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:

Moody, Dustin; Perlner, Ray; Smith-Tone, Daniel.
"Key Recovery Attack on Cubic Simple Matrix Encryption."
Paper presented at Selected Areas in Cryptography (SAC 2016), St. Johns, Newfoundland, Canada. August 10, 2016 - August 12, 2016.

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

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

Moody, Dustin; Perlner, Ray; Smith-Tone, Daniel.
"Key Recovery Attack on Cubic Simple Matrix Encryption."
Paper presented at Selected Areas in Cryptography (SAC 2016), St. Johns, Newfoundland, Canada. August 10, 2016 - August 12, 2016.

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.

Moody, Dustin; Perlner, Ray; Smith-Tone, Daniel.
"Key Recovery Attack on Cubic Simple Matrix Encryption."
Paper presented at Selected Areas in Cryptography (SAC 2016), St. Johns, Newfoundland, Canada. August 10, 2016 - August 12, 2016.

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

Moody, Dustin; Perlner, Ray; Smith-Tone, Daniel.
"Key Recovery Attack on Cubic Simple Matrix Encryption."
Paper presented at Selected Areas in Cryptography (SAC 2016), St. Johns, Newfoundland, Canada. August 10, 2016 - August 12, 2016.

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)

Moody, Dustin; Perlner, Ray; Smith-Tone, Daniel.
"Key Recovery Attack on Cubic Simple Matrix Encryption."
Paper presented at Selected Areas in Cryptography (SAC 2016), St. Johns, Newfoundland, Canada. August 10, 2016 - August 12, 2016.