Key Recovery Attack on the Cubic ABC Simple Matrix 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@nist.gov, ray.perlner@nist.gov, daniel.smith@nist.gov

Abstract. In the last few years multivariate public key cryptography has experienced an infusion of new ideas for encryption. Among these new strategies is the ABC Simple Matrix family of encryption schemes which utilize the structure of a large matrix algebra to construct effectively invertible systems of nonlinear equations hidden by an isomorphism of polynomials. The cubic version of the ABC Simple Matrix Encryption was developed with provable security in mind and was published including a heuristic security argument claiming that an attack on the scheme should be at least as difficult as solving a random system of quadratic equations over a finite field.
In this work, we prove that these claims are erroneous. We present a complete key recovery attack breaking full sized instances of the scheme. Interestingly, the same attack applies to the quadratic version of ABC, but is far less efficient; thus, the enhanced security scheme is less secure than the original.

Key words: multivariate public key cryptography, differential invariant, MinRank, encryption

1 Introduction

Classical public key cryptography is mainly based on arithmetic constructions on Abelian groups. Since the discovery by Peter Shor in the 1990s of efficient algorithms for factoring and computing discrete logarithms with quantum computers, see [1], there has been a growing interest in the international community in the task of constructing algorithms resistant to cryptanalysis with quantum computers. Indeed, in light of the announcement [2] by the National Institute of Standards and Technology (NIST) of an imminent call for proposals for post-quantum standards, the challenge of migrating from the homogeneous heritage of public key cryptography to a more diverse collection of tools has become mainstream.

One possible candidate for practical, efficient, and nonconforming solutions to some of the most consequential public key applications is Multivariate Public Key Cryptography(MPKC). Multivariate schemes are attractive in certain applications because of the maleability of the schemes. Different modifications of similar ideas can make a scheme more suited to lightweight architectures, enhance security, or parametrize various aspects of performance.

In addition, MPKC is one among a few serious candidates to have risen to prominence as post-quantum options. 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.

MPKC has experienced a fair amount of success in the realm of digital signatures. Some trustworthy schemes that have survived for almost two decades include UOV [3], HFE- [4], and HFEv- [5]. 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 [6] which reduces the key size dramatically, and Gui, a new HFEv- scheme, see [7], has parameters far more appealing than QUARTZ due to greater confidence in the complexity of algebraically solving the underlying system of equations [8].

The situation with multivariate public key encryption is quite different, however. Many attempts at multivariate encryption, see [9, 10] for example, have been shown to be weak based on rank or differential weaknesses. Recently, a few interesting attempts to achieve multivariate encryption have surfaced. ZHFE, see [11], and the ABC Simple Matrix Scheme, see [12], both use fundamentally new structures for the derivation of an encryption system. While it was shown that the best attack known on the Simple Matrix structure, see [13] — which relies on the differential invariant structure of the central map — supports the claimed security level of the scheme, a subset of the original authors proposed a cubic version of the scheme, [14], as a step towards provable security.

In this article, we present a key recovery attack on a full scale version of the Cubic Simple Matrix encryption scheme, having a complexity on the order of q^{s+2} for characteristic $p > 3$, q^{s+3} for characteristic 3 and q^{2s+6} for characteristic 2. Here s is the dimension of the matrices in the scheme, and q is the cardinality of the finite field used. This technique is an extension and augmentation of the technique of [13], and, similarly, exploits a differential invariant property of the core map to perform a key recovery attack. We can show that the attack uses a property which uniquely distinguishes the isomorphism class of the central map from that of a random collection of formulae.

Specifically, our attack breaks CubicABC($q = 127$,$s = 7$), designed for 80-bit security, in approximately 2^{76} operations (or around 2^{80} if one pessimistically uses $\omega = 3$ as the linear algebra constant). More convincingly, our attack completely breaks CubicABC($q = 127$,$s = 8$), designed for 100-bit security, in approximately 2^{84} operations (or 2^{88} for $\omega = 3$). Furthermore, the attack is fully parallelizable and requires very little memory; hence, the differential invariant

attack is far more efficient than algebraic attacks, the basis for the original security estimation. Thus, the security claims in [14] are clearly unfounded; in fact, the cubic version of the scheme, whose security was claimed to be closely related to an NP-complete problem, is actually less secure than the quadratic case.

The paper is organized as follows. In the next section, we present the structure of the Cubic ABC Simple Matrix encryption scheme. In the following section, we recall differential invariants and present a natural extension of this notion to the case of cubic polynomials. The differential invariant structure of the ABC scheme is derived in the subsequent section and the effect of this structure on minrank calculations is determined. We next calculate the complexity of the full attack including the linear algebra steps required to extend the distinguisher into a key recovery mechanism. Finally, we review these results and discuss the surprising relationship between the practical security of the Cubic ABC scheme and its quadratic counterpart.

2 The Cubic ABC Matrix Encryption Scheme

In [14], the Cubic ABC Matrix encryption scheme is proposed. The motivation behind the scheme is to use a large matrix algebra over a finite field to construct an easily invertible cubic map. The construction uses matrix multiplication to combine random quadratic formulae and random linear formula into cubic formulae in a way that allows a user with knowledge of the structure of the matrix algebra and polynomial isomorphism used to compose the scheme to invert the map.

Let $k = \mathbb{F}_q$ be a finite field. Linear forms and variables over k will be denoted with lower case letters. Vectors of any dimension over k will be denoted with bold font, $\mathbf{v}$. Fix $s \in \mathbb{N}$ and set $n = s^2$ and $m = 2s^2$. An element of $M_s(k)$, $M_n(k)$ or $M_m(k)$, or the linear transformations they represent, will be denoted by upper case letters, such as M. When the entries of the matrix are being considered functions of a variable, the matrix will be denoted $M(\mathbf{x})$. Let ϕ represent the vector space isomorphism from $M_{s\times 2s}(k)$ to k^{2s^2} sending a matrix to the column vector consisting of the concatenation of its rows. The output of this map, being a vector, will be written with bold font; however, to indicate the relationship to its matrix preimage, it will be denoted with an upper case letter, such as $\mathbf{M}$.

The scheme utilizes an isomorphism of polynomials to hide the internal structure. Let $\mathbf{x} = \left[x_1, x_2, \ldots, x_n\right]^\top \in k^n$ denote plaintext while $\mathbf{y} = \left[y_1, \ldots, y_m\right] \in k^m$ denotes ciphertext. Fix two invertible linear transformations $T \in M_m(k)$ and $U \in M_n(k)$. (One may use affine transformations, but there is no security or performance benefit in doing so.) Denote the input and output of the central map by $\mathbf{u} = U\mathbf{x}$ and $\mathbf{v} = T^{-1}(\mathbf{y})$.

The construction of the central map is as follows. Define three $s \times s$ matrices A, B, and C in the following way:

$$A = \begin{bmatrix} p_1 & p_2 & \cdots & p_s \\ p_{s+1} & p_{s+2} & \cdots & p_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ p_{s^2-s+1} & p_{s^2-s+2} & \cdots & p_{s^2} \end{bmatrix}, B = \begin{bmatrix} b_1 & b_2 & \cdots & b_s \\ b_{s+1} & b_{s+2} & \cdots & b_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ b_{s^2-s+1} & b_{s^2-s+2} & \cdots & b_{s^2} \end{bmatrix},$$

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 p_i are quadratic forms on $\mathbf{u}$ chosen independently and uniformly at random from among all quadratic forms and the b_i and c_i are linear forms on $\mathbf{u}$ chosen independently and uniformly at random from among all linear forms.

We define two $s \times s$ matrices $E_1 = AB$ and $E_2 = AC$. Since A is quadratic and B and C are linear in u_i, E_1 and E_2 are cubic in the u_i. The central map $\mathcal{E}$ is defined by

$$\mathcal{E} = \phi \circ (E_1 || E_2).$$

Thus $\mathcal{E}$ is an m dimensional vector of cubic forms in $\mathbf{u}$. Finally, the public key is given by $\mathcal{F} = T \circ \mathcal{E} \circ U$.

Encryption with this system is standard: given a plaintext $(x_1, \ldots, x_n)$, compute $(y_1, \ldots, y_m) = \mathcal{F}(x_1, \ldots, x_n)$. Decryption is somewhat more complicated.

To decrypt, one inverts each of the private maps in turn: apply T^{-1}, invert $\mathcal{E}$, and apply U^{-1}. To "invert" $\mathcal{E}$, one assumes that $A(\mathbf{u})$ is invertible, and forms a matrix

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

where the w_i are indeterminants. Then using the relations $A^{-1}(\mathbf{u})E_1(\mathbf{u}) = B(\mathbf{u})$ and $A^{-1}(\mathbf{u})E_2(\mathbf{u}) = C(\mathbf{u})$, we have $m = 2s^2$ linear equations in $2n = 2s^2$ unknowns w_i and u_i. 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 $E_1(\mathbf{u})$ and $E_2(\mathbf{u})$ to obtain a large system of equations in very few variables which can be solved efficiently in a variety of ways.

3 Subspace Differential Invariants for Cubic Maps

Let $f : k^n \to k^m$ be an arbitrary fixed function on k^n. Consider the discrete differential $Df(\mathbf{a}, \mathbf{x}) = f(\mathbf{a} + \mathbf{x}) - f(\mathbf{a}) - f(\mathbf{x}) + f(\mathbf{0})$.

If f is quadratic, we can express the differential as an n-tuple of bilinear differential coordinate forms in the following way: $[Df(\mathbf{a},\mathbf{x})]_i = \mathbf{a}^\top Df_i\mathbf{x}$, where Df_i is a symmetric matrix representation of the action on the ith coordinate of the bilinear differential. If the function f is cubic $Df(\mathbf{a},\mathbf{x})$ is a symmetric bi-quadratic function. By the symmetry, it is well defined to compute a second differential $D^2f(\mathbf{a},\mathbf{b},\mathbf{x})$ by computing the discrete differential of Df with respect to either $\mathbf{a}$ or $\mathbf{x}$. In this case, we may consider the second differential as an n-tuple of trilinear differential coordinate forms by letting D^2f_i be the symmetric 3-tensor representing the action on the ith coordinate of the trilinear differential.

In [13], the following definition of a subspace differential invariant was provided:

Definition 1 *A* subspace differential invariant *of a quadratic map $f : k^n \to k^m$ 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. $A \in Span_X(Df_i)$.*

This definition captures the idea of a subspace of the span of the public polynomials acting linearly on a subspace of the plaintext space in the same way. Such behavior is strange for quadratic maps in general. Furthermore, as shown in [13], this behavior is computable regardless of the rank of the maps involved.

A natural generalization of this definition is the following:

Definition 2 *A* subspace differential invariant *of a cubic map $f : k^n \to k^m$ with respect to a subspace $X \subseteq k^m$ is a pair of subspaces $(V_1, V_2) \subseteq (k^n)^2$ for which there exists a subspace $W \subseteq k^n$ with $dim(W) \leq mindim(V_i)$ such that for all $A = \sum_{i=1}^m x_i D^2 f_i$ where $(x_1,\ldots,x_m) \in X$, for all $\mathbf{a} \in V_2$, for all $\mathbf{b} \in V_2$ and for all $\mathbf{x} \in W^\perp$ we have that $A(\mathbf{a},\mathbf{b},\mathbf{x}) = 0$.*

This definition captures the notion of a subspace of the span of the public cubic polynomials acting quadratically on a subspace of the plaintext space in the same way. Such behavior is strange for cubic maps in general.

4 The Differential Invariant Structure of the Cubic ABC scheme

4.1 Column Band Spaces

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

$$\mathcal{E}_{(i-1)s+j} = \sum_{l=1}^{s} p_{(i-1)s+l} b_{(l-1)s+j}, \tag{1}$$

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

$$\mathcal{E}_{s^2+(i-1)s+j} = \sum_{l=1}^{s} p_{(i-1)s+l} c_{(l-1)s+j} \tag{2}$$

where i and j run from 1 to s.

Consider the s sets of s polynomials that form the columns of E_1, i.e. for each $j \in \{1, \ldots, s\}$ consider $(\mathcal{E}_j, \mathcal{E}_{s+j}, \ldots, \mathcal{E}_{s^2-s+j})$. With high probability, the linear forms $b_j, b_{s+j}, \ldots, b_{s^2-s+j}$ are linearly independent, and if so the polynomials may be re-expressed, using a linear change of variables to $(u'_1, \ldots u'_{s^2})$ where $u'_i = b_{(i-1)s+j}$ for $i = 1, \ldots, s$. After the change of variables, the only cubic monomials contained in $(\mathcal{E}_j, \mathcal{E}_{s+j}, \ldots, \mathcal{E}_{s^2-s+j})$ will be those containing at least one factor of $u'_1, \ldots, u'_s$. We can make a similar change of variables to reveal structure in the s sets of s polynomials that form the columns of E_2: Setting $u'_i = c_{(i-1)s+j}$ for $i = 1, \ldots, s$ and a fixed j, the only cubic monomials contained in $(\mathcal{E}_{s^2+j}, \mathcal{E}_{s^2+s+j}, \ldots, \mathcal{E}_{2s^2-s+j})$ will be those containing at least one factor of $u'_1, \ldots, u'_s$.

More generally, we can make a similar change of variables to reveal structure in any of a large family of s dimensional subspaces of the span of the component polynomials of E_1 and E_2, which we will call column band spaces in analogy to the band spaces used to analyze the quadratic ABC cryptosystem in [13]. Each family is defined by a fixed linear combination, (β, γ), of the columns of E_1 and E_2:

Definition 3 *The column band space defined by the* $2s$*-dimensional linear form* (β, γ) *is the space of cubic maps,* $\mathcal{B}_{\beta,\gamma}$ *, given by:*

$$\mathcal{B}_{\beta,\gamma} = \mathit{Span}(\mathcal{E}_{\beta,\gamma,1}, \ldots, \mathcal{E}_{\beta,\gamma,s})$$

where

$$\mathcal{E}_{\beta,\gamma,i} = \sum_{j=1}^{s} (\beta_j \mathcal{E}_{(i-1)s+j} + \gamma_j \mathcal{E}_{s^2+(i-1)s+j})$$

$$= \sum_{l=1}^{s} \left(p_{(i-1)s+l} \sum_{j=1}^{s} \left(\beta_j b_{(l-1)s+j} + \gamma_j c_{(l-1)s+j} \right) \right)$$

Theorem 1 *There is a pair of subspaces* $(V_1, V_2) \in (k^n)^2$ *which is a subspace differential invariant with respect to* $\mathcal{B}_{\beta,\gamma}$ *for all* (β, γ)*. Moreover, there exists an* $\mathbf{x}_1 \in k^n$ *such that* $rank(D^2\mathcal{E}(\mathbf{x}_1)) \leq 2s$ *for all* $\mathcal{E} \in \mathcal{B}_{\beta,\gamma}$*.*

Proof. Note that under a change of variables $(x_1, \ldots, x_{s^2}) \xmapsto{M} (u'_1, \ldots u'_{s^2})$, where $u'_i = \sum_{j=1}^{s} \left(\beta_j b_{(i-1)s+j} + \gamma_j c_{(i-1)s+j} \right)$ for $i = 1, \ldots, s$, the only cubic monomials contained in the elements of $\mathcal{B}_{\beta,\gamma}$ will be those containing at least one factor of $u'_1, \ldots, u'_s$. In such a basis, the second differential of any map in $\mathcal{B}_{\beta,\gamma}$, and thus the second differential of $\mathcal{E}$ can be visualized as a 3-tensor with a special block form, see Figure 1.

Let V be the $(s^2 - s)$-dimensional preimage $M^{-1}(\mathrm{Span}(u'_1, \ldots, u'_s)^\perp)$. This 3-tensor $D^2\mathcal{E}$ may be thought of as a bilnear map which takes two vectors $\mathbf{x}_1, \mathbf{x}_2 \in V$, i.e. of the form:

$$(0, \ldots, 0, u'_{s+1}(\mathbf{x}_k), \ldots, u'_{s^2}(\mathbf{x}_k))^\top$$

to a covector of the form:

$$(y(u'_1), \ldots, y(u'_s), 0, \ldots, 0).$$

Thus, in this basis $D^2\mathcal{E}(\mathbf{x}_1)$ is a symmetric matrix which is zero on $V \times V$. Therefore, $rank(D^2\mathcal{E}(\mathbf{x})) \leq 2s$. One checks that (V, V) is a subspace differential with respect to $\mathcal{B}_{\beta,\gamma}$ with $W := V^{\perp}$, since $dim(W) = s < s^2 - s = dim(V)$.

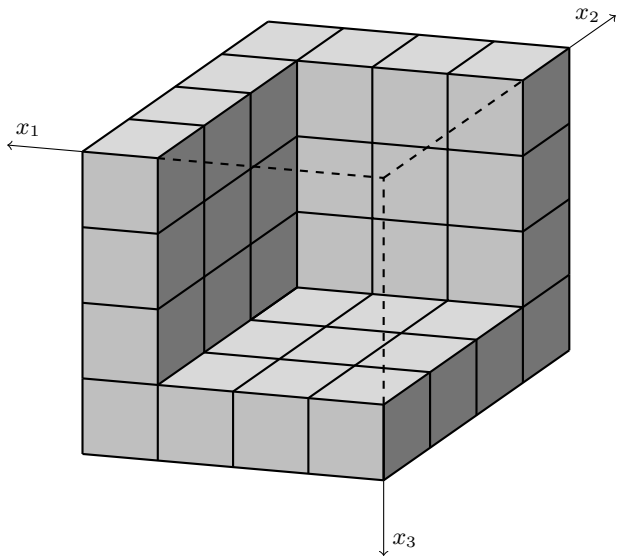

Fig. 1. 3-tensor structure of the second differential of a band space map. Solid regions correspond to nonzero coefficients. Transparent regions correspond to zero coefficients.

We will define the term "band-kernel" to describe the space of vectors of the same form as x_1 and x_2 in the proof above, i.e.:

Definition 4 *The band kernel of $\mathcal{B}_{\beta,\gamma}$, denoted $\mathcal{BK}_{\beta,\gamma}$, is the space of vectors, x, such that*

$$u'_i = \sum_{j=1}^{s} \left(\beta_j b_{(i-1)s+j}(x) + \gamma_j c_{(i-1)s+j}(x)\right) = 0$$

for $i = 1, \ldots, s$.

5 A Variant of MinRank Exploiting the Column Band Space Structure

A minrank-like attack may be used to locate the column band-space maps defined in the previous section. In this case, the attack proceeds by selecting s^2-dimensional vectors $\mathbf{x}_1$, $\mathbf{x}_2$, $\mathbf{x}_3$, and $\mathbf{x}_4$, setting

$$\begin{aligned}\sum_{i=1}^{2s^2} t_i D^2\mathcal{E}_i(\mathbf{x}_1, \mathbf{x}_2) = 0\\ \sum_{i=1}^{2s^2} t_i D^2\mathcal{E}_i(\mathbf{x}_3, \mathbf{x}_4) = 0,\end{aligned} \tag{3}$$

and solving for the t_i. The attack succeeds when $\sum_{i=1}^{2s^2} t_i\mathcal{E}_i \in \mathcal{B}_{\beta,\gamma}$ and $\mathbf{x}_1$, $\mathbf{x}_2$, $\mathbf{x}_3$, and $\mathbf{x}_4$ are all within the corresponding band kernel. If these conditions are met, then the rank of the 2-tensor $\sum_{i=1}^{2s^2} t_i D^2\mathcal{E}_i(\mathbf{x}_k)$ for $k = 1, 2, 3, 4$ will be at most $2s$, and this will be easily detectable.

The attack complexity will be significantly reduced if several of the $\mathbf{x}_k$ are set equal to one another. In odd characteristic fields, we can reduce the number of independently chosen vectors to 2, (for example, by setting $\mathbf{x}_1 = \mathbf{x}_2$ and $\mathbf{x}_3 = \mathbf{x}_4$.) In characteristic 2, however, the antisymmetry of the 2nd differential prevents the equation $\sum_{i=1}^{2s^2} t_i D^2\mathcal{E}_i(\mathbf{x}_1, \mathbf{x}_1) = 0$ from imposing a nontrivial constraint on the t_i. Even in characteristic 2, though, the number of independently chosen vectors can be reduced to 3 (e.g. by setting $\mathbf{x}_1 = \mathbf{x}_4$.)

Theorem 2 *The probability that 2 randomly chosen vectors, $\mathbf{x}_1$ and $\mathbf{x}_2$, are both in the band kernel of some band-space $\mathcal{B}_{\beta,\gamma}$ is approximately $\frac{1}{q-1}$; The probability that 3 randomly chosen vectors, $\mathbf{x}_1$, $\mathbf{x}_2$, and $\mathbf{x}_3$, are all in the band kernel of some band-space $\mathcal{B}_{\beta,\gamma}$ is approximately $\frac{1}{(q-1)q^s}$.*

Proof. The condition that the $\mathbf{x}_k$ are all contained within a band kernel is that there be a nontrivial linear combination of the columns of the following matrix equal to zero (i.e. that the matrix has nonzero column corank):

$$\left[\begin{array}{cccc|cccc} b_1(\mathbf{x}_1) & b_2(\mathbf{x}_1) & \dots & b_s(\mathbf{x}_1) & c_1(\mathbf{x}_1) & c_2(\mathbf{x}_1) & \dots & c_s(\mathbf{x}_1) \\ b_{s+1}(\mathbf{x}_1) & b_{s+2}(\mathbf{x}_1) & \dots & b_{2s}(\mathbf{x}_1) & c_{s+1}(\mathbf{x}_1) & c_{s+2}(\mathbf{x}_1) & \dots & c_{2s}(\mathbf{x}_1) \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{s^2-s+1}(\mathbf{x}_1) & b_{s^2-s+2}(\mathbf{x}_1) & \dots & b_{s^2}(\mathbf{x}_1) & c_{s^2-s+1}(\mathbf{x}_1) & c_{s^2-s+2}(\mathbf{x}_1) & \dots & c_{s^2}(\mathbf{x}_1) \\ \hline b_1(\mathbf{x}_2) & b_2(\mathbf{x}_2) & \dots & b_s(\mathbf{x}_2) & c_1(\mathbf{x}_2) & c_2(\mathbf{x}_2) & \dots & c_s(\mathbf{x}_2) \\ b_{s+1}(\mathbf{x}_2) & b_{s+2}(\mathbf{x}_2) & \dots & b_{2s}(\mathbf{x}_2) & c_{s+1}(\mathbf{x}_2) & c_{s+2}(\mathbf{x}_2) & \dots & c_{2s}(\mathbf{x}_2) \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{s^2-s+1}(\mathbf{x}_2) & b_{s^2-s+2}(\mathbf{x}_2) & \dots & b_{s^2}(\mathbf{x}_2) & c_{s^2-s+1}(\mathbf{x}_2) & c_{s^2-s+2}(\mathbf{x}_2) & \dots & c_{s^2}(\mathbf{x}_2) \\ \hline \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \end{array}\right] \tag{4}$$

In the case with 2 randomly chosen vectors, the matrix is a uniformly random $2s \times 2s$ matrix, which has nonzero column corank with probability approximately $\frac{1}{q-1}$. In the case with 3 randomly chosen vectors, the matrix is a uniformly random $3s \times 2s$ matrix, which has nonzero column corank with probability approximately $\frac{1}{(q-1)q^s}$.

Theorem 3 *If* $\mathbf{x}_1$, $\mathbf{x}_2$, $\mathbf{x}_3$, *and* $\mathbf{x}_4$ *are chosen in such a way that all four vectors are in the band kernel of a column band space* $\mathcal{B}_{\beta,\gamma}$ *and also that the symmetric tensor products* $\mathbf{x}_1 \odot \mathbf{x}_2$ *and* $\mathbf{x}_3 \odot \mathbf{x}_4$ *are linearly independent from one another and statistically independent from the private quadratic forms,* $p_{(i-1)s+j}$ *in the matrix* A*, then the tensor products* $\mathbf{x}_1 \otimes \mathbf{x}_2$ *and* $\mathbf{x}_3 \otimes \mathbf{x}_4$ *are both in the kernel of some column band-space differential* $D^2\mathcal{E} = \sum_{\mathcal{E}_{\beta,\gamma,i} \in \mathcal{B}_{\beta,\gamma}} \tau_i D^2\mathcal{E}_{\beta,\gamma,i}$ *with probability approximately* $\frac{1}{(q-1)q^s}$.

Proof. A $D\mathcal{E}$ meeting the above condition exists iff there is a nontrivial solution to the following system of equations

$$\begin{aligned} \sum_{\mathcal{E}_{\beta,\gamma,i} \in \mathcal{B}_{\beta,\gamma}} \tau_i D^2\mathcal{E}_{\beta,\gamma,i}(\mathbf{x}_1, \mathbf{x}_2) = 0, \\ \sum_{\mathcal{E}_{\beta,\gamma,i} \in \mathcal{B}_{\beta,\gamma}} \tau_i D^2\mathcal{E}_{\beta,\gamma,i}(\mathbf{x}_3, \mathbf{x}_4) = 0. \end{aligned} \tag{5}$$

Expressed in a basis (e.g. the u'_i basis used in Definition 4) 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 column band-space differentials, $D^2\mathcal{E}_{\beta,\gamma,i}$ are 3-tensors of the form shown in Figure 1.

Likewise $\mathbf{x}_1$, $\mathbf{x}_2$, $\mathbf{x}_3$, and $\mathbf{x}_4$ take the form $(0|\ \mathbf{x}_k\ )$. The 2-tensors $D^2\mathcal{E}_{\beta,\gamma,i}(\mathbf{x}_k)$ can then be represented by matrices of the form:

$$D^2\mathcal{E}_{\beta,\gamma,i}(\mathbf{x}_k) = \left[\begin{array}{c|c} S_{k,i} & R_{k,i} \\ \hline R_{k,i}^\top & 0 \end{array}\right] \tag{6}$$

where $R_{k,i}$ is a random $s \times s^2 - s$ matrix and $S_{k,i}$ is a random symmetric $s \times s$ matrix. Removing the redundant degrees of freedom we have the system of $2s$ equations in s variables:

$$\begin{aligned} \sum_{i=1}^{s} \tau_i R_{1,i} {\mathbf{x}_2}^\top = 0, \\ \sum_{i=1}^{s} \tau_i R_{3,i} {\mathbf{x}_4}^\top = 0. \end{aligned} \tag{7}$$

This has a nontrivial solution precisely when the following $2s \times s$ matrix has nonzero column corank:

$$M = \left[\begin{array}{c|c|c|c} | & | & & | \\ R_{1,1}{\mathbf{x}_2}^\top & R_{1,2}{\mathbf{x}_2}^\top & \dots & R_{1,s}{\mathbf{x}_2}^\top \\ | & | & & | \\ \hline | & | & & | \\ R_{3,1}{\mathbf{x}_4}^\top & R_{3,2}{\mathbf{x}_4}^\top & \dots & R_{3,s}{\mathbf{x}_4}^\top \\ | & | & & | \end{array}\right] \tag{8}$$

This is a random matrix over $k = \mathbb{F}_q$, which has nonzero column corank with probability approximately $\frac{1}{(q-1)q^s}$, for practical parameters.

To verify that the conditions given in the theorem are sufficient to establish the randomness of the matrix M, we can give the following explicit expression for the matrix M, which is most easily derived by applying the product rule for the discrete differential to Definition 3:

$$M = \left[\begin{array}{cccc} Dp_1(\mathbf{x}_1,\mathbf{x}_2) & Dp_{s+1}(\mathbf{x}_1,\mathbf{x}_2) & \cdots & Dp_{s^2-s+1}(\mathbf{x}_1,\mathbf{x}_2) \\ Dp_2(\mathbf{x}_1,\mathbf{x}_2) & Dp_{s+2}(\mathbf{x}_1,\mathbf{x}_2) & \cdots & Dp_{s^2-s+2}(\mathbf{x}_1,\mathbf{x}_2) \\ \vdots & \vdots & \ddots & \vdots \\ Dp_s(\mathbf{x}_1,\mathbf{x}_2) & Dp_{2s}(\mathbf{x}_1,\mathbf{x}_2) & \cdots & Dp_{s^2}(\mathbf{x}_1,\mathbf{x}_2). \\ \hline Dp_1(\mathbf{x}_3,\mathbf{x}_4) & Dp_{s+1}(\mathbf{x}_3,\mathbf{x}_4) & \cdots & Dp_{s^2-s+1}(\mathbf{x}_3,\mathbf{x}_4) \\ Dp_2(\mathbf{x}_3,\mathbf{x}_4) & Dp_{s+2}(\mathbf{x}_3,\mathbf{x}_4) & \cdots & Dp_{s^2-s+1}(\mathbf{x}_3,\mathbf{x}_4) \\ \vdots & \vdots & \ddots & \vdots \\ Dp_s(\mathbf{x}_3,\mathbf{x}_4) & Dp_{2s}(\mathbf{x}_3,\mathbf{x}_4) & \cdots & Dp_{s^2}(\mathbf{x}_3,\mathbf{x}_4) \end{array}\right] \tag{9}$$

Combining the results of Theorems 2 and 3, we find that for each choice of the vectors $\mathbf{x}_k$, there is a column band-space map among the solutions of Equation (3) with probability approximately $\frac{1}{(q-1)^2q^{2s}}$ for even characteristic and $\frac{1}{(q-1)^2q^s}$ for odd characteristic. Equation (3) is a system of $2s^2$ equations in $2s^2$ variables; one might expect it to generally have a 0-dimensional space of solutions. In some cases, however, there are linear dependencies among the equations, due to the fact that the $D^2\mathcal{E}_i$ are symmetric tensors. In even characteristic, we get 4 linear dependencies: $D^2\mathcal{E}_i(\mathbf{x}_1,\mathbf{x}_2)(\mathbf{x}_1) = 0$, $D^2\mathcal{E}_i(\mathbf{x}_1,\mathbf{x}_2)(\mathbf{x}_2) = 0$, $D^2\mathcal{E}_i(\mathbf{x}_3,\mathbf{x}_4)(\mathbf{x}_3) = 0$, and $D^2\mathcal{E}_i(\mathbf{x}_3,\mathbf{x}_4)(\mathbf{x}_4) = 0$, and an additional linear dependency when we reduce the number of independent vectors to 3 by setting $\mathbf{x}_1 = \mathbf{x}_4$: $D^2\mathcal{E}_i(\mathbf{x}_1,\mathbf{x}_2)(\mathbf{x}_3) + D^2\mathcal{E}_i(\mathbf{x}_3,\mathbf{x}_4)(\mathbf{x}_2) = 0$, resulting in a 5-dimensional space of solutions. In characteristic 3, reducing the number of independent vectors to 2 results in 2 linear dependencies among the equations: e.g. setting $\mathbf{x}_1 = \mathbf{x}_2$ and $\mathbf{x}_3 = \mathbf{x}_4$, we have $D^2\mathcal{E}_i(\mathbf{x}_1,\mathbf{x}_2)(\mathbf{x}_1) = 0$ and $D^2\mathcal{E}_i(\mathbf{x}_3,\mathbf{x}_4)(\mathbf{x}_3) = 0$. In higher characteristic, there are no linear dependencies imposed on the equations by setting $\mathbf{x}_1 = \mathbf{x}_2$ and $\mathbf{x}_3 = \mathbf{x}_4$.

For characteristic 2, finding the expected 1-dimensional space of band-space solutions in a 5-dimensional space costs $q^4 + q^3 + q^2 + q + 1$ rank operations, which in turn cost $(s^2)^\omega$ field operations, where $\omega \approx 2.373$ is the linear algebra constant. Likewise, for characteristic 3, finding the expected 1-dimensional space of band-space solutions in a 2-dimensional space costs $q+1$ rank operations. Thus the total cost of finding a column band-space map using our variant of MinRank is approximately $q^{2s+6}s^{2\omega}$ for charactersitic 2, $q^{s+3}s^{2\omega}$ for characteristic 3, and $q^{s+2}s^{2\omega}$ for higher characteristic.

6 Complexity of Invariant Attack

The detection of a low rank induced bilinear form $D^2\mathcal{E}(x)$ already constitutes a distinguisher from a random system of equations. Extending this calculation to

a full key recovery requires further use of the differential invariant structure of the public key.

First, note that U is not a critical element of the scheme. If A is a random matrix of quadratic forms and B and C are random matrices of linear forms, so are $A \circ U$, $B \circ U$ and $C \circ U$ for any full rank map U. Thus, since clearly $T \circ \phi(AB||AC) \circ U = T \circ \phi((A \circ U)(B \circ U)||(A \circ U)(C \circ U))$, we may absorb the action of U into A, B, and C, and consider the public key to be of the form:

$$P(\mathbf{x}) = T \circ \phi(AB||AC)(\mathbf{x}).$$

Next, consider a trilinear form $D^2\mathcal{E}$ in the band space generated by $\mathcal{B}_{\beta,\gamma}$. Since the coefficients of $D^2\mathcal{E}$ are products of coefficients of A and coefficients of an element of $Im(B||C)$, both of which are uniform i.i.d., there is a change of basis M in which $D^2\mathcal{E}$ has the form in Figure 1 and the nonzero coefficients are uniform i.i.d.

Consider $D^2\mathcal{E}(\mathbf{x}_1)$ and $D^2\mathcal{E}(\mathbf{x}_2)$ for $\mathbf{x}_1, \mathbf{x}_2$ in the band kernel corresponding to $\mathcal{B}_{\beta,\gamma}$. Being maps from the same band space, there is a basis in which both $D^2\mathcal{E}(\mathbf{x}_1)$ and $D^2\mathcal{E}(\mathbf{x}_2)$ have the form in Figure 2. Thus, with high probability for $s \geq 2$, the kernels of both maps are contained in the corresponding band kernel, $\mathcal{B}_{\beta,\gamma}$, and $\text{span}(\ker(D^2\mathcal{E}(\mathbf{x}_1) \cup \ker(D^2\mathcal{E}(\mathbf{x}_2)) = \mathcal{B}_{\beta,\gamma}$.

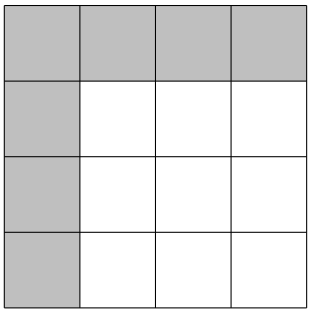

Fig. 2. Structure of the bilinear forms induced by cubic maps in the same band space.

Remark 1 *Here we have utilized a property which explicitly distinguishes differential invariant structure from rank structure.*

Given the basis for an $s^2 - s$ dimensional band kernel $\mathcal{BK}$, we may choose a basis $\{v_1, \ldots, v_s\}$ for the subspace of the dual space vanishing on $\mathcal{BK}$. We can

also find a basis $\mathcal{E}_{v_1}, \ldots, \mathcal{E}_{v_s}$ for the band space itself by solving the linear system

$$\begin{aligned}
\sum_{\mathcal{E}_i} \tau_i D^2 \mathcal{E}_i(\mathbf{x}_{11}, \mathbf{x}_{12}, \mathbf{x}_{13}) &= 0, \\
\sum_{\mathcal{E}_i} \tau_i D^2 \mathcal{E}_i(\mathbf{x}_{21}, \mathbf{x}_{22}, \mathbf{x}_{23}) &= 0, \\
&\vdots = \vdots \\
\sum_{\mathcal{E}_i} \tau_i D^2 \mathcal{E}_i(\mathbf{x}_{t1}, \mathbf{x}_{t2}, \mathbf{x}_{t3}) &= 0,
\end{aligned}$$

where $t \approx 2s^2$ and $\mathbf{x}_{ij}$ is in the band kernel.

Since the basis $\mathcal{E}_{v_1}, \ldots, \mathcal{E}_{v_s}$ is in a single band space, there exists an element $\begin{bmatrix} b'_1 & \cdots & b'_s \end{bmatrix}^\top \in ColSpace(B||C)$ and two matrices Ω_1 and Ω_2 such that

$$\Omega_1 A \left(\Omega_2 \begin{bmatrix} b'_1 \\ \vdots \\ b'_s \end{bmatrix} \right) =: A' \left(\begin{bmatrix} v_1 \\ \vdots \\ v_s \end{bmatrix} \right) = \begin{bmatrix} \mathcal{E}_{v_1} \\ \vdots \\ \mathcal{E}_{v_s} \end{bmatrix}.$$

Solving the above system of equations over $\mathbb{F}_q[x_1, \ldots, x_{s^2}]$ uniquely determines A' in $\mathbb{F}_q[x_1, \ldots, x_{s^2}]/\langle v_1, \ldots, v_s \rangle$. To recover all of A', note that the above system is part of an equivalent key

$$\mathcal{F} = T' \circ A'(B'||C')$$

where $\begin{bmatrix} v_1 & \cdots & v_s \end{bmatrix}^\top$ is the first column of B'.

Applying T'^{-1} to both sides and inserting the information we know we may construct the system

$$A'(B'||C') = T'^{-1}\mathcal{F} \tag{10}$$

Solving this system of equations modulo $\langle v_1, \ldots, v_s \rangle$ for B', C' and T'^{-1} we can recover a space of solutions, which we will restrict by arbitrarily fixing the value of T'^{-1}. Note that the elements of T'^{-1} are constant polynomials, and therefore $T'^{-1} (\mathrm{mod}\, \langle v_1, \ldots, v_s \rangle)$ is the same as T'^{-1}. Thus, for any choice of T'^{-1} in this space, the second column of $T'^{-1}\mathcal{F}$ is a basis for a band space. Moreover, the elements $v'_{s+1}, \ldots, v'_{2s}$ of the second column of $B' (\mathrm{mod}\, \langle v_1, \ldots, v_s \rangle)$ are the image, modulo $\langle v_1, \ldots, v_s \rangle$, of linear forms vanishing on the corresponding band kernel. Therefore, the intersection $\bigcap_{i=1}^{s} \ker(v_i) \cap \bigcap_{i=s+1}^{2s} \ker(v'_i)$ is the intersection $\mathcal{BK}_2 \cap \mathcal{BK}_1$ of the band kernels of our two band spaces.

We can reconstruct the full band kernel of this second band space using the same method we used to obtain our first band kernel: We take a map $\mathcal{E}_2$ from the second column of $T'^{-1}\mathcal{F}$, and two vectors x_a and x_b from $\mathcal{BK}_2 \cap \mathcal{BK}_1$, and we compute $\mathcal{BK}_2 = \mathrm{span}(\ker(D^2\mathcal{E}_2(\mathbf{x}_a) \cup \ker(D^2\mathcal{E}_2(\mathbf{x}_b))$. We can now solve for the second column of B', $\begin{bmatrix} v_{s+1} & \cdots & v_{2s} \end{bmatrix}^\top$, uniquely over $\mathbb{F}_q[x_1, \ldots, x_{s^2}]$ (NOT modulo $\langle v_1, \ldots, v_s \rangle$) by solving the following system of linear equations:

$$\begin{aligned} v_i \equiv v_i' (\mathrm{mod}\, \langle v_1, \ldots, v_s \rangle) \\ v_i(\mathbf{x}_1) = 0 \\ v_i(\mathbf{x}_2) = 0 \\ \vdots = \vdots \\ v_i(\mathbf{x}_{s^2-s}) = 0 \end{aligned}$$

where $i = s+1, \ldots, 2s$, and $(\mathbf{x}_1, \ldots, \mathbf{x}_{s^2-s})$ is a basis for $\mathcal{BK}_2$. We can now solve for A' (again, uniquely over $\mathbb{F}_q[x_1, \ldots, x_{s^2}]$) by solving:

$$A' \left(\begin{bmatrix} v_1 \\ \vdots \\ v_s \end{bmatrix} \right) \equiv \begin{bmatrix} \mathcal{E}_{v_1} \\ \vdots \\ \mathcal{E}_{v_s} \end{bmatrix} (\mathrm{mod}\, \langle v_1, \ldots, v_s \rangle)$$

$$A' \left(\begin{bmatrix} v_{s+1} \\ \vdots \\ v_{2s} \end{bmatrix} \right) \equiv \begin{bmatrix} \mathcal{E}_{v_{s+1}} \\ \vdots \\ \mathcal{E}_{v_{2s}} \end{bmatrix} (\mathrm{mod}\, \langle v_{s+1}, \ldots, v_{2s} \rangle)$$

where $\begin{bmatrix} \mathcal{E}_{v_{s+1}} & \cdots & \mathcal{E}_{v_{2s}} \end{bmatrix}^\top$ is the second column of $T'^{-1}\mathcal{F}$. This allows us to solve equation 10 for the rest of B' and C', completing the attack.

The primary cost of the attack involves finding the band space map. The rest of the key recovery is additive in complexity and dominated by the band space map recovery; thus, the total complexity of the attack is of the same order as band space map recovery. Hence, the cost of private key extraction is approximately $q^{2s+6}s^{2\omega}$ for characteristic 2, $q^{s+3}s^{2\omega}$ for characteristic 3, and $q^{s+2}s^{2\omega}$ for higher characteristic. We note that with these parameters we can break full sized instances of this scheme with parameters chosen for the 80-bit and 100-bit security levels via the criteria presented in [14].

Specifically, our attack breaks CubicABC($q = 127$,$s = 7$), designed for 80-bit security, in approximately 2^{76} operations (or around 2^{80} if one pessimistically uses $\omega = 3$ as the linear algebra constant). More convincingly, our attack completely breaks CubicABC($q = 127$,$s = 8$), designed for 100-bit security, in approximately 2^{84} operations (or 2^{88} for $\omega = 3$). Furthermore, the attack is fully parallelizable and requires very little memory; hence, the differential invariant attack is far more efficient than algebraic attacks, the basis for the original security estimation. Thus, the security claims in [14] are clearly unfounded; in fact, the cubic version of the scheme, whose security was claimed to be closely related to an NP-complete problem, is actually less secure than the quadratic case.

We can explain this dramatic discrepancy on the fact that the parameters in [14] are derived by assuming that the algebraic attack is the most effective. In the case of the quadratic ABC scheme, for the proposed parameters, the attack of [13] was slower than the algebraic attack, though asymptotically faster. In the

case of the Cubic scheme, the attack is actually more efficient, in asymptotics as well as for practical parameters.

7 Experiments

Using SAGE [15], we performed some minrank computations on small scale variants of the Cubic ABC scheme. The computations were done on a computer with a 64 bit quad-core Intel i7 processor, with clock cycle 2.8 GHz. We were interested in verifying our complexity estimates on the most costly step in the attack, the MinRank instance, rather than the full attack on the ABC scheme. Given as input the finite field size q, and the scheme parameter s, we computed the average number of vectors v required to be sampled in order for the rank of the 2-tensor $D^2\mathcal{E}(v)$ to fall to $2s$. As explained in Section 5, when the rank falls to this level, we have identified the subspace differential invariant structure of the scheme and can exploit this structure to attack the scheme. Our results for odd q are given in Table 1.

	$s=3$	$(q-1)^2q^s$	$s=4$	$(q-1)^2q^s$	$s=5$	$(q-1)^2q^s$
$q=3$	14.75	108	333	324	952	972
$q=5$	378	2000	9986	10000		
$q=7$	1688	12348	72951	86436		
$q=9$	606	46656				
$q=11$	13574	133100				

Table 1. Average number of vectors needed for the rank to fall to $2s$ (for odd q)

For higher values of q and s the computations took too long to produce sufficiently many data points and obtain meaningful results with SAGE. When q is odd, our analysis predicted the number of vectors needed would be on the order of $(q-1)^2q^s$. Table 1 shows the comparison between our experiments and the expected value. We see that for $s=3$, the rank fell quicker than expected, while for $s>3$ the results are quite near the predicted value. This is because when $s=3$ our complexity estimates given in Section 5 are simply not accurate enough, which happens for small values of q and/or s.

For even q, we also ran some experiments. We found that for $s=3$ and $q=2,4$, or 8, with high probability only a single vector was needed before the rank fell to $2s$. For $s=4$ and $s=5$, the computations were only feasible in SAGE for $q=2$. The average number of vectors needed in the $s=4$ case was 244, with the expected value being $(q-1)^2q^{2s}=256$. With $s=5$, the average number in our experiments was 994 (although the number of trials was small), with the expected value 1024. For higher values of q and s the computations took too long to obtain meaningful results.

8 Conclusion

The ABC schemes are very interesting new ideas for multivariate public key schemes. Essentially all of MPKC can be bisected into big field schemes, utilizing the structure of an extension of the field used for public calculations, and small field schemes which require no such extension. (For the purpose of this comment we consider "medium" field schemes to be big field schemes.)

The ABC cryptosystems present a fundamentally new structure for the development of schemes. In fact, if we consider the structure of simple algebras over the public field (which are surely the only such structures we should consider for secure constructions) then "big field" and "big matrix algebra" complete the picture of possible large structure schemes.

It is interesting to note that the authors provide in [14] a heuristic security argument for the scheme and, as reinforced in the first presentation of the scheme at [16], suggest that with some work the scheme may be able to be shown provably secure. The idea behind their argument is at least somewhat reasonable, if not precise. Their argument essentially amounts to the following: every cubic polynomial in the public key is in the ideal generated by the quadratic forms in A under a certain basis; thus, one might expect the public key to contain a subset of the information one would obtain by applying one step of a Gröbner basis algorithm such as F4, see [17].

Unfortunately, this analysis is not very tight. In fact, we exploit the subspace differential invariant structure inherent to the ABC methodology to show that for odd characteristic the cubic scheme is less secure than its quadratic counterpart. We may therefore conclude that any attempt at a secure cubic "big matrix algebra" scheme must rely on the application of modifiers. The challenge, then, is to construct such a scheme which is still essentially injective for the purpose of encryption. Schemes such as this one can never compete with the secure multivariate options for digital signatures we already know.

We are thus left with the same lingering question that has been asked for the last two decades: Is secure multivariate encryption possible? Currently there is a small list of candidates none of which has both been extensively reviewed and has existed for longer than a few years. If we are to discover a secure multivariate encryption scheme with a convincing security proof or some other security metric, it will require some new techniques and new science. Only time will tell.

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, L., Jordan, S., Liu, Y., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D.: Report on post-quantum cryptography. NISTIR 8105 (2016) http://dx.doi.org/10.6028/NIST.IR.8105.
3. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. EUROCRYPT 1999. LNCS **1592** (1999) 206–222

4. Patarin, J., Goubin, L., Courtois, N.: C $^{*}_{-+}$ and HM: Variations around two schemes of T.Matsumoto and H.Imai. Asiacrypt 1998, Springer **1514** (1998) 35–49
5. Patarin, J., Courtois, N., Goubin, L.: Quartz, 128-bit long digital signatures. In Naccache, D., ed.: CT-RSA. Volume 2020 of Lecture Notes in Computer Science., Springer (2001) 282–297
6. 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. Volume 6498 of Lecture Notes in Computer Science., Springer (2010) 33–48
7. Petzoldt, A., Chen, M., Yang, B., Tao, C., Ding, J.: Design principles for hfev-based multivariate signature schemes. In Iwata, T., Cheon, J.H., eds.: Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part I. Volume 9452 of Lecture Notes in Computer Science., Springer (2015) 311–334
8. Ding, J., Yang, B.Y.: Degree of regularity for hfev and hfev-. [18] 52–66
9. Goubin, L., Courtois, N.: Cryptanalysis of the ttm cryptosystem. In Okamoto, T., ed.: ASIACRYPT. Volume 1976 of Lecture Notes in Computer Science., Springer (2000) 44–57
10. Tsujii, S., Gotaishi, M., Tadaki, K., Fujita, R.: Proposal of a signature scheme based on sts trapdoor. In Sendrier, N., ed.: PQCrypto. Volume 6061 of Lecture Notes in Computer Science., Springer (2010) 201–217
11. Porras, J., Baena, J., Ding, J.: Zhfe, a new multivariate public key encryption scheme. [16] 229–245
12. Tao, C., Diene, A., Tang, S., Ding, J.: Simple matrix scheme for encryption. [18] 231–242
13. Moody, D., Perlner, R.A., Smith-Tone, D.: An asymptotically optimal structural attack on the ABC multivariate encryption scheme. [16] 180–196
14. Ding, J., Petzoldt, A., Wang, L.: The cubic simple matrix encryption scheme. [16] 76–87
15. Developers, T.S.: SageMath, the Sage Mathematics Software System (Version 7.3). (2016) `http://www.sagemath.org`.
16. Mosca, M., ed.: Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings. Volume 8772 of Lecture Notes in Computer Science., Springer (2014)
17. Faugere, J.C.: A new efficient algorithm for computing grobner bases (f4). Journal of Pure and Applied Algebra **139** (1999) 61–88
18. Gaborit, P., ed.: Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013. Proceedings. In Gaborit, P., ed.: PQCrypto. Volume 7932 of Lecture Notes in Computer Science., Springer (2013)