A Polynomial-Time Key-Recovery Attack on MQQ Cryptosystems

Jean-Charles Faugère[1,2,3] and Danilo Gligoroski[4] and Ludovic Perret[2,1,3] and
Simona Samardjiska[4,5] and Enrico Thomae[6]

INRIA, Paris-Rocquencourt Center[1],
Sorbonne Universités, UPMC Univ Paris 06, Équipe PolSys, LIP6, F-75005, Paris,[2]
CNRS, UMR 7606, LIP6, F-75005, Paris, France[3],
Department of Telematics, NTNU, Trondheim, Norway[4],
FCSE, UKIM, Skopje, Macedonia[5],
Operational Services, Germany[6].
jean-charles.faugere@inria.fr,danilog@item.ntno.no,ludovic.perret@lip6.fr,
simonas@item.ntno.no,Enrico.Thomae@rub.de

Abstract. We investigate the security of the family of MQQ public key cryptosystems using multivariate quadratic quasigroups (MQQ). These cryptosystems show especially good performance properties. In particular, the MQQ-SIG signature scheme is the fastest scheme in the ECRYPT benchmarking of cryptographic systems (eBACS). We show that both the signature scheme MQQ-SIG and the encryption scheme MQQ-ENC, although using different types of MQQs, share a common algebraic structure that introduces a weakness in both schemes. We use this weakness to mount a successful polynomial time key-recovery attack that finds an equivalent key using the idea of so-called *good keys*. In the process we need to solve a MinRank problem that, because of the structure, can be solved in polynomial-time assuming some mild algebraic assumptions. We highlight that our theoretical results work in characteristic 2 which is known to be the most difficult case to address in theory for MinRank attacks and also without any restriction on the number of polynomials removed from the public-key. This was not the case for previous MinRank like-attacks against $\mathcal{MQ}$ schemes. From a practical point of view, we are able to break an MQQ-SIG instance of 80 bits security in less than 2 days, and one of the more conservative MQQ-ENC instances of 128 bits security in little bit over 9 days. Altogether, our attack shows that it is very hard to design a secure public key scheme based on an easily invertible MQQ structure.

Keywords. MQ cryptography, MQQ cryptosystems, Equivalent keys, Good keys, MinRank, Gröbner bases

1 Introduction

Multivariate quadratic ($\mathcal{MQ}$) public key schemes are cryptosystems based (in part) on the NP-hard problem of solving polynomial systems of quadra-tic equations over finite fields, also known as the $\mathcal{MQ}$-problem. Until the mid 2000's,

$\mathcal{MQ}$ cryptography was developing very rapidly, producing many interesting and versatile design ideas such as C* [24], HFE [33], SFLASH [12], UOV [26], TTM [29], TTS [42]. However, many of them were soon successfully cryptanalysed, and the biggest surprise was probably the break of SFLASH in 2007 [15], shortly after it was chosen by the NESSIE European Consortium [31] as one of the three recommended public key signature schemes. As a consequence, the confidence in $\mathcal{MQ}$ cryptosystems declined, and so did the research in this area as well.

Now, several years later, it seems that there have emerged new important reasons for renewal of the interest in a new generation of $\mathcal{MQ}$ schemes. In the past two years, the algorithms for solving the Discrete Logarithm (DL) problem underwent an extraordinary development (for instance, but not limited to [1]). This clearly illustrates the risk to not consider alternatives to classical assumptions based on number theory. In parallel, two of the most important standardization bodies in the world, NIST and ETSI have recently started initiatives for developing cryptographic standards not based on number theory, with a particular focus on primitives resistant to quantum algorithms [32,16].

A common characteristic of all $\mathcal{MQ}$ schemes is the construction of the public key as $\mathcal{P} = T \circ \mathcal{F} \circ S$ where $\mathcal{F}$ is some easily invertible quadratic mapping, masked by two bijective affine transformations S and T. A consequence of these construction is that some specific properties of the secret-key can be recovered on the public-key. In particular, one of the most important characteristic of $\mathcal{MQ}$ schemes that allows a successful key-recovery is connected to unexpected high rank defect on the matrices associated to the public-key. The attacks on TTM [11], STS [38,37], Rainbow [7,14], HFE and MultiHFE [27,25,5,6] are all in essence based on the problem of finding a low rank linear combination of matrices, known as MinRank in cryptography [10]. This problem is NP-hard [10] and was used to design a zero-knowledge authentication scheme [13]. Although NP-hard, the instances of MinRank arising from $\mathcal{MQ}$ schemes are often easy, thus providing a powerful tool for finding equivalent keys in canonical form.

1.1 Our Contribution

In this paper, we are concerned with the security analysis of a particular family of $\mathcal{MQ}$ (Multivariate Quadratic) cryptosystems, namely the MQQ schemes proposed in 2008 [21]. In these schemes the secret map $\mathcal{F}$ is derived from multivariate quadratic quasigroups (MQQ), which makes the inversion of $\mathcal{F}$ especially efficient. A message-recovery attack was proposed in [30], and later in [19], it was proven that a direct attack [30] can be done in polynomial-time. In [22], the authors proposed a signature scheme, called MQQ-SIG, based on the same idea and secure against direct attacks, as well as claimed to be CMA secure. They made heavy use of the minus modifier, known from HFE-[33], to repair MQQ. Finally, in [23] the authors proposed an enhanced variant of the MQQ encryption scheme, called MQQ-ENC. The MQQ-SIG signature scheme is the fastest scheme in signing in the ECRYPT Benchmarking of Cryptographic Systems (eBACS) SUPERCOP [4], and is therefore very appealing for practical use.

We show in this paper that this family of designs has a fundamental weakness which allows us to mount an efficient key-recovery attack on all known constructions based on MQQ. More precisely, we can recover a key, equivalent to the secret-key, by solving simultaneous instances of MinRank (Theorem 3) problems, which due to the structure of the schemes can be solved in polynomial-time. To do so, we first assume that the field is not too big. That is to say, we assume that $q = \mathcal{O}(n)$ which is indeed the case for most of the parameters proposed so far for MQQ cryptosystems. Of independent interest, we show that the simultaneous MinRank problem is equivalent to a rectangular MinRank (Corollary 1) problem. For the complexity of our attack, we summarize the first result below:

Theorem 1. *Let $\omega, 2 \leqslant \omega < 3$ be the linear algebra constant. Let $\mathcal{P} = T \circ \mathcal{F} \circ S$ be the public mapping of* MQQ-SIG *or* MQQ-ENC *consisting of $n - r$ polynomials in n variables over $\mathbb{F}_q$ (with* $\mathrm{Char}(\mathbb{F}_q) = 2$*). $\mathcal{F}$ is a set of quadratic polynomials derived from multivariate quadratic quasigroups* (MQQ)*, while S and T are invertible matrices used to mask the structure of $\mathcal{F}$. Then, the last columns of S and T (up to equivalence) can be recovered in $\mathcal{O}(n^{\omega})$. More generally, a key equivalent to the secret-key in* MQQ-SIG *or* MQQ-ENC *can be found by solving $n - r$* MinRank *instances with $N - r$ matrices from $\mathbb{F}_q^{N\times(N-r)}$ where $N, r + 2 \leqslant N \leqslant n - 1$. If $q = \mathcal{O}(n)$ then each* MinRank *can be solved in polynomial-time assuming a mild regularity condition on the public matrices. Under this condition and assuming $q = \mathcal{O}(n)$, we can recover a key equivalent to the secret-key in*

$$\mathcal{O}(n^{\omega+3}), \textit{with probability } 1 - 1/q.$$

The genericity assumption required in the previous result is that the rank defect in the skew-symmetric matrices derived from the public polynomials is a not too big constant. We have implemented our attack in practice and verified that this assumption is reasonable. We highlight that our theoretical results work in characteristic 2 which is known to be the most difficult case to address in theory [25,5,6] for MinRank attacks. Also, we emphasize that our attack works without any restriction on the number of polynomials removed from the public-key (the minus modifier). This was not the case for previous MinRank like-attacks against $\mathcal{MQ}$ schemes.
If we relax the condition on the size of q, we can still bound the complexity (although, we require a slightly stronger assumption).

Theorem 2 (informal version of Theorem 5). *Let $\omega, 2 \leqslant \omega < 3$ be the linear algebra constant. Let $\mathcal{P} = T \circ \mathcal{F} \circ S$ be the public mapping of* MQQ-SIG *or* MQQ-ENC *consisting of $n - r$ polynomials in n variables over $\mathbb{F}_q$ (with* $\mathrm{Char}(\mathbb{F}_q) = 2$*). Assuming that the kernels of the skew-symmetric matrices derived from the public-key behave as random subspaces and a genericity condition on the MinRank modeling, then we can recover a key, equivalent to the secret-key, in*

$$\mathcal{O}\left(n^{3\,\omega+1}\right), \textit{with probability } \left(1 - \tfrac{1}{q}\right)\left(1 - \tfrac{1}{q^{n-3}}\right). \qquad (1)$$

The assumption used in Theorem 2 means that we can restrict our attention to a sub-system of our modeling of the simultaneous MinRank (Theorem 3) such that the sub-system is bi-linear with a block of variables of constant size. If the sub-system behaves as a generic affine bi-linear system, this implies that the maximum degree reached during a Gröbner basis computation is constant [17]. This is what we observed in practice.
Indeed, in order to verify our assumptions and the correctness of the attack, we implemented the attack in Magma (Ver. 2.19-10 [8]). The results obtained confirm the computed theoretical complexity. Using the implementation, we demonstrated that our attack is very efficient by practically breaking instances with recommended parameters. For example, we recovered an equivalent key for MQQ-SIG 160, of claimed security of $\mathcal{O}(2^{80})$, in 2^{48} operations, *i.e.* in less than 2 days. Similarly, for MQQ-ENC 128 defined over $\mathbb{F}_4$ with claimed security of $\mathcal{O}(2^{128})$, we recovered an equivalent key in $2^{50.6}$ operations which took a little bit over 9 days. We also emphasize that the practical results obtained, almost perfectly match the theoretical complexity bound (1) derived in Section 7.1.
Altogether, our attack shows that it is very hard to design a secure scheme based on an easily invertible MQQ structure. It seems that using MQQs successfully in future $\mathcal{MQ}$ designs may require deep insight from quasigroup theory, in order to obtain the necessary security while preserving the attractive performance level.

1.2 Organization of the Paper

The paper is organized as follows. In Sect. 2 we present the necessary preliminaries about $\mathcal{MQ}$ cryptosystems. We also recall the MinRank problem and the known tools for solving it, as well as the concepts of equivalent keys and good keys. In Sect. 3 we describe the cryptosystems from the MQQ family, and in Sect. 4 we uncover the algebraic structure that the two systems, MQQ-SIG and MQQ-ENC share, and that shows the weaknesses of the cryptosystems. Sect. 5 is devoted to the presentation of the main idea behind our key recovery attack on both MQQ-ENC and MQQ-SIG. We further point out the difference in the attack in odd and even characteristic fields, and present the necessary modifications of the attack for even characteristic fields. As a result of the analysis, in Sect. 6 we conclude that the problem of finding good keys can be modeled as a special instance of MinRank for rectangular matrices. The complexity analysis of our attack is given in Sect. 7. We conclude the paper in Sect. 8.

2 Preliminaries

2.1 Basic Notations

Throughout this paper, $\mathbb{F}_q$ will denote the finite field of q elements, $\mathcal{M}_{n\times m}(\mathbb{F}_q)$ will denote the set of $n\times m$ matrices over $\mathbb{F}_q$ and $\mathrm{GL}_n(\mathbb{F}_q)$ will denote the general linear group of degree n over $\mathbb{F}_q$. First, we briefly recall the general principle of $\mathcal{MQ}$ public key cryptosystems. This will allow to fix some notations. The public key of an $\mathcal{MQ}$ cryptosystem is usually given by a multivariate quadratic map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, that is

$$\mathcal{P}(x_1,\ldots,x_n) := \begin{pmatrix} p_1(x_1,\ldots,x_n) = \sum\limits_{1 \leqslant i \leqslant j \leq n} \widetilde{\gamma}_{i,j}^{(1)} x_i x_j + \sum\limits_{i=1}^{n} \widetilde{\beta}_i^{(1)} x_i + \widetilde{\alpha}^{(1)} \\ \vdots \\ p_m(x_1,\ldots,x_n) = \sum\limits_{1 \leqslant i \leqslant j \leqslant n} \widetilde{\gamma}_{i,j}^{(m)} x_i x_j + \sum\limits_{i=1}^{n} \widetilde{\beta}_i^{(m)} x_i + \widetilde{\alpha}^{(m)} \end{pmatrix}$$

for some coefficients $\widetilde{\gamma}_{i,j}^{(s)}, \widetilde{\beta}_i^{(s)}$, and $\widetilde{\alpha}^{(s)} \in \mathbb{F}_q$.
In our attack, we will see that w.l.o.g. we can restrict our attention to the homogeneous components of highest degree, i.e. to the quadratic components. Classically, a quadratic form can be written as $p_s(x_1,\ldots,x_n) := \sum\limits_{1 \leq i \leq j \leq n} \widetilde{\gamma}_{i,j}^{(s)} x_i x_j = x^\intercal \mathfrak{P}^{(s)} x$, where $x := (x_1,\ldots,x_n)^\intercal$ and $\mathfrak{P}^{(s)}$ is an $n \times n$ matrix describing the degree-2 homogeneous component of p_s. The public key $\mathcal{P}$ is obtained by obfuscating a structured central map $\mathcal{F} : x \in \mathbb{F}_q^n \to \big(f_1(x),\ldots,f_m(x)\big) \in \mathbb{F}_q^m$. We denote by $\mathfrak{F}^{(s)}$ an $n \times n$ matrix describing the homogeneous quadratic part of f_s. In order to hide the structured central map, we choose two secret linear [1] transformations $S \in \mathrm{GL}_n(\mathbb{F}_q)$, $T \in \mathrm{GL}_m(\mathbb{F}_q)$ and define the public key as $\mathcal{P} := T \circ \mathcal{F} \circ S$.

Remark 1. It is known that the matrix of a quadratic form is constructed differently depending on the parity of the field characteristic. In odd characteristic, $\mathfrak{P}^{(s)}$ is a symmetric matrix, *i.e.* $\mathfrak{P}_{i,j}^{(s)} := \widetilde{\gamma}_{i,j}^{(s)}/2$ for $i \neq j$ and $\mathfrak{P}_{i,i}^{(s)} := \widetilde{\gamma}_{i,i}^{(s)}$. Over fields $\mathbb{F}_q$ of characteristic 2, we cannot choose $\mathfrak{P}^{(s)}$ in this manner, since $(\widetilde{\gamma}_{i,j} + \widetilde{\gamma}_{j,i}) x_i x_j = 2\widetilde{\gamma}_{i,j} x_i x_j = 0$ for $i \neq j$. Instead, let $\widetilde{\mathfrak{P}}^{(s)}$ be the upper-triangular representation of p_s, *i.e.* $\widetilde{\mathfrak{P}}_{i,j}^{(s)} = \widetilde{\gamma}_{i,j}^{(s)}$ for $i \leq j$. The symmetric form is obtained by $\mathfrak{P}^{(s)} := \widetilde{\mathfrak{P}}^{(s)} + \widetilde{\mathfrak{P}}^{(s)\intercal}$. In this case only the upper-triangular part represents the according polynomial, and all elements on the diagonal are zero. This implies that for $x, y \in \mathbb{F}_q^n$ the symmetric bilinear form $x^\intercal \mathfrak{P}^{(s)} y$ is alternating and has even rank.

2.2 The MinRank Problem

The problem of finding a low rank linear combination of matrices is a basic linear algebra problem [10] known as MinRank in cryptography [13]. The MinRank problem over a finite field $\mathbb{F}_q$ is as follows.
MinRank (MR)
Input: $n, m, r, k \in \mathbb{N}$, where $n < m$ and $M_0, M_1, \ldots, M_k \in \mathcal{M}_{n \times m}(\mathbb{F}_q)$.
Question: Find – if any – a k-tuple $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_q^k$ such that:

[1] Note that S and T can actually be chosen to be affine. We restrict ourselves to linear secrets for the sake of simplicity. However, we mention that the attack can be simply adapted to work in the affine case (see [27,34]).

$$\operatorname{Rank}\left(\sum_{i=1}^{k} \lambda_i \, M_i - M_0\right) \leqslant r.$$

In Appendix A, we review some known techniques for solving MinRank.

2.3 Good Keys

Our attack relies on so-called *equivalent keys* introduced by Wolf and Preneel [40,41]. We briefly recall below the concept of equivalent keys, and then present *good keys* which are at the core of our attack.

Let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset \mathbb{F}_q[x_1, \ldots, x_n]^m$. For $k, 1 \leqslant k \leqslant m$, we denote by $I^{(k)} \subseteq \{x_i x_j \,|\, 1 \leqslant i \leqslant j \leqslant n\}$ a subset of the degree-2 monomials. We define $\mathcal{F}\big|_I = \{f_1\big|_{I^{(1)}}, \ldots, f_m\big|_{I^{(m)}}\}$ where $f_k\big|_{I^{(k)}} := \sum_{x_i x_j \in I^{(k)}} \gamma_{i,j}^{(k)} x_i x_j$ is the projection of f_k to $I^{(k)}$.

Definition 1. *Let* $(\mathcal{F}, S, T), (\mathcal{F}', S', T') \in \mathbb{F}_q[x_1, \ldots, x_n]^m \times \mathrm{GL}_n(\mathbb{F}_q) \times \mathrm{GL}_m(\mathbb{F}_q)$. *We say that* $(\mathcal{F}, S, T)$ *and* $(\mathcal{F}', S', T')$ *are* equivalent keys, *denoted by* $(\mathcal{F}, S, T) \simeq (\mathcal{F},' S', T')$, *if and only if* $(T \circ \mathcal{F} \circ S = T' \circ \mathcal{F}' \circ S') \wedge \left(\mathcal{F}\big|_I = \mathcal{F}'\big|_I\right)$, *that is,* $\mathcal{F}$ *and* $\mathcal{F}'$ *share the same structure when restricted to a fixed set* $I = \{I^{(1)}, \ldots, I^{(m)}\}$.

Since the relation $\simeq$ given by Definition 1 is an equivalence relation [40], the set of all keys S, T can be partitioned into several equivalence classes. For a large fraction of all equivalence classes, we can find special representatives S' and T' with fixed entries at certain values.

For ease of notation, let $\overline{S} := S^{-1}$ and $\overline{T} := T^{-1}$. Obviously $\mathcal{P} = T \circ \mathcal{F} \circ S$, implies that $\mathcal{F} = \overline{T} \circ \mathcal{P} \circ \overline{S}$. This leads to the equality below on the quadratic forms:

$$\mathfrak{F}^{(k)} = \overline{S}^{\intercal} \left(\sum_{j=1}^{m} \bar{t}_{k,j} \mathfrak{P}^{(j)}\right) \overline{S}, \; \forall k, 1 \leqslant k \leqslant m. \tag{2}$$

The corresponding system of equations is as follows:

$$\mathfrak{F}_{i,j}^{(k)} = \sum_{x=1}^{m} \sum_{y=1}^{n} \sum_{z=1}^{n} \mathfrak{P}_{y,z}^{(x)} \bar{t}_{k,x} \bar{s}_{y,i} \bar{s}_{z,j}. \tag{3}$$

Due to the structure of the secret mapping $\mathfrak{F}$, we know that certain coefficients in $\mathfrak{F}^{(i)}$ are systematically zero. This allows then to obtain cubic equations on the components of $\overline{S}$ and $\overline{T}$. In general, the system of equations has too many variables for being solved efficiently in this form.

The concept of equivalent keys allows to reduce the number of variables by introducing two linear maps $(\Sigma, \Omega) \in \mathrm{GL}_m(\mathbb{F}_q) \times \mathrm{GL}_n(\mathbb{F}_q)$ such that $\mathcal{P} = T \circ \Sigma^{-1} \circ \Sigma \circ \mathcal{F} \circ \Omega \circ \Omega^{-1} \circ S$. If $\mathcal{F}$ and $\mathcal{F}' := \Sigma \circ \mathcal{F} \circ \Omega$ share the same structure (cf. Def. 1), then $T' := T\Sigma^{-1}$ and $S' = \Omega^{-1} S$ will be equivalent keys. Depending on Σ and Ω we can define a canonical form of the secret-keys and typically fix

large parts of T and S (see [40,39,41]). We note that it may happen that such a canonical key does not exist. For example, the Unbalanced Oil and Vinegar Scheme has such an equivalent key with probability roughly $1 - 1/q$ [36].
The idea of *good keys* [37] is to further decrease the number of unknowns or unfixed coefficients in (S', T'). Here, we do not aim to preserve all the zero coefficients of $\mathcal{F}$, but just some of them. This way, we have more freedom to choose Σ and Ω and thus further reduce the number of variables. On the other hand, we can generate less equations. Finding the best trade-off is not obvious and strongly depends on the underlying structure of $\mathcal{F}$. Formally, we define good keys through the following definition.

Definition 2 ([37]). *Let $(\mathcal{F}, S, T), (\mathcal{F}', S', T')$ be in $\mathbb{F}_q[x_1, \ldots, x_n]^m \times \mathrm{GL}_n(\mathbb{F}_q) \times \mathrm{GL}_m(\mathbb{F}_q)$. Let $I = \{I^{(1)}, \ldots, I^{(m)}\}$ and $J = \{J^{(1)}, \ldots, J^{(m)}\}$ such that $J^{(k)} \subsetneq I^{(k)}$ for all $k, 1 \leqslant k \leqslant m$ with at least one $J^{(k)} \neq \emptyset$. We shall say that $(\mathcal{F}', S', T') \in \mathbb{F}_q[x_1, \ldots, x_n]^m \times \mathrm{GL}_n(\mathbb{F}_q) \times \mathrm{GL}_m(\mathbb{F}_q)$ is a* good key *for $(\mathcal{F}, S, T)$ if and only if:*

$$\left(T \circ \mathcal{F} \circ S = T' \circ \mathcal{F}' \circ S'\right) \wedge \left(\mathcal{F}\big|_J = \mathcal{F}'\big|_J\right).$$

3 MQQ Cryptosystems

The Multivariate Quadratic Quasigroup (MQQ) scheme was proposed in 2008 [21]. The underlying idea is to use bijective multivariate quadratic maps obtained through the existence of left and right inverses in some quasigroup, in order to build the trapdoor map $\mathcal{F}$.

Definition 3. *Let Q be a set and $\mathfrak{q} : Q \times Q \to Q$ be a binary operation on Q. We call $(Q, \mathfrak{q})$ a* left (resp. right) quasigroup *if*

$$\forall\, \overline{u}, \overline{v} \in Q, \exists!\, \overline{x}, \overline{y} \in Q : \mathfrak{q}(\overline{u}, \overline{x}) = \overline{v} \quad (resp.\ \mathfrak{q}(\overline{y}, \overline{u}) = \overline{v}).$$

If $(Q, \mathfrak{q})$ is both left and right quasigroup, then we simply call it a quasigroup.

Clearly, $\mathfrak{q}$ defines a bijective map if we fix some $\overline{u} \in Q$. Hence, we can define two inverse operations $\mathfrak{q}_\backslash(\overline{u}, \overline{v}) = \overline{x}$ and $\mathfrak{q}_/(\overline{v}, \overline{u}) = \overline{y}$, called left and right parastrophe, respectively. A *multivariate quadratic quasigroup* (MQQ) is a special quasigroup, that can be described through a multivariate quadratic map over some finite field $\mathbb{F}_q$. In [21], $\mathbb{F}_2$ is used to built such MQQs of order 2^d, with parameter $d = 5$ and bilinear maps $\mathfrak{q}$. The central map $\mathcal{F}$ is constructed using a so called quasigroup string transformation of the MQQs, in order to scale the number of variables.

Definition 4. *Let $Q := \mathbb{F}_q^d$ and $\mathfrak{q}_i : Q \times Q \to Q$ be such that $(Q, \mathfrak{q}_i)$ forms a quasigroup for $1 \leqslant i \leqslant \ell$ and some parameter ℓ which allows to scale the scheme later on. We fix some element $\overline{u} \in Q$, call it leader and define $\mathcal{F} : \mathbb{F}_q^{\ell d} \to \mathbb{F}_q^{\ell d}$ through*

$$\begin{array}{rcl}
(f_1, \quad \ldots, f_d\ ) & := & \mathfrak{q}_1(\overline{u}, \overline{x}_1), \\
(f_{d+1}, \quad \ldots, f_{2d}) & := & \mathfrak{q}_2(\overline{x}_1, \overline{x}_2), \\
\vdots & & \vdots \\
(f_{(\ell-1)d+1}, \ldots, f_{\ell d}) & := & \mathfrak{q}_\ell(\overline{x}_{\ell-1}, \overline{x}_\ell).
\end{array}$$

In order to find pre-images of $\mathcal{F}$, we use the corresponding left-parastrophe operations of $\mathfrak{q}_1, \dots, \mathfrak{q}_\ell$. In addition, the authors of [21] used the Dobbertin bijection to deal with the linear part of $\mathcal{F}$ that comes from $\mathfrak{q}_1(\overline{u}, \overline{x}_1)$ for some fixed $\overline{u} \in Q$ and the fact that they chose bilinear maps $\mathfrak{q}_i$.

Unfortunately, this trapdoor provided a lot of structure so the MQQ encryption scheme was broken by a direct attack on the public key [30]. Faugère *et al.* showed in [19] that the degree of regularity of the equations generated by the pubic key can be bounded from above by a small constant. Thus, the complexity of a direct Gröbner basis attack is polynomial.

3.1 MQQ-SIG Signature Scheme

Recently, in [22] a signature scheme was proposed, called MQQ-SIG, which is based on the same idea but makes heavy use of the minus modifier, known from HFE-[33]. MQQ-SIG does not use the Dobbertin bijection and the construction of the quasigroup is different and given by the map $\mathfrak{q} : \mathbb{F}_2^d \times \mathbb{F}_2^d \to \mathbb{F}_2^d$:

$$\mathfrak{q}(\overline{x}, \overline{y}) := B \cdot (I + A_0) \cdot B_2 \cdot \overline{y} + B \cdot B_1 \cdot \overline{x} + \overline{c}, \tag{4}$$

where $\overline{x} := (x_1, x_2, \dots, x_d)^\intercal, \overline{y} := (y_1, y_2, \dots, y_d)^\intercal$, $\overline{c} \in \mathbb{F}_2^d$ and B_1, B_2, $B \in \mathrm{GL}_d(\mathbb{F}_2)$ are arbitrary. $A_0 = [\,0 \quad U_1 \cdot B_1 \cdot \overline{x} \quad U_2 \cdot B_1 \cdot \overline{x} \quad \dots \quad U_{d-1} \cdot B_1 \cdot \overline{x}\,]$, is a $d \times d$ block matrix where U_i, $i \in \{1, \dots d-1\}$ are upper triangular matrices over $\mathbb{F}_2$ having all elements 0 except the elements in the rows from $\{1, \dots, i\}$ that are strictly above the main diagonal.
A key feature of the MQQ-SIG scheme is the application of the minus modifier. In particular, $n/2$ of the equations are removed in the public key $\mathcal{P}$, in order to prevent direct algebraic and MinRank attacks. Therefore, we obtain a signature expansion of factor two for messages of length $n/2$. Further the public key is rather large, since it is defined over $\mathbb{F}_2$. In order to reduce the size of the public key the designers decided to split the message in two and sign it using the same trapdoor function twice. The proposed parameters are $n \in \{160, 192, 224, 256\}$ for the trapdoor function for security levels of 2^{80}, 2^{96}, 2^{112}, 2^{128} binary operations respectively, and $d = 8$ for the order 2^d of the quasigroup.

3.2 MQQ-ENC Encryption Scheme

The encryption scheme MQQ-ENC was recently proposed in [23], and it follows the same line of design as its predecessors. Again, the internal mapping $\mathcal{F}$ is a quasigroups string transformation and the affine secrets S and T are built from two circulant matrices. The minus modifier is used again, but since it is an encryption scheme, only a small fixed number r of polynomials is removed. This destroys the bijectivity of $\mathcal{P}$, so to enable correct decryption a universal hash function is used, and decryption is performed by going through all possible pre-images of $\mathcal{P}$. Compared to its predecessors, MQQ-ENC can be defined over any small field $\mathbb{F}_{p^k}$ and instead of bilinear quasigroups, the authors used more general left quasigroups, *i.e.* mappings that are bijections only in the second variable.

Lemma 1 ([35]). *Let p be prime and $k > 0$ be an integer. For all $s, 1 \leqslant s \leqslant d$, we define the component $\mathfrak{q}_s \in \mathbb{F}_{p^k}[x_1, \ldots, x_d, y_1, \ldots, y_d]$ by:*

$$\mathfrak{q}_s(x_1, \ldots, x_d, y_1, \ldots, y_d) := p_s(y_s) + \sum_{1 \leqslant i,j \leqslant d} \alpha_{i,j}^{(s)} x_i x_j + \sum_{s<i,j \leqslant d} \beta_{i,j}^{(s)} y_i y_j + \sum_{1 \leqslant i \leqslant d, s<j \leqslant d} \gamma_{i,j}^{(s)} x_i y_j + \sum_{1 \leqslant i \leqslant d} \delta_i^{(s)} x_i + \sum_{s<i \leqslant d} \epsilon_i^{(s)} y_i + \eta^{(s)}, \quad (5)$$

where $p_s(y_s) \in \{a^{(s)} y_s, a^{(s)} y_s^2\}$ for even p, and $p_s(y_s) = a^{(s)} y_s$ for odd p, for some $a^{(s)} \neq 0$. The function $\mathfrak{q} = (\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_d) : \mathbb{F}_{p^k}^{2d} \to \mathbb{F}_{p^k}^d$, as defined in (5), defines a left multivariate quadratic quasigroup (LMQQ) $(\mathbb{F}_{p^k}^d, \mathfrak{q})$ of order p^{kd}.

Lemma 2. *Let $(\mathbb{F}_{p^k}^d, \mathfrak{q})$ be an* LMQQ *as defined by Lemma 1. Let D and D_y be $d \times d$ nonsingular matrices and $\overline{c}, \overline{c}_y$ vectors of dimension d over $\mathbb{F}_{p^k}$. Then $\hat{\mathfrak{q}}(\overline{x}, \overline{y}) := D \cdot \mathfrak{q}(\overline{x}, D_y \cdot \overline{y} + \overline{c}_y) + \overline{c}$ is again an LMQQ of order p^{kd}. We say that $\hat{\mathfrak{q}}$ is linearly isotopic to $\mathfrak{q}$.*

The recommended values for the parameters n, k, r, d, p for a security level of 2^{128} are $d = 8$, $p = 2$ and $(n, k, r) \in \{(256, 1, 8), (128, 2, 4), (64, 4, 2), (32, 8, 1)\}$.

4 The Algebraic Structure of MQQ-ENC and MQQ-SIG

We explain the algebraic structure that both MQQ-ENC and MQQ-SIG share. This is the weaknesses that we are going to exploit to mount our attack.
First of all, we note that the trapdoor of MQQ-SIG can be seen as a very special case of MQQ-ENC when defined over $\mathbb{F}_2$. Indeed, the quasigroup string transformation only makes use of the left translation (the bijection in the second variable) of a quasigroup $\mathfrak{q}$, *i.e.* the additional bijectivity in the first variable is unnecessary. Thus, we can regard the MQQs used in MQQ-SIG as left quasigroups without loss of generality. Even more, it can be shown (cf. Proposition 1) that the MQQs used in MQQ-SIG are linearly isotopic to quasigroups that can be represented in the form given in Lemma 1, with some additional constraints on the coefficients.

Proposition 1 ([35]). *Let $(\mathbb{F}_2^d, \hat{\mathfrak{q}})$ be a quasigroup used in* MQQ-SIG. *Then $\hat{\mathfrak{q}}$ can be represented by $\hat{\mathfrak{q}}(\overline{x}, \overline{y}) = B \cdot \mathfrak{q}(B_1 \cdot \overline{x}, B_2 \cdot \overline{y}) + \overline{c}$ for some invertible matrices B, B_1, B_2, a vector $\overline{c}$, and $\mathfrak{q} = (\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_d)$ with*

$$\mathfrak{q}_s(\overline{x}, \overline{y}) = x_s + y_s + \sum_{s<i,j \leqslant d} \gamma_{i,j}^{(s)} x_i y_j + \sum_{s<i \leqslant d} \delta_i^{(s)} x_i + \sum_{s<i \leqslant d} \epsilon_i^{(s)} y_i + \eta^{(s)},$$

for all $1 \leq s \leq d$ and coefficients $\gamma_{i,j}^{(s)}, \delta_i^{(s)}, \epsilon_i^{(s)}, \eta^{(s)} \in \mathbb{F}_{p^k}$.

In the sequel, we will investigate the more general trapdoor of MQQ-ENC, since all the properties of MQQ-ENC apply to MQQ-SIG as well. In order to avoid redundancy and to provide a clear and simple algebraic description, we exploit the following simplification. In the central map $\mathcal{F}$ the authors used LMQQs constructed through Lemma 2, and not directly LMQQs from Lemma 1. This was done to mask the otherwise triangular structure of the LMQQs from Lemma 1. However, the linear isotopy, can actually be absorbed by S and T. First of all, as we are only considering quadratic coefficients later on, we can safely ignore $\overline{c}_y$ and $\overline{c}$. Further, the linear transformation D can be absorbed by T, *i.e.* instead of using $\hat{\mathfrak{q}}$ and the original T, we work with $\mathfrak{q}$ and $T \cdot (I_{\frac{n}{d}} \otimes D)$, with $\otimes$ the matrix tensor product of the $\frac{n}{d}$ dimensional identity matrix and D. The same holds for the transformation of variables S. Instead of working with $\mathfrak{q}$ and the original transformation S, we work with $(I_{\frac{n}{d}} \otimes D_y^{-1}) \cdot S$ and $\tilde{\mathfrak{q}}(\overline{x}_1, \overline{x}_2) := \mathfrak{q}(D_y^{-1}\overline{x}_1, \overline{x}_2)$. As there is no structure hidden in the first component of $\mathfrak{q}$, all the systematical zeros in $\tilde{\mathfrak{q}}$ and $\mathfrak{q}$ equal and thus we can assume a central map $\mathcal{F}$ with $\mathfrak{q}$ according to Lemma 1. Writing the quadratic part of $\mathfrak{q}_s = x^{\intercal}\mathfrak{Q}^{(s)}x$ in its quadratic form with $x = (x_1, \ldots, x_d, y_1, \ldots, y_d)^{\intercal}$, we can illustrate the matrix $\mathfrak{Q}^{(s)}$ by Figure 1.

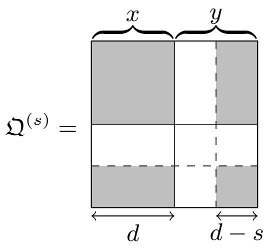

Fig. 1. The quadratic form $\mathfrak{Q}^{(s)}$ of $\mathfrak{q}_s$. Gray parts denote arbitrary values, white parts denote systematic zeros.

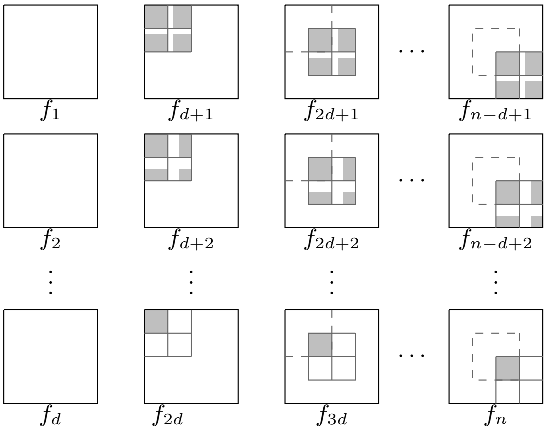

Fig. 2. Matrices of the quadratic forms of the central map $\mathcal{F}$ of MQQ-ENC. Gray parts denote some arbitrary values, whereas white parts denote systematic zeros.

Note that both in odd and even characteristic, the coefficient of y_s^2 does not occur in $\mathfrak{Q}^{(s)}$. In odd characteristic, $p_s(y_s) = a^{(s)}y_s$, *i.e.* it is always linear. For characteristic 2, we have either $p_s(y_s) = a^{(s)}y_s$ or $p_s(y_s) = a^{(s)}y_s^2$, but nevertheless, it is again always linear, and the representation of $\mathfrak{Q}^{(s)}$ has systematic zeros on the main diagonal. The central polynomials f_s (Definition 4), with $s, 1 \leqslant s \leqslant m$ are illustrated in Figure 2.

Another simplification can be made regarding the secret affine transformations S and T. First of all, we neglect linear terms, as we do not use them and they also never interfere with the coefficients of quadratic monomials. Thus we can assume S and T to be linear transformations. Note that using coefficients of linear terms could only speed up the attack, as long as they are not all chosen uniformly at random. Second, in [23] as well as in [22], the authors did not choose S and T purely at random but as a combination of two circulant matrices. This structure was meant to reduce the key size and speed up the decryption process. We note that we do not use this special structure to speed up our attack. As we are recovering $(I_{\frac{n}{d}} \otimes D_y^{-1}) \cdot S$ instead of S and $T \cdot (I_{\frac{n}{d}} \otimes D)$ instead of T, for some randomly chosen D and D_y, we lose most of the structure anyway. Therefore we assume to recover some random matrices in the sequel. Note that this gives a worst case complexity of our attack.

5 Key-Recovery Attack

In this part, we present an efficient algebraic key-recovery attack on MQQ-ENC and MQQ-SIG. To do so, we combine a MinRank attack and good keys in order to recover the columns of S and T.

5.1 High Level Description of the Attack

Remark 2. From now on for better readability, but without loss of generality, we assume the change of variables: $x_{n-id+j} \mapsto x_{n-id+d-j+1}$. (This corresponds to moving the white bands in Fig. 1 to the lower right corner.)

Our attack is performed in $n-r-1$ steps, and in each *Step N*, where $N \in \{n, \dots r+2\}$, we remove the variable x_N from all but the first of the public polynomials $\mathcal{P}$. This is done by finding a good key $(\overline{S}'_N, \overline{T}'_N)$ of a particular form. At the end of each step, we remove the first polynomial form $\mathcal{P}$, since, at this point, that is the only polynomial that contains the variable x_N and repeat the procedure with the rest of the polynomials. Thus, at each *Step N*, w.l.o.g. we can assume that the size of all public matrices is N. After $n-r-1$ steps, we obtain the equivalent key $\overline{S}' = \overline{S}'_n \circ \cdots \circ \overline{S}'_{r+2}$ and $\overline{T}' = \overline{T}'_{r+2} \circ \cdots \circ \overline{T}'_n$. We can summarize the steps of our attack in Alg. 1.

Algorithm 1 High Level Description of the Key-Recovery Attack

```
Input: $n-r$ public polynomials $\mathcal{P}$ in $n$ variables.
  for $N := n$ down to $r+2$ do
    Consider that all public polynomials involve $\leqslant N$ variables.
    Step $N$:
        Find a good key $(\overline{S}'_N, \overline{T}'_N)$.
        Transform the public key as $\mathcal{P} \leftarrow \overline{T}'_N \circ \mathcal{P} \circ \overline{S}'_N$,
        and if $N < n$ remove the first polynomial from $\mathcal{P}$.
  end for;
Output: The equivalent key $\overline{S}' = \overline{S}'_n \circ \cdots \circ \overline{S}'_{r+2}$ and $\overline{T}' = \overline{T}'_{r+2} \circ \cdots \circ \overline{T}'_n$.
```

5.2 Detailed Description of the Attack

We describe in this part the steps performed in Alg. 1. We consider first the case $N = n$ which is a bit different from the others steps.

Step $n = N$. How to recover a linear component of the secret-key. Let $\mathcal{P}$ be the $n-r$ public polynomials in n variables of an MQQ scheme. From now on, we denote by $\mathfrak{P}^{(1)}, \ldots, \mathfrak{P}^{(n-r)}$ the corresponding public matrices. As explained, the public-key is constructed as $\mathcal{P} = T \circ \mathcal{F} \circ S$ where $\mathcal{F}$ is a set of quadratic polynomials constructed as in Sect. 3 and S and T are two bijective linear maps used to mask the structure of $\mathcal{P}$. We denote by $\mathfrak{F}^{(1)}, \ldots, \mathfrak{F}^{(n)}$ the quadratic forms of $\mathcal{F}$.

We explain how to recover one column of the secret transformation S using good keys. This corresponds to the first step performed in Alg. 1 and will allow to remove the variable x_n. Recall from Subsect. 2.3 that we are looking for two linear maps $(\Sigma, \Omega) \in \mathrm{GL}_m(\mathbb{F}_q) \times \mathrm{GL}_n(\mathbb{F}_q)$ such that

$$\mathcal{P} = T \circ \Sigma^{-1} \circ \Sigma \circ \mathcal{F} \circ \Omega \circ \Omega^{-1} \circ S.$$

and $\mathcal{F}' := \Sigma \circ \mathcal{F} \circ \Omega$ preserves some of the structure of $\mathcal{F}$ (cf. Def. 2). Then, $T' := T\Sigma^{-1}$ and $S' = \Omega^{-1}S$ will be good keys.

A crucial observation for MQQ-ENC is that the central polynomials f_i, do not contain the monomials $x_n x_i$ for any $i, 1 \leqslant i < n$. This means that we preserve some structure even if we choose $\Sigma = T$ and thus a good key $T' = I$. In order to preserve the corresponding systematic zero coefficients, Ω is allowed to map every variable to every variable, except x_n. We can then choose the good key S', or more precisely $\overline{S}' := S'^{-1} = \overline{S}\Omega$, to be of the form given in Figure 3.

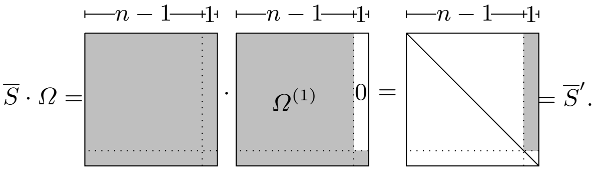

Fig. 3. Unique transformation Ω to obtain the good key $\overline{S}'$.

Obviously, a good key $\overline{S}'$ – according to Figure 3 – almost always exists. We can choose the first $n-1$ columns of Ω equal to the first $n-1$ columns of S. However, there is a small probability for Ω to not be invertible, in which case, a good key does not exist.

Lemma 3. *If $\overline{S}_{n,n} = 0$, then a good key $\overline{S}'$ as given in Figure 3 does not exist.*

Proof. Due to the structure of Ω in Figure 3, we have $\overline{S}_{n,n}\Omega_{n,n} = \overline{S}'_{n,n}$. Thus, $\overline{S}_{n,n} = 0$ implies that $\overline{S}'_{n,n} = 0$ and $\overline{S}'$ can not be invertible. □

Remark 3. To guarantee that a good key as in Figure 3 exists with high probability, we can randomize the public quadratic forms $\mathfrak{P}^{(1)}, \ldots, \mathfrak{P}^{(m)}$ with a random invertible matrix $S_{rand} \in \mathrm{GL}_n(\mathbb{F}_q)$. That is, we construct a new equivalent set of public polynomials $\mathfrak{P}_{rand}^{(i)}$:

$$\mathfrak{P}_{rand}^{(i)} := S_{rand}^{\intercal} \mathfrak{P}^{(i)} S_{rand} = (S S_{rand})^{\intercal} \left(\sum_{j=1}^{n} t_{i,j} \mathfrak{F}^{(j)} \right) S S_{rand}.$$

Since $S_{\ell,\ell} = 0$ holds with probability $1/q$, the average number of randomizations to obtain a nonzero entry at position (ℓ, ℓ) is $q/(q-1)$. From now on, we will always assume that – up to randomization – good keys as in Figure 3 exist.

Using a good key $\overline{T}' = I$ and $\overline{S}'$ as in Figure 3, the algebraic system (3) can be rewritten as:

$$\mathfrak{F}_{i,j}^{\prime(k)} = \sum_{y=1}^{n} \sum_{z=1}^{n} \mathfrak{P}_{y,z}^{(k)} \overline{s}'_{y,i} \overline{s}'_{z,j}.$$

We constructed $\mathcal{F}' := \Sigma \circ \mathcal{F} \circ \Omega$ such that the monomial $x_n x_i$ does not appear for any $i, 1 \leqslant i < n$. This yields $\mathfrak{F}_{n,j}^{\prime(k)} = 0$, for all $k, 1 \leqslant k \leqslant m$, and $j, 1 \leqslant j < n$. Also, for all $j \neq n$, we have that $\overline{s}'_{z,j} = 0$ for $z \neq j$ and $\overline{s}'_{j,j} = 1$ due to the structure of $\overline{S}'$. This yields a system of $m(n-1)$ linear equations in $(n-1)$ variables (since $\overline{s}'_{n,n} = 1$), given by

$$\sum_{y=1}^{n} \mathfrak{P}_{y,j}^{(k)} \overline{s}'_{y,n} = 0, \text{ for all } k, 1 \leqslant k \leqslant m, \text{ and } j, 1 \leqslant j < n.$$

After solving the system, we obtain the good key S'. We can then transform the public polynomials $\mathcal{P}$ with the change of variables $\overline{S}' x$, i.e.:

$$\mathcal{P} \circ \overline{S}' = T \circ \Sigma^{-1} \circ \Sigma \circ \mathcal{F} \circ \Omega \circ \Omega^{-1} \circ S \circ \overline{S}' = \mathcal{F}'.$$

From the previous discussion, the transformed public polynomials $\mathcal{P} \circ \overline{S}'$ do not contain the variable x_n in any of the quadratic terms.

Remark 4. To ease the notation, we continue to denote the obtained transformed polynomials and their matrix representations as before (we regard $\mathcal{P} \circ \overline{S}'$ as being the public $\mathcal{P}$). Since we removed the variable x_n, we can consider that now the dimension of the public matrices $\mathfrak{P}^{(i)}$ is $n-1$. We explain now how to remove the variables $x_{n-1}, x_{n-2} \ldots$ down to x_{r+2}.

Step $N \in \{n-1, \ldots, r+2\}$ – Using MinRank to recover the entire secret key. We assume that the dimension of all public matrices $\mathfrak{P}^{(i)}$ is $N \in \{n-1, \ldots, r+2\}$. Observe that the variable x_N occurs in at most one polynomial of the central map $\mathcal{F}$, namely f_N (cf. Figure 2). This suggests to find a linear combination of two public polynomials, w.l.o.g. p_1 and p_k, with $k, 1 < k \leqslant m$ such that x_N no longer occurs, so we want to find $\lambda \in \mathbb{F}_q$ such that:

$$\mathfrak{P}^{(k)} + \lambda \mathfrak{P}^{(1)} = S^{\intercal} \left(\sum_{j=1}^{N-1} (t_{k,j} + \lambda t_{k,j}) \mathfrak{F}^{(j)} \right) S. \tag{6}$$

To recover such linear combination, we exploit the fact that the rank is invariant under a bijective linear transformation of variables, i.e. for all k, $\mathrm{Rank}(\mathfrak{P}^{(k)}) = \mathrm{Rank}(S^{\mathsf{T}}\mathfrak{P}^{(k)}S)$. Thus, we can use the rank as distinguisher to recover parts of $\overline{T}$. More precisely, we need to solve the following MinRank instance:

$$\text{Find } \lambda \in \mathbb{F}_q \text{ such that } \mathrm{Rank}\left(\mathfrak{P}^{(k)} + \lambda\mathfrak{P}^{(1)}\right) < N. \tag{7}$$

The good key $(\overline{S}'_N, \overline{T}'_N)$ given in Fig. 4 is a solution of (7). Indeed, using the two public polynomials $\mathfrak{P}^{(1)}, \mathfrak{P}^{(k)}$ and thanks to (3), we obtain the following system of $N-1$ quadratic equations in $N-1$ variables:

$$\mathfrak{F}'^{(k)}_{i,j} = \sum_{y=1}^{N}\sum_{z=1}^{N}\left(\mathfrak{P}^{(k)}_{y,z} + \lambda\mathfrak{P}^{(1)}_{y,z}\right)\overline{s}'_{y,i}\overline{s}'_{z,j}.$$

By construction, $\mathfrak{F}'^{(k)}_{N,j} = 0$ for all $j, 1 \leqslant j < N$. Also, for all $j < N$ and $z \neq j$ we have that $\overline{s}'_{z,j} = 0$ and $\overline{s}'_{j,j} = 1$. This gives

$$\sum_{y\,=\,1}^{N}\left(\mathfrak{P}^{(k)}_{y,j} + \lambda\mathfrak{P}^{(1)}_{y,j}\right)\overline{s}'_{y,N} = 0, \text{ for all } j,\ 1 \leqslant j < n. \tag{8}$$

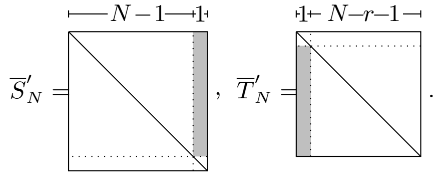

Fig. 4. The good key $(\overline{S}'_N, \overline{T}'_N)$.

Applying the same reasoning for all of the public matrices $\mathfrak{P}^{(k)}$, $1 < k \leqslant N-r+1$ we obtain the good key $(\overline{S}'_N, \overline{T}'_N)$. The correctness of the procedure follows from the next theorem.

Theorem 3. *Let N be the number of variables in the $N-r+1$ public polynomials of* MQQ-ENC *(or* MQQ-SIG*) during step $N \in \{n-1, \ldots, r+2\}$. Let $\overline{s}' = (\overline{s}'_{1,N}, \overline{s}'_{2,N}, \ldots, \overline{s}'_{N-1,N}, 1)$ and $\overline{t}' = (1, \overline{t}'_{2,1}, \overline{t}'_{3,1}, \ldots, \overline{t}'_{N-r+1,1})$ be unknown vectors. Thus, it holds that $(\overline{s}'_0, \overline{t}'_0)$ is a solution of:*

$$\overline{s}'\left(\mathfrak{P}^{(k)} + \overline{t}'_{k,1}\mathfrak{P}^{(1)}\right) = \mathbf{0}_{1\times N}, \quad \forall k, 1 < k \leqslant N-r+1 \tag{9}$$

if and only if $(\overline{S}'_N, \overline{T}'_N)$ is a good key for MQQ-ENC *(respectively* MQQ-SIG*), where $\overline{S}'_N$ is obtained from the identity matrix I_N by replacing the last column with $\overline{s}'_0$, and $\overline{T}'_N$ is obtained from I_N by replacing the first column with $\overline{t}'_0$.*

Proof. From (2), we have that:

$$\mathfrak{F}'^{(k)} = \overline{S}'^{\mathsf{T}}_N\left(\mathfrak{P}^{(k)} + \overline{t}'_{k,1}\mathfrak{P}^{(1)}\right)\overline{S}'_N, \ \forall k, 1 < k \leqslant N-r+1, \text{ or equivalently :}$$

$$\mathfrak{F}'^{(k)}_{i,j} = \sum_{y=1}^{N}\sum_{z=1}^{N}\left(\mathfrak{P}^{(k)}_{y,z} + \overline{t}'_{k,1}\mathfrak{P}^{(1)}_{y,z}\right)\overline{s}'_{y,i}\overline{s}'_{z,j}, \forall 1 < k \leqslant N-r+1.$$

Thus, if $(\overline{S}'_N, \overline{T}'_N)$ is a good key, then $\mathfrak{F}'^{(k)}_{i,N} = 0$ (or equivalently $\mathfrak{F}'^{(k)}_{N,i} = 0$) for every $1 \leqslant i < N$. By construction, for every $1 \leqslant i < N$, $\overline{s}'_{y,i} = 0$, for all $y \neq i$, and $\overline{s}'_{i,i} = 1$. Hence, $(\overline{S}'_N, \overline{T}'_N)$ is a good key if and only if for every i, k, s.t. $1 \leqslant i < N$ and $1 < k \leqslant N - r + 1$ it holds that:

$$\sum_{z=1}^{N} \left(\mathfrak{P}^{(k)}_{i,z} + \overline{t}'_{k,1} \mathfrak{P}^{(1)}_{i,z} \right) \overline{s}'_{z,N} = 0.$$

The last system is equivalent to (9), so the claim follows. □

Remark 5. Note that Theorem 3 can be applied to *Step n* as well. In this case it is known that $\overline{t}'_{k,1} = 0$, so instead of a system of quadratic equations we obtain a system of linear equations as explained in the previous part. So, *Step* $n = N$ is actually just an easier sub-case of the others steps.

6 Modeling Good Keys as MinRank for Rectangular Matrices

Theorem 3 shows that the problem of finding a good key is equivalent to finding the intersection of the kernels of some linear combinations of the public matrices. This can be nicely modeled as a special instance of the MinRank problem for rectangular matrices.

Corollary 1. *Let N, $\overline{s}'$ and $\overline{t}'$ be as in Theorem 3. Let*

$$\mathfrak{P} = [\mathfrak{P}^{(2)} | \mathfrak{P}^{(3)} | \ldots | \mathfrak{P}^{(N-r+1)}]_{N \times N(N-r)}, \ \mathfrak{P}_i = [\mathbf{0} | \ldots | \mathbf{0} | \mathfrak{P}^{(1)} | \mathbf{0} | \ldots | \mathbf{0}]_{N \times N(N-r)}$$

be block matrices, where $\mathfrak{P}^{(1)}$ is the i-th block in $\mathfrak{P}_i$. It holds that finding a good key $(\overline{S}'_N, \overline{T}'_N)$ of the form given in Theorem 3 for MQQ-ENC *(or* MQQ-SIG*) is equivalent to solving the MinRank instance defined below:*

$$\textit{Find } \overline{t}'_{2,1}, \ldots, \overline{t}'_{N-r+1,1} \in \mathbb{F}_q \ \textit{s.t.} \ \mathrm{Rank} \left(\mathfrak{P} + \sum_{k=2}^{N-r+1} \overline{t}'_{k,1} \mathfrak{P}_k \right) < N. \qquad (10)$$

Proof. Using the Kipnis-Shamir modeling, the MinRank instance (10) can be expressed exactly as the system (9). The claim follows from Theorem 3. □

In Alg. 2, we summarize our key-recovery attack on MQQ-ENC and MQQ-SIG based on the results from Theorem 3, Remark 5 and Corollary 1.

7 Complexity of the Key-Recovery Attack

In this part, we show that the complexity of our attack is polynomial. To do so, we present a complexity analysis of the Alg. 2. We also present experimental results which confirm our theoretical results.

Algorithm 2 Key Recovery

```
Input: $n - r$ public polynomials $\mathcal{P}$ in $n$ variables.
  for $N := n$ down to $r + 2$ do
    Consider the dimension of all public matrices $\mathfrak{P}^{(i)}$ to be $N$.
    If $N = n$, set $b = 0$, otherwise set $b = 1$.
    Step Rectangular MinRank($N$):
      Let $\overline{s}' = (\overline{s}'_{1,N}, \overline{s}'_{2,N}, \ldots, \overline{s}'_{N-1,N}, 1)$ and $\overline{t}' = (\overline{t}'_{2,1}, \overline{t}'_{3,1}, \ldots, \overline{t}'_{N-r+b,1})$
      be unknown vectors.
      Find a good key $(\overline{S}'_N, \overline{T}'_N)$ by solving the system (9) in $(\overline{s}', \overline{t}')$:
        $\overline{s}' \left( \mathfrak{P} + \sum_{k=2}^{N-r+b} \overline{t}'_{k,1} \mathfrak{P}_k \right) = \mathbf{0}_{1\times N(N-r)}$, where if $b = 0$, then $\overline{t}' = (0, 0, \ldots, 0)$;
      for $\mathfrak{P} = [\mathfrak{P}^{(2)} | \mathfrak{P}^{(3)} | \ldots | \mathfrak{P}^{(N-r+1)}]_{1\times N(N-r)}$ and
      $\mathfrak{P}_i = [\mathbf{0} | \ldots | \mathbf{0} | \mathfrak{P}^{(1)} | \mathbf{0} | \ldots | \mathbf{0}]_{1\times N(N-r)}$ with $\mathfrak{P}^{(1)}$ being the $i$-th block in $\mathfrak{P}_i$.
    Transform the public key: $\mathcal{P} \leftarrow \overline{T}'_N \circ \mathcal{P} \circ \overline{S}'_N$,
    If $b = 1$ remove the first polynomial from $\mathcal{P}$ ($\mathcal{P}$ now contains $N - r$ polynomials).
  end for;
Output: The equivalent keys $\overline{S}' = \overline{S}'_n \circ \cdots \circ \overline{S}'_{r+2}$ and $\overline{T}' = \overline{T}'_{r+2} \circ \cdots \circ \overline{T}'_n$.
```

7.1 Theoretical Complexity

The goal of this part is to bound the complexity of solving the algebraic equations (9) arising at each step of Alg. 2. As we will see from the experimental results (Sect. 7.2), it appears that the system (9) can be solved efficiently in practice. In particular, the maximum degree reached during the Gröbner basis computation is bounded by a small constant, 3. We will now theoretically explain this fact.
A strategy for bounding the complexity of solving (9) is to consider a subset of the equations. In particular, the equations of (9) derived from a given $k, 1 < k \leqslant N - r + 1$ correspond to a Kipnis-Shamir modeling of the MinRank problem (7). To give intuition, we consider a pair of matrices $\left(\mathfrak{P}^{(1)}, \mathfrak{P}^{(k)}\right)$ such that $\mathfrak{P}^{(1)}$ is invertible. Setting $\mathfrak{P}^* = \mathfrak{P}^{(k)}\left(\mathfrak{P}^{(1)}\right)^{-1}$, we obtain that (7) is equivalent to:

$$\text{Find } \lambda \in \mathbb{F}_q \text{ such that } \mathrm{Det}(\mathfrak{P}^* - \lambda I_N) = 0. \tag{11}$$

We can compute the roots of the characteristic polynomial, which are the eigenvalues of $\mathfrak{P}^* - \lambda I_N$, and the corresponding eigenvectors. All such pairs will vanish the k-th equation of (9). We can then substitute each possible eigenvector in the other equations and solve the linear system involving the remaining unknowns. We have found a part of the secret-key as soon as the linear system is consistent. However, the complexity of this approach will depend on the multiplicity of the eigenvalues. If all the roots of (11) are simple, then the approach described, allows to solve the system (9) in polynomial-time.

Remark 6. In characteristic 2, the previous discussion does not directly apply since the matrix representation of a public polynomial has always an even rank (cf. Remark 1). In particular, the situation is as follows:

- When N is even, the rank of the skew-symmetric matrices $\mathfrak{P}^{(1)}$ and $\mathfrak{P}^{(k)}$ is $\leqslant N$. A drop of the rank will likely yield $\operatorname{Rank}\left(\mathfrak{P}^{(k)} + \lambda \mathfrak{P}^{(1)}\right) = N - 2$. In this case, we can expect that the MinRank problem has unique solution λ. For this λ, the dimension of $\operatorname{Ker}\left(\mathfrak{P}^{(k)} + \lambda \mathfrak{P}^{(1)}\right)$ is 2 (in this case, (11) would have a root of multiplicity > 1). Since $\overline{s}'_{N,N} = 1$ in (8), we obtain q solutions for the good key $\overline{S}'_N$.
- For odd N, the rank of the matrices $\mathfrak{P}^{(1)}$ and $\mathfrak{P}^{(k)}$ is $\leqslant N - 1$, which means that (7) is satisfied for any λ. In this case, since $\overline{s}'_{N,N} = 1$, for each $\lambda \in \mathbb{F}_q$ we get a unique solution for the good key $\overline{S}'_N$ if the rank defect is minimum, just one.

To analyse the complexity of this simple approach, we introduce:

Definition 5. *Let $\mathbb{F}_q$ be a field of characteristic 2 and $(A, B) \in \mathbb{F}_q^{N\times N} \times \mathbb{F}_q^{N\times N}$ be a pencil [20] of skew-symmetric matrices. We shall say that the pencil is generic if for all $\lambda_0 \in \mathbb{F}_q, \operatorname{Ker}(A + \lambda_0 B)$ is of dimension $\leqslant 2$ if N is even and $\leqslant 1$ otherwise.*

If N is odd, a generic pencil (A, B) means that the pencil is always of maximal possible rank. If N is even, the pencil is generic if the rank defect, if any, is minimal, just one.

Remark 7. For the parameter sets of the MQQ cryptosystems, we can assume with high probability that the pencils from the public matrices are generic. Indeed, let $\lambda(q, n) = \prod_{i=1}^{n} \left(1 - 1/q^i\right)$ be the probability that a $n \times n$ matrix over $\mathbb{F}_q$ is invertible. It is known from [28] (and recalled in [9, Section 10]) that the probability that a skew-symmetric matrix is of maximal rank $(n-1)$ when n is odd is $\mathrm{Pr}_{\mathrm{odd}} = \frac{\lambda(q,n)}{\lambda(q^2,(n-1)/2)} \frac{1}{1-1/q}$ and the probability that it is of rank $\geqslant n-2$ when n is even is: $\mathrm{Pr}_{\mathrm{even}} = \frac{\lambda(q,n)}{\lambda(q^2,(n-1)/2)} \left(1 + \frac{q^n-1}{q^{n-2}(q^2-1)(q-1)}\right)$. Having this in mind, we get that the probability that the pencils in question are generic is $(\mathrm{Pr}_{\mathrm{odd}})^q$ or $(\mathrm{Pr}_{\mathrm{even}})^q$, depending on the parity of n. In either case, for the parameter sets of MQQ-ENC and MQQ-SIG (as in Section 7.2), it can be checked that the probability is bigger than 0.7.

We first assume that the field q is not too big, typically $q = \mathcal{O}(n)$. This is indeed the case for most of the parameters proposed so far for MQQ cryptosystems.

Theorem 4. *Let $N \in \{n-1, \ldots, r+2\}$ and let $\mathbb{F}_q$ be a field of characteristic 2 such that $q = \mathcal{O}(n)$. Let $\mathfrak{P}^{(1)}, \ldots, \mathfrak{P}^{(N-r+1)} \in \mathbb{F}_q^{N\times N}$ be the skew-symmetric matrices occurring in Algorithm 2 at step* Rectangular MinRank(N). *If there exists $i_0, 2 \leqslant i_0 \leqslant (N - r + 1)$ such that the pencil $(\mathfrak{P}^{(1)}, \mathfrak{P}^{(i_0)})$ is generic, then, the system (9) of Theorem 3 can be solved with probability $1 - 1/q$ in $\mathcal{O}(n^{\omega+2})$ operations, where $2 \leqslant \omega < 3$ is the linear algebra constant. In total, and under the assumptions, there exists an algorithm which recovers a key equivalent to the secret-key in*

$$\mathcal{O}\left(n^{\omega+3}\right) \textit{ operations with probability } 1 - 1/q.$$

The proof can be found in Appendix B. Theorem 4 can be extended even if we assume that there exists a pencil of matrices for which the rank defect is small, that is, a constant. More generally, for arbitrary q and N, we show that we can get a complexity which is independent of the field size and polynomial in the number of variables. More precisely, the following result holds (proof in Appendix B).

Theorem 5. *Let $\mathbb{F}_q$ be an arbitrary field of characteristic 2 and let $N \in \{n-1,\ldots,r+2\}$. We assume that the system (9) of Theorem 3 is not harder to solve than a generic affine bi-linear system (Theorem 7). Let the matrices $\mathfrak{P}^{(1)},\ldots,\mathfrak{P}^{(N-r+1)} \in \mathbb{F}_q^{N\times N}$ be as in Algorithm 2. If there exist $i_0, i_1 \in \{2,\ldots,(N-r+1)\}$ such that the pencils $(\mathfrak{P}^{(1)},\mathfrak{P}^{(i_0)})$, and $(\mathfrak{P}^{(1)},\mathfrak{P}^{(i_1)})$ are generic, and if we assume that the corresponding kernels behave like random, then, for all $N \in \{n-1,\ldots,r+2\}$, the system (9) of Theorem 3 can be solved in $\mathcal{O}(N^{3\,\omega})$, with $2 \leqslant \omega < 3$ the linear algebra constant. In total, and under the assumptions, there exists an algorithm which recovers a key equivalent to the secret-key in*

$$\mathcal{O}(n^{3\,\omega+1}) \text{ field operations with probability } \left(1-\tfrac{1}{q}\right)\left(1-\tfrac{1}{q^{n-3}}\right).$$

7.2 Experimental Results

For the parameter sets proposed for MQQ-ENC [23] and MQQ-SIG [22] the results from Theorem 5 lead to the complexities given in Table 1 and Table 2. They have been calculated using the more precise formula $C(n,r,q) = \sum_{N=r+2}^{n-1}\binom{N+4}{3}^{\omega}$.

Table 1. Theoretical complexities, in terms of field operations, of the key recovery attack on MQQ-ENC compared to the original decryption algorithm. All of the parameters are for claimed security of $\mathcal{O}(2^{128})$.

2^k	k	n	r	d	Decryption	Key Recovery
2	1	256	8	8	2^{25}	$2^{56.3}$
4	2	128	4	8	2^{23}	$2^{48.2}$
16	4	64	2	8	2^{21}	$2^{40.3}$
256	8	32	1	8	2^{20}	$2^{32.5}$

Table 2. Theoretical complexities, in terms of field operations, of the key recovery attack on MQQ-SIG compared to the claimed security level.

Security	n	d	Key Recovery
2^{80}	160	8	$2^{50.8}$
2^{96}	192	8	$2^{52.9}$
2^{112}	224	8	$2^{54.7}$
2^{128}	256	8	$2^{56.2}$

We have implemented the attack in Magma (Version 2.19-10 [8]) on a workstation with 32 cores based on Intel Xeon 2.27GHz, with 1TB of RAM memory. The results of the practical attack are summarized in Table 3 and Table 4.

From the tables, we can see that all our experiments, for both MQQ-ENC, and MQQ-SIG, confirmed that the maximum degree reached during the Gröbner basis computation ($d_{\max}$) of the system (9) is 3, consistent with Theorem 4. Furthermore, the results are almost a perfect match with the theoretical calculations of Theorem 5.

Table 3. Results of the practical attack on MQQ-ENC.

2^k	k	n	r	d	Key Recovery Theoretical	Key Recovery Practical		
						cycles	sec	$d_{\max}$
2	1	64	8	8	$2^{40.3}$	$2^{43.4}$	5421	3
2	1	96	8	8	$2^{44.9}$	$2^{47.8}$	111844	3
4	2	64	4	8	$2^{40.3}$	$2^{43.7}$	6978	3
4	2	96	4	8	$2^{44.9}$	$2^{47.8}$	109258	3
4	2	128	4	8	$2^{48.2}$	$2^{50.6}$	787214	3
16	4	32	2	8	$2^{32.5}$	$2^{34.7}$	14	3
16	4	48	2	8	$2^{37.0}$	$2^{38.9}$	251	3
16	4	64	2	8	$2^{40.3}$	$2^{41.6}$	1783	3

Table 4. Results of the practical attack on MQQ-SIG.

n	r	d	Key Recovery Theoretical	Key Recovery Practical		
				cycles	sec	$d_{\max}$
64	32	8	$2^{40.3}$	$2^{40.1}$	560	3
96	48	8	$2^{44.9}$	$2^{43.2}$	4822	3
128	64	8	$2^{48.2}$	$2^{46.0}$	34376	3
160	80	8	$2^{50.8}$	$2^{48.0}$	120882	3

8 Conclusion

Mounting a successful key recovery attack against MQQ-ENC and MQQ-SIG using good keys, we have yet again shown that MinRank is a fundamental problem in $\mathcal{MQ}$ cryptography. We have, however, also shown that it is necessary to take into account the parity of the characteristic of the field when using MinRank to reveal the good key. Because of the different representation of quadratic polynomials over fields of characteristic 2, the attack, otherwise valid over odd characteristic fields, can not be directly applied. Interestingly, this has often been overlooked in the literature. By unveiling the pitfalls in the attack of the MQQ schemes arising from the even characteristic of the field, our analysis shows that the same modification is necessary when attacking similar $\mathcal{MQ}$ schemes over fields of characteristic 2 using MinRank.

Acknowledgements

We thank the anonymous referees for detailed comments which greatly improved this work. Jean-Charles Faugère, and Ludovic Perret have been partially supported by the HPAC grant (ANR-11-BS02-013) of the French National Research

Agency. Simona Samardjiska has been partially supported by FCSE, UKIM, Macedonia and the COINS Research School of Computer and Information Security, Norway.

References

1. Barbulescu, R., Gaudry, P., Joux, A., Thomé, E.: A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In: P.Q. Nguyen, E. Oswald (eds.) Advances in Cryptology - EUROCRYPT 2014. Proc., *LNCS*, vol. 8441, pp. 1–16. Springer (2014).
2. Bardet, M., Faugère, J.C., Salvy, B.: On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In: Proc. of International Conference on Polynomial System Solving (ICPSS), pp. 71–75 (2004)
3. Bardet, M., Faugère, J.C., Salvy, B., Yang, B.Y.: Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. In: Proc. of MEGA 2005, Eighth Int. Symposium on Effective Methods in Algebraic Geometry (2005)
4. Bernstein, D.J., Lange, T. (eds.): eBACS: ECRYPT Benchmarking of Cryptographic Systems. (2014). URL `http://bench.cr.yp.to`
5. Bettale, L., Faugère, J.C., Perret, L.: Cryptanalysis of multivariate and odd-characteristic hfe variants. In: Public Key Cryptography – PKC 2011, *LNCS*, vol. 6571, pp. 441–458. Springer (2011)
6. Bettale, L., Faugre, J.C., Perret, L.: Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. Designs, Codes and Cryptography **69**(1), 1–52 (2013)
7. Billet, O., Gilbert, H.: Cryptanalysis of Rainbow. In: SCN, *LNCS*, vol. 4116, pp. 336–347. Springer (2006)
8. Bosma, W., Cannon, J., Playoust, C.: The Magma Algebra System. I. The User Language. J. Symbolic Comput. **24**(3-4), 235–265 (1997). Computational algebra and number theory (London, 1993)
9. Bouillaguet, C.: Etudes d'hypothèses algorithmiques et attaques de primitives cryptographiques. Ph.D. thesis, Paris Diderot, France (2011)
10. Buss, W., Frandsen, G., Shallit, J.: The computational complexity of some problems of linear algebra. Journal of Computer and System Sciences (1999)
11. Courtois, N., Goubin, L.: Cryptanalysis of the TTM cryptosystem. In: Advances in Cryptology – ASIACRYPT '00, *LNCS*, vol. 1976, pp. 44–57. Springer (2000)
12. Courtois, N., Goubin, L., Patarin, J.: Sflash, a fast asymmetric signature scheme for low-cost smartcards - primitive specification and supporting documentation. URL `https://www.cosic.esat.kuleuven.ac.be/nessie/workshop/`
13. Courtois, N.T.: Efficient zero-knowledge authentication based on a linear algebra problem MinRank. In: Advances in Cryptology – ASIACRYPT 2001, *LNCS*, vol. 2248, pp. 402–421. Springer (2001)
14. Ding, J., Yang, B.Y., Chen, C.H.O., Chen, M.S., Cheng, C.M.: New differential-algebraic attacks and reparametrization of rainbow. In: ACNS, *LNCS*, vol. 5037, pp. 242–257 (2008)
15. Dubois, V., Fouque, P.A., Shamir, A., Stern, J.: Practical cryptanalysis of SFLASH. In: Proc. of the 27th annual international cryptology conference on Advances in cryptology, CRYPTO'07, pp. 1–12. Springer-Verlag, Berlin, Heidelberg (2007)
16. ETSI: 2nd Quantum-Safe Crypto Workshop in partnership with the IQC. `http://www.etsi.org/news-events/events/770-etsi-crypto-workshop-2014`, [Retrieved: September 2014]

17. Faugère, J.C., Din, M.S.E., Spaenlehauer, P.J.: Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1, 1): Algorithms and complexity. J. Symb. Comput. **46**(4), 406–437 (2011)
18. Faugère, J.C., Levy-dit-Vehel, F., Perret, L.: Cryptanalysis of MinRank. In: Advances in Cryptology – CRYPTO 2008, *LNCS*, vol. 5157, pp. 280–296. Springer (2008)
19. Faugère, J.C., Ødegård, R.S., Perret, L., Gligoroski, D.: Analysis of the MQQ Public Key Cryptosystem. In: CANS, *LNCS*, vol. 6467, pp. 169–183. Springer (2010)
20. Gantmacher, F.: The Theory of Matrices, Vol. 1. Chelsea (1959)
21. Gligoroski, D., Markovski, S., Knapskog, S.J.: Multivariate Quadratic Trapdoor Functions based on Multivariate Quadratic Quasigroups. In: Proc. of the American Conference on Applied Mathematics, MATH, pp. 44–49. World Scientific and Engineering Academy and Society (WSEAS) (2008)
22. Gligoroski, D., Ødegård, R.S., Jensen, R.E., Perret, L., Faugère, J.C., Knapskog, S.J., Markovski, S.: MQQ-SIG - An Ultra-Fast and Provably CMA Resistant Digital Signature Scheme. In: INTRUST, *LNCS*, vol. 7222, pp. 184–203. Springer (2011)
23. Gligoroski, D., Samardjiska, S.: The Multivariate Probabilistic Encryption Scheme MQQ-ENC. In: SCC (2012)
24. Imai, H., Matsumoto, T.: Algebraic methods for constructing asymmetric cryptosystems. In: J. Calmet (ed.) AAECC, *LNCS*, vol. 229, pp. 108–119. Springer (1985)
25. Jiang, X., Ding, J., Hu, L.: Kipnis-Shamir attack on HFE revisited. In: Information Security and Cryptology, *LNCS*, vol. 4990, pp. 399–411. Springer (2007)
26. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. In: IN ADVANCES IN CRYPTOLOGY EUROCRYPT 1999, pp. 206–222. Springer (1999)
27. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization. In: Advances in Cryptology – CRYPTO '99, *LNCS*, vol. 1666, pp. 19–30. Springer (1999)
28. MacWilliams, J.: Orthogonal matrices over finite fields. Orthogonal matrices over finite fields. The American Mathematical Monthly **76**(2), 152?–164 (1969)
29. Moh, T.T.: A public key system with signature and master key functions. Communications in Algebra **27**(5), 2207–2222 (1999)
30. Mohamed, M.S.E., Ding, J., Buchmann, J., Werner, F.: Algebraic Attack on the MQQ Public Key Cryptosystem. In: CANS, *LNCS*, vol. 5888, pp. 392–401. Springer (2009)
31. NESSIE: New european schemes for signatures, integrity, and encryption (2003). `https://www.cosic.esat.kuleuven.be/nessie/`, [Retrieved: September 2014]
32. NIST: Workshop on Cybersecurity in a Post-Quantum World. `http://www.nist.gov/itl/csd/ct/post-quantum-crypto-workshop-2015.cfm`, [Retrieved: September 2014]
33. Patarin, J.: Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms. In: Advances in Cryptology – EUROCRYPT '96, *LNCS*, vol. 1070, pp. 33–48. Springer (1996)
34. Perret, L.: A Fast Cryptanalysis of the Isomorphism of Polynomials with One Secret Problem. In: EUROCRYPT, *LNCS*, vol. 3494, pp. 354–370. Springer (2005)
35. Samardjiska, S., Chen, Y., Gligoroski, D.: Algorithms for Construction of Multivariate Quadratic Quasigroups (MQQs) and Their Parastrophe Operations in Arbitrary Galois Fields. J. Inf. Assurance and Security **7**(3), 146–172 (2012)

36. Thomae, E.: About the Security of Multivariate Quadratic Public Key Schemes. Ph.D. thesis, Ruhr-University Bochum, Germany (2013)
37. Thomae, E., Wolf, C.: Cryptanalysis of Enhanced TTS, STS and all its Variants, or: Why Cross-Terms are Important. In: Progress in Cryptology – AFRICACRYPT 2012, *LNCS*, vol. 7374, pp. 188–202. Springer (2012)
38. Wolf, C., Braeken, A., Preneel, B.: On the security of stepwise triangular systems. Designs, Codes and Cryptography **40**(3), 285–302 (2006)
39. Wolf, C., Preneel, B.: Equivalent keys in HFE, C*, and variations. In: Progress in Cryptology – Mycrypt 2005, *LNCS*, vol. 3715, pp. 33–49. Springer (2005)
40. Wolf, C., Preneel, B.: Large Superfluous Keys in Multivariate Quadratic Asymmetric Systems. In: Public Key Cryptography, *LNCS*, vol. 3386, pp. 275–287. Springer (2005)
41. Wolf, C., Preneel, B.: Equivalent Keys in Multivariate Quadratic Public Key Systems. Journal of Mathematical Cryptology **4**, 375–415 (2011)
42. Yang, B.Y., Chen, J.M., Chen, Y.H.: TTS: High-Speed Signatures on a Low-Cost Smart Card. In: CHES, *LNCS*, vol. 3156, pp. 371–385. Springer (2004)

A The MinRank problem

The MinRank problem over a finite field $\mathbb{F}_q$ is defined as follows.
MinRank (MR)
Input: $n, m, r, k \in \mathbb{N}$, where $n < m$ and $M_0, M_1, \ldots, M_k \in \mathcal{M}_{n\times m}(\mathbb{F}_q)$.
Question: Find – if any – a k-tuple $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_q^k$ such that:

$$\mathrm{Rank}\left(\sum_{i=1}^{k} \lambda_i\, M_i - M_0\right) \leqslant r.$$

Kipnis and Shamir [27] proposed to model the MinRank problem as a multivariate polynomial system of equations. The basic idea of the modeling is that the matrix $\left(\sum_{i=1}^{k} \lambda_i\, M_i - M_0\right)$ has rank $\leqslant r$ if and only if there exists a set of $n-r$ independent vectors in its left kernel. Writing this set as a matrix in echelon form, yields a system of $n\,(n-r)$ equations in $r\,(n-r)+k$ variables given in matrix form:

$$\begin{pmatrix} 1 & & & x_{1,1} & \ldots & x_{1,r} \\ & \ddots & & \vdots & & \vdots \\ & & 1 & x_{n-r,1} & \ldots & x_{n-r,r} \end{pmatrix} \cdot \left(\sum_{i=1}^{k} \lambda_i\, M_i - M_0\right) = \mathbf{0}_{n\times n}. \tag{12}$$

Note that, over a finite field, the set of unknown independent vectors can be written in such a systematic form with high probability. Initially, relinearization [27] was used to solve this algebraic system. The authors of [18] proposed instead to use Gröbner bases tools to solve this system. In addition, [18] noticed that the system has a specific structure: it is formed by bilinear equations [17]. We recall the complexity of the F$_5$ algorithm for computing a grevlex Gröbner basis of a polynomial system as given in [2,3].

Theorem 6. *The complexity of computing a Gröbner basis of a zero-dimensional (i.e. with a finite number of solutions in the algebraic closure of the coefficient field) polynomial system of m equations in n variables with F_5 is*

$$\mathcal{O}\left(m \cdot \binom{n + d_{\mathrm{reg}}}{d_{\mathrm{reg}}}^{\omega}\right),$$

where d_{reg} is the degree of regularity of the ideal and $2 \leqslant \omega \leqslant 3$ the linear algebra constant.

Informally, d_{reg} is the maximum degree reached during a Gröbner basis computation. It has to be noticed that if the degree of regularity does not depend on the number of variables, the complexity then becomes polynomial in n.
From Theorem 6, we can see that in order to estimate the complexity of finding the MinRank solution with this modeling, we need a good estimate of the degree of regularity of the system (12). Using the fact that (12) is an affine bilinear system, the following tight bound can be appropriately used for the purpose.

Theorem 7 ([17]). *Let X and Y be two blocks of variables of sizes n_X and n_Y respectively. We shall say $f \in \mathbb{K}[X, Y]$ is bilinear if $f(\alpha X, \beta Y) = \alpha\,\beta\, f(X, Y)$ for all $(\alpha, \beta) \in \mathbb{K} \times \mathbb{K}$. For the grevlex ordering, the degree of regularity of a generic affine bilinear zero-dimensional system over $\mathbb{K}[X, Y]$ is upper bounded by*

$$d_{\mathrm{reg}} \leqslant \min(n_X, n_Y) + 1.$$

In particular, this result implies that computing the Gröbner basis of generic affine bilinear zero-dimensional system with $\min(n_X, n_Y) \in \mathcal{O}(1)$ can be done in polynomial-time.

B Complexity Theorems Proofs

B.1 Proof of Theorem 4.

Proof. W.L.O.G., we can assume that $i_0 = 2$ (up to re-ordering the equations). Let λ_2 be a root of the degree-N univariate polynomial Det $\left(\mathfrak{P}^{(2)} + X \cdot \mathfrak{P}^{(1)}\right)$. We denote by $K_2 = \mathrm{Ker}\left(\mathfrak{P}^{(2)} + \lambda_2 \mathfrak{P}^{(1)}\right)$ the corresponding kernel.
We first assume that N is odd. By the genericity assumption, we know that K_2 is of dimension one. Since $\overline{s}'_{N,N} = 1$ in (8), each K_2 yields an unique $\overline{s_2}'$ (stated differently, $\overline{s_2}'$ is the vector generating K_2 in a systematic basis). There is at most $q = \mathcal{O}(n)$ distinct values for $\overline{s_2}'$. We then plug each $\overline{s_2}'$ in (9) which reduces then to a system of linear equation in the $\overline{t}'$. We know that there is at least one $\overline{s_2}'$ which leads to a consistent system. If $N < n$ is odd, we can then solve (9) in $\mathcal{O}(n^{\omega+1})$.
When N is even, the situation is very similar. The only difference is that K_2 is of dimension 2. Since $\overline{s}'_{N,N} = 1$ in (8), each K_2 yields $q = \mathcal{O}(n)$ distinct $\overline{s_2}'$. There is at most $N < n$ distinct values for $\overline{s_2}'$. As before, we plug each possible

$\overline{s_2}'$ in (9) which yields a system of linear equation in the $\overline{t}'$. Thus, if N is even, we can then solve (9) in $\mathcal{O}(n^{\omega+2})$.
Note that because of Lemma 3, the system will give a solution with probability $\frac{q-1}{q}$, so we need to randomize the public polynomials on average $\frac{q}{q-1}$ times.
The whole procedure needs to be repeated for every N starting from $n-1$ down to $r+2$. Note that in the first iteration, when $N=n$, we actually solve only a linear system of equations. □

B.2 Proof of Theorem 5.

Proof. Denote by $\binom{n}{k}_q = \frac{(q^n-1)(q^n-q)\ldots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\ldots(q^k-q^{k-1})}$ the Gaussian binomial coefficient, that gives the number of k-dimensional subspaces of an n-dimensional vector space.
The main idea of the proof is to show that in (9) it is enough to consider only two coordinates of $\overline{t}'$ in order to get a unique solution for $\overline{s}'$ with overwhelming probability. Namely, it is enough to consider only the equations corresponding to $i_0=2, i_1=3$ (w.l.o.g. up to reordering of equations):

$$\overline{s}'\left(\mathfrak{P}^{(2)}+\overline{t}'_{2,1}\mathfrak{P}^{(1)}\right)=\mathbf{0}_{1\times N}, \tag{13}$$

$$\overline{s}'\left(\mathfrak{P}^{(3)}+\overline{t}'_{3,1}\mathfrak{P}^{(1)}\right)=\mathbf{0}_{1\times N}. \tag{14}$$

For odd N, for both $i\in\{2,3\}$ we have that $\mathrm{Dim}(\mathrm{Ker}(\mathfrak{P}^{(i)}+\lambda\mathfrak{P}^{(1)}))=1$ for every $\lambda\in\mathbb{F}_q$. Denote the set $\{\mathrm{Ker}(\mathfrak{P}^{(2)}+\lambda\mathfrak{P}^{(1)})|\lambda\in\mathbb{F}_q\}$ by R_2, and the set $\{\mathrm{Ker}(\mathfrak{P}^{(3)}+\lambda\mathfrak{P}^{(1)})|\lambda\in\mathbb{F}_q\}$ by R_3. We know that, if there exists a good key, it will be a vector in the vector space that is the intersection $R_2\cap R_3$. The probability that the intersection contains another vector space by chance is $|R_1|\cdot|R_2|/\binom{N}{1}_q\approx q^{(3-N)}$, which is very small for big enough N. Similarly, for even N, there exist λ_2, λ_3 such that for both $i\in\{2,3\}$, $\mathrm{Dim}(\mathrm{Ker}(\mathfrak{P}^{(i)}+\lambda_i\mathfrak{P}^{(1)}))=2$. Now, if a good key exists, it will be in the intersection of the kernels and all other elements in the intersection will be linearly dependent of the good key. Hence, in this case the probability that we get a solution of the system that is not a good key is the same as the probability that the two kernels coincide, which equals $1/\binom{N}{2}_q\approx q^{(4-2N)}$. This again is very small. Thus, in total, with probability of $1-\frac{1}{q^{N-3}}$, it is enough to use only equations (13) and (14).
The task now reduces to solving a bilinear system of equations of bidegree $(1,1)$, over $\mathbb{F}_q[\overline{t}'_{i_0,1},\overline{t}'_{i_1,1},\overline{s}'_{1,N},\ldots,\overline{s}'_{N-1,N}]$. From Theorem 7, such system can be solved in $\mathcal{O}\left(\binom{N+4}{3}^{\omega}\right)$.
Again because of Lemma 3, we need to randomize the public polynomials on average $\frac{q}{q-1}$ times. The step of solving the system (9) needs to be repeated for every N starting from $n-1$ down to $r+2$. Note that, when $N=n$, we actually solve only a linear system of equations, which is of smaller complexity.
In total, asymptotically, since we have $\mathcal{O}(n)$ steps of complexity $\mathcal{O}(\binom{n+4}{3}^{\omega})$, we obtain the total complexity of the attack. □