheme, the attack scales in bit complexity in proportion to the parameter r which is less than the square root of the number of variables. This analysis is tighter than any relevant rank analysis in the literature, with the most appropriate technique in [17] scaling in bit complexity linearly with $2s$. In comparison, even the bit complexity of algebraic attacks scale superlinearly in s, though the break-even point for the two attacks is slightly beyond the 120-bit security threshold. Taking both time and memory into consideration, however, the differential invariant attack may be the more practical.

A remarkable fact about the attack outlined in this article is that it exploits characteristics which uniquely distinguish the public polynomials in the ABC scheme or its improvement from random formulae, namely, the existence of the s subspace differential invariants. The existence of the differential invariants relative to the band spaces is *equivalent* to the property of being isomorphic to a product of matrices of linear forms as in the central map of the ABC scheme; indeed, the attack produces such an isomorphism. In this sense, it is hard to imagine any key recovery attack on such a scheme designed for 80-bit security which is significantly more efficient in terms of time than the algebraic attack, directly solving the system via Gröbner Bases, or an XL variant such as the Mutant XL algorithms, see [18–20].

On the other hand, it is worthwhile mentioning Gröbner basis techniques for solving MinRank problems using minors modeling as in [21], and perhaps most notably exemplified in [22]. Assuming no additional structure in the MinRank instances arising from the cryptanalysis of the ABC scheme generic, the degree of regularity of the resulting MinRank polynomial systems is $2s+1$ for small values of s, and so the complexity of this approach is immense. The actual MinRank

instances arising from the ABC scheme, however, hold some of the structure of the central map and so there is some hope for improvement in this area, though this remains an open problem.

While it is clear that the decryption failure issue of the ABC scheme can be fixed by inflating the field size and/or by making the core matrices rectangular, the scalability of the scheme is an issue. The public key size of the original scheme scales with the *sixth* power of s. If we take into consideration security requirements beyond 80 bits, the ABC scheme becomes problematic; increasing s by one more than doubles the key size. While the evidence seems to suggest that the enhanced ABC scheme, despite having such a distinct differential structure, may ironically be secure, the task of turning the scheme into a more finely tuneable technology is still an open question.

References

1. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Sci. Stat. Comp. 26, 1484 (1997)
2. Chen, A.I.-T., Chen, M.-S., Chen, T.-R., Cheng, C.-M., Ding, J., Kuo, E.L.-H., Lee, F.Y.-S., Yang, B.-Y.: SSE implementation of multivariate PKCs on modern x86 CPUs. In: Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS, vol. 5747, pp. 33–48. Springer, Heidelberg (2009)
3. Chen, A.I.-T., Chen, C.-H.O., Chen, M.-S., Cheng, C.-M., Yang, B.-Y.: Practical-sized instances of multivariate PKCs: Rainbow, TTS, and ℓIC-derivatives. In: Buchmann, J., Ding, J. (eds.) PQCrypto 2008. LNCS, vol. 5299, pp. 95–108. Springer, Heidelberg (2008)
4. Yang, B.-Y., Cheng, C.-M., Chen, B.-R., Chen, J.-M.: Implementing minimized multivariate PKC on low-resource embedded systems. In: Clark, J.A., Paige, R.F., Polack, F.A.C., Brooke, P.J. (eds.) SPC 2006. LNCS, vol. 3934, pp. 73–88. Springer, Heidelberg (2006)
5. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 206–222. Springer, Heidelberg (1999)
6. Patarin, J., Goubin, L., Courtois, N.T.: C_-+^* and HM: Variations around two schemes of T. Matsumoto and H. Imai. In: Ohta, K., Pei, D. (eds.) ASIACRYPT 1998. LNCS, vol. 1514, pp. 35–50. Springer, Heidelberg (1998)
7. Patarin, J., Courtois, N., Goubin, L.: QUARTZ, 128-bit long digital signatures. In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 282–297. Springer, Heidelberg (2001)
8. Petzoldt, A., Bulygin, S., Buchmann, J.: CyclicRainbow – A multivariate signature scheme with a partially cyclic public key. In: Gong, G., Gupta, K.C. (eds.) INDOCRYPT 2010. LNCS, vol. 6498, pp. 33–48. Springer, Heidelberg (2010)
9. Anonymous: New parameters for quartz. Private Communication (2013)
10. Ding, J., Yang, B.Y.: Degree of regularity for hfev and hfev-. In: [23], pp. 52–66
11. Goubin, L., Courtois, N.T.: Cryptanalysis of the TTM cryptosystem. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 44–57. Springer, Heidelberg (2000)
12. Tsujii, S., Gotaishi, M., Tadaki, K., Fujita, R.: Proposal of a signature scheme based on STS trapdoor. In: Sendrier, N. (ed.) PQCrypto 2010. LNCS, vol. 6061, pp. 201–217. Springer, Heidelberg (2010)

13. Tao, C., Diene, A., Tang, S., Ding, J.: Simple matrix scheme for encryption. In: [23], pp. 231–242
14. Tao, C., Diene, A., Tang, S., Ding, J.: Improvement of simple matrix scheme for encryption. Personally Communicated (2013), Corresponding Author: Ding, J.
15. Bardet, M., Faugere, J.C., Salvy, B.: On the complexity of gröbner basis computation of semi-regular overdetermined algebraic equations. In: Proceedings of the International Conference on Polynomial System Solving (2004)
16. Perlner, R.A., Smith-Tone, D.: A classification of differential invariants for multivariate post-quantum cryptosystems. In: [23], pp. 165–173
17. Yang, B.-Y., Chen, J.-M.: Building secure tame-like multivariate public-key cryptosystems: The new TTS. In: Boyd, C., González Nieto, J.M. (eds.) ACISP 2005. LNCS, vol. 3574, pp. 518–531. Springer, Heidelberg (2005)
18. Ding, J., Buchmann, J., Mohamed, M., Mohamed, W., Weinmann, R.: Mutant xl. In: SCC 2008, LMIB, pp. 16–22 (2008)
19. Mohamed, M.S.E., Mohamed, W.S.A.E., Ding, J., Buchmann, J.: *MXL2*: Solving polynomial equations over GF(2) using an improved mutant strategy. In: Buchmann, J., Ding, J. (eds.) PQCrypto 2008. LNCS, vol. 5299, pp. 203–215. Springer, Heidelberg (2008)
20. Mohamed, M.S.E., Cabarcas, D., Ding, J., Buchmann, J., Bulygin, S.: MXL$_3$: An efficient algorithm for computing gröbner bases of zero-dimensional ideals. In: Lee, D., Hong, S. (eds.) ICISC 2009. LNCS, vol. 5984, pp. 87–100. Springer, Heidelberg (2010)
21. Faugère, J.C., Din, M.S.E., Spaenlehauer, P.J.: Computing loci of rank defects of linear matrices using gröbner bases and applications to cryptology. In: Koepf, W. (ed.) ISSAC, pp. 257–264. ACM (2010)
22. Bettale, L., Faugère, J.C., Perret, L.: Cryptanalysis of hfe, multi-hfe and variants for odd and even characteristic. Des. Codes Cryptography 69, 1–52 (2013)
23. Gaborit, P. (ed.): PQCrypto 2013. LNCS, vol. 7932. Springer, Heidelberg (2013)