Linearity Measures for $\mathcal{MQ}$ Cryptography

Simona Samardjiska [1,2] and Danilo Gligoroski [1]

Department of Telematics, NTNU, Trondheim, Norway,[1]
FCSE, UKIM, Skopje, Macedonia.[2]
simonas@item.ntno.no,simona.samardjiska@finki.ukim.mk, danilog@item.ntno.no

Abstract. We propose a new general framework for the security of multivariate quadratic ($\mathcal{MQ}$) schemes with respect to attacks that exploit the existence of linear subspaces. We adopt linearity measures that have been used traditionally to estimate the security of symmetric cryptographic primitives, namely the nonlinearity measure for vectorial functions introduced by Nyberg at Eurocrypt '92, and the (s,t)–linearity measure introduced recently by Boura and Canteaut at FSE'13. We redefine some properties of $\mathcal{MQ}$ cryptosystems in terms of these known symmetric cryptography notions, and show that our new framework is a compact generalization of several known attacks in $\mathcal{MQ}$ cryptography against single field schemes. We use the framework to explain various pitfalls regarding the successfulness of these attacks. Finally, we argue that linearity can be used as a solid measure for the susceptibility of $\mathcal{MQ}$ schemes to these attacks, and also as a necessary tool for prudent design practice in $\mathcal{MQ}$ cryptography.

Keywords Strong (s,t)–linearity, (s,t)–linearity, MinRank, good keys, separation keys

1 Introduction

In the past two decades, as a result of the advancement in quantum algorithms, the crypto community showed increasing interest in algorithms that would be potentially secure in the post quantum world. One of the possible alternatives are multivariate quadratic ($\mathcal{MQ}$) public key cryptosystems based on the NP-hard problem of solving quadratic polynomial systems of equations over finite fields.

Many different $\mathcal{MQ}$ schemes emerged over the years most of which fall into two main categories - single field schemes including UOV (Unbalanced Oil and Vinegar) [1], Rainbow [2], TTM (Tame Transformation Method) [3], STS (Stepwise Triangular System) [4], MQQ-SIG (Multivariate Quadratic Quasigroups - Signature scheme) [5], TTS (Tame Transformation Signatures) [6], EnTTS (Enhanced TTS) [7] and mixed field schemes including C* [8], SFLASH [9], HFE (Hidden Field Equation) [10], MultiHFE [11,12], QUARTZ [13]. Unfortunately, over the years, most of them have been successfully cryptanalysed [14,15,4,16,17]. Three major types of attacks have proven devastating for $\mathcal{MQ}$ cryptosystems:

i. MinRank attacks – based on the problem of finding a low rank linear combination of matrices, known as MinRank [18]. Although NP-hard, the instances of MinRank arising from $\mathcal{MQ}$ schemes are often easy, and provide a powerful tool against single field schemes [14,4].

ii. Equivalent Keys attacks – based on finding an equivalent key for the respective scheme. The concept was introduced by Wolf and Preneel [19], and later further developed by Thomae and Wolf [16] to the generalization of good keys. The attacks on TTM [14], STS [4,16], HFE and MultiHFE [15,17] can all be seen from this perspective.
iii. Differential attacks – based on specific invariants of the differential of a given public key, such as the dimension of the kernel, or some special symmetry. It was introduced by Fouque *et al.* in [20] to break the perturbed version of the C^* scheme PMI [21], and later also used in [22,23,24,25].

Interestingly, the history of $\mathcal{MQ}$ cryptography has witnessed cases where, despite the attempt to inoculate a scheme against some attack, the enhanced variant has fallen victim to the same type of attacks. Probably the most famous example is the SFLASH [9] signature scheme, that was build using the minus modifier on the already broken C^* [26], and selected by the NESSIE European Consortium [27] as one of the three recommended public key signature schemes. It was later broken by Dubois *et al.* in [24,25] using a similar differential technique as in the original attack on C^*. Another example is the case of Enhanced STS [28], which was designed to be resistant to rank attacks, that broke its predecessor STS. Even the authors themselves soon realized that this was not the case, and the enhanced variant is vulnerable to a HighRank attack.

Such examples indicate that the traditional "break and patch" practice in $\mathcal{MQ}$ cryptography should be replaced by a universal security framework. Indeed, in the last few years, several proposals have emerged that try to accomplish this [29,30,31]. Notably, the last two particularly concentrate on the properties of the differential of the used functions, a well known cryptanalytic technique from symmetric cryptography. We will show here that another well known measure from symmetric cryptography, namely linearity, is fundamental for the understanding of the security of $\mathcal{MQ}$ schemes.

1.1 Our Contribution

We propose a new general framework for the security of $\mathcal{MQ}$ schemes with respect to attacks that exploit the existence of linear subspaces. Our framework is based on two linearity measures that we borrow from symmetric cryptography, and adopt them suitably in the context of $\mathcal{MQ}$ cryptography. To our knowledge, this is the first time that the notion of linearity has been used to analyse the security of $\mathcal{MQ}$ schemes.

In particular, we take the linearity measure for vectorial functions introduced by Nyberg [32] already in 1992, and the (s,t)–linearity measure introduced recently by Boura and Canteaut [33] at FSE'13. We extend the first to a new notion of strong (s,t)–linearity in order to include an additional important parameter of the size of the vector subspace of the components of the function that have common linear space. We show that strong (s,t)–linearity and (s,t)–linearity are intrinsically connected to the security of $\mathcal{MQ}$ schemes, and can be used to explain almost all attacks on single field schemes, such as rank attacks, good keys attacks and attacks on oil and vinegar schemes. Indeed this is possible, since all these attacks share a common characteristic: They try to recover a subspace with respect to which the public key of an $\mathcal{MQ}$ scheme is linear. Therefore they can all be considered as linear attacks on $\mathcal{MQ}$ schemes.

We devise two generic attacks that separate the linear subspaces, and that are a generalization of the aforementioned known attacks. We present one of the possible modellings of the attacks using system solving techniques, although other techniques are possible as well. Using the properties of strong (s,t)–linearity and (s,t)–linearity, we show what are the best strategies for the attacks. Notably, the obtained systems of equations are equivalent to those that can be obtained using good keys [16], a technique based on equivalent keys and missing cross terms. By this we show that our new framework provides a different, elegant perspective on why good keys exist, and why they are so powerful in cryptanalysis. Furthermore, we use our framework to explain various pitfalls regarding design choices of $\mathcal{MQ}$ schemes and the successfulness of the linear attacks against them. Finally, we argue that linearity can be used as a solid measure for the susceptibility of $\mathcal{MQ}$ schemes to linear attacks, and also as a necessary tool for prudent design practice in $\mathcal{MQ}$ cryptography.

1.2 Organization of the Paper

The paper is organized as follows. In Section 2 we briefly introduce the design principles of $\mathcal{MQ}$ schemes and also recall the well known measure of nonlinearity of functions. In the next Section 3, we introduce the notion of strong (s,t)–linearity, which is basically an extension of the standard linearity measure and review the recently introduced (s,t)–linearity measure. In Sections 4 and 5 we show how the two linearity measures fit in the context of $\mathcal{MQ}$ cryptography. Some discussion on the matter proceeds in Section 6, and the conclusions are presented in Section 7.

2 Preliminaries

Throughout the text, $\mathbb{F}_q$ will denote the finite field of q elements, where $q = 2^d$, and $a = (a_1, \ldots, a_n)^\intercal$ will denote a vector from $\mathbb{F}_q^n$.

2.1 Vectorial Functions and Quadratic Forms

Definition 1. *Let n, m be two positive integers. The functions from $\mathbb{F}_q^n$ to $\mathbb{F}_q^m$ are called (n,m) functions or vectorial functions. For an (n,m) function $f = (f_1, \ldots, f_m)$, f_i are called the coordinate functions of f.*

Classically, a quadratic form

$$f(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} \gamma_{ij} x_i x_j : \mathbb{F}_q^n \to \mathbb{F}_q$$

can be written as $x^\intercal \mathfrak{F} x$ using its matrix representation $\mathfrak{F}$. This matrix is constructed differently depending on the parity of the field characteristic. In odd characteristic, $\mathfrak{F}$ is chosen to be a symmetric matrix, where $\mathfrak{F}_{ij} = \gamma_{ij}/2$ for $i \neq j$ and $\mathfrak{F}_{ij} = \gamma_{ij}$ for $i = j$. Over fields $\mathbb{F}_q$ of even characteristic $\mathfrak{F}$ can not be chosen in this manner, since $(\gamma_{ij} + \gamma_{ji}) x_i x_j = 0$ for $i \neq j$. Instead, let $\widetilde{\mathfrak{F}}$ be the uniquely defined upper-triangular representation of f, *i.e.,* $\widetilde{\mathfrak{F}}_{ij} = \gamma_{ij}$ for $i \le j$. Now, we obtain a symmetric form by $\mathfrak{F} := \widetilde{\mathfrak{F}} + \widetilde{\mathfrak{F}}^\intercal$. Note that, in this case *only* the upper-triangular part represents the according polynomial and $\mathfrak{F}$ is always of even rank.

2.2 $\mathcal{MQ}$ Cryptosystems

The public key of a $\mathcal{MQ}$ cryptosystem is usually given by an (n, m) function $\mathcal{P}(x) = (p_1(x), \ldots, p_m(x)) : \mathbb{F}_q^n \to \mathbb{F}_q^m$, where

$$p_s(x) = \sum_{1 \leq i \leq j \leq n} \widetilde{\gamma}_{ij}^{(s)} x_i x_j + \sum_{i=1}^{n} \widetilde{\beta}_i^{(s)} x_i + \widetilde{\alpha}^{(s)}$$

for every $1 \leqslant s \leqslant m$, and where $x = (x_1, \ldots, x_n)^\intercal$.
The public key $\mathcal{P}$ is obtained by masking a structured central (n, m) function $\mathcal{F} = (f_1, \ldots, f_m)$ using two secret linear transformations $S, T \in \mathrm{GL}_n(\mathbb{F}_q)$ and defined as $\mathcal{P} = T \circ \mathcal{F} \circ S$. We denote by $\mathfrak{P}^{(s)}$ and $\mathfrak{F}^{(s)}$ the $(n \times n)$ matrices describing the homogeneous quadratic part of p_s and f_s, respectively.

Example 1.

i. The internal map of UOV [1] is defined as $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, with central polynomials

$$f_s(x) = \sum_{i \in V, j \in V} \gamma_{ij}^{(s)} x_i x_j + \sum_{i \in V, j \in O} \gamma_{ij}^{(s)} x_i x_j + \sum_{i=1}^{n} \beta_i^{(s)} x_i + \alpha^{(s)}, \tag{1}$$

for every $s = 1 \ldots m$, where $n = v + m$, $V = \{1, \ldots, v\}$ and $O = \{v + 1, \ldots, n\}$ denote the index sets of the vinegar and oil variables, respectively. The public map $\mathcal{P}$ is obtained by $\mathcal{P} = \mathcal{F} \circ \mathcal{S}$, since the affine $\mathcal{T}$ is not needed (Indeed, any component $w^\intercal \cdot \mathcal{F}$ has again the form 1).

ii. The internal map $\mathcal{F} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ of C^* [8] is defined by

$$\mathcal{F}(x) = x^{2^\ell + 1}, \text{where} \gcd(2^\ell + 1, 2^n - 1) = 1.$$

This condition ensures that $\mathcal{F}$ is bijective.

iii. The representatives of the family of Stepwise Triangular Systems (STS) [4] have an internal map $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ defined as follows. Let L be the number of layers, and let $r_i, 0 \leq i \leq L$ be integers such that $0 = r_0 < r_1 < \cdots < r_L = n$. The central polynomials in the k-th layer are defined by

$$f_i(x_1, \ldots, x_n) = f_i(x_1, \ldots, x_{r_k}), \quad r_{k-1} + 1 \leq i \leq r_k.$$

We describe briefly two important cryptanalytic tools in $\mathcal{MQ}$ cryptography, that are of particular interest for us.

The MinRank Problem The problem of finding a low rank linear combination of matrices is a known NP-hard linear algebra problem [34] known as MinRank in cryptography [18]. It has been shown that it underlies the security of several $\mathcal{MQ}$ cryptographic schemes [14,4,15]. It is defined as follows.
MinRank $MR(n, r, k, M_1, \ldots, M_k)$
Input: $n, r, k \in \mathbb{N}$, where $M_1, \ldots, M_k \in \mathcal{M}_{n \times n}(\mathbb{F}_q)$.
Question: Find – if any – a k-tuple $(\lambda_1, \ldots, \lambda_k) \in \mathbb{F}_q^k \setminus \{(0, 0, \ldots, 0)\}$ such that:

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

Good Keys The concept of equivalent keys formally introduced by Wolf and Preneel in [35] is fundamentally connected to the security of $\mathcal{MQ}$ schemes. In essence, any key that preserves the structure of the secret map is an equivalent key. This natural notion was later generalized by Thomae and Wolf [16] to the concept of *good keys* that only preserve some of the structure of the secret map. Good keys improve the understanding of the level of applicability of MinRank against $\mathcal{MQ}$ schemes, and are a powerful tool for cryptanalysis. Good keys are defined as follows.

Let $k, 1 \leq k \leq m$ and $\mathcal{F} = \{f_1, \ldots, f_m\}$ be a set of polynomials of $\mathbb{F}_q[x_1, \ldots, x_n]$. Let $I^{(k)} \subseteq \{x_i x_j \,|\, 1 \leq i \leq j \leq n\}$ be a subset of the degree-2 monomials, and let $\mathcal{F}\big|_I = \{f_1\big|_{I^{(1)}}, \ldots, f_m\big|_{I^{(m)}}\}$ where $f_k\big|_{I^{(k)}} := \sum_{x_i x_j \in I^{(k)}} \gamma_{ij}^{(k)} x_i x_j$.

Definition 2 ([16]). *Let* $(\mathcal{F}, S, T), (\mathcal{F}', S', T') \in \mathbb{F}_q[x_1, \ldots, x_n]^m \times \mathrm{GL}_n(\mathbb{F}_q) \times \mathrm{GL}_m(\mathbb{F}_q)$ *Let also* $J^{(k)} \subsetneq I^{(k)}$ *for all* $k, 1 \leq k \leq m$ *with at least one* $J^{(k)} \neq \emptyset$. *We call* $(\mathcal{F}', S', T') \in \mathbb{F}_q[x_1, \ldots, x_n]^m \times \mathrm{GL}_n(\mathbb{F}_q) \times \mathrm{GL}_m(\mathbb{F}_q)$ *a* good key *of* $(\mathcal{F}, S, T)$ *if and only if:*

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

2.3 Linearity of Vectorial Functions

Linearity is one the most important measures for the strength of an (n, m) function for use in symmetric cryptoprimitives. We provide here some well known results about this notion.

Definition 3 ([32]). *The linearity of an* (n, m) *function* f *is measured using its Walsh transform, and is given by*

$$\mathcal{L}(f) = \max_{w \in \mathbb{F}_q^m \setminus \{0\}, u \in \mathbb{F}_q^n} \left| \sum_{x \in \mathbb{F}_q^n} (-1)^{w^\intercal \cdot f(x) + u^\intercal \cdot x} \right|$$

The nonlinearity of an (n, m) *function* f *is the Hamming distance between the set of nontrivial components* $\left\{w^\intercal \cdot f | w \in \mathbb{F}_q^m \setminus \{0\}\right\}$ *of* f *and the set of all affine functions. It is given by*

$$\mathcal{N}(f) = (q-1)(q^{n-1} - \frac{1}{q}\mathcal{L}(f)).$$

Definition 4. *A vector* $w \in \mathbb{F}_q^n$ *is called a linear structure of an* (n, m) *function* f *if the derivative* $D_w f(x) = f(x + w) - f(x)$ *is constant,* i.e., *if*

$$f(x + w) - f(x) = f(w) - f(0)$$

for all $x \in \mathbb{F}_q^n$. *The space generated by the linear structures of* f *is called the linear space of* f.

Nyberg [32] proved the following results.

Proposition 1 ([32]). *The dimension of the linear space of an (n, m) function is invariant under bijective linear transformations of the input space and of the coordinates of the function.*

Proposition 2 ([32]). *Let $x^{\intercal}\mathfrak{F}x$ be the matrix representation of a quadratic form f. Then, the linear structures of f form the linear subspace* $\mathrm{Ker}(\mathfrak{F})$.

The linear structures can provide a measure for the distance of the quadratic forms from the set of linear forms. Indeed the link is given by the following theorem.

Theorem 1 ([32]).

1. *Let $x^{\intercal}\mathfrak{F}x$ be the matrix representation of a quadratic form f, and let* $\mathrm{Rank}(\mathfrak{F}) = r$. *Then the linearity of f is $\mathcal{L}(f) = q^{n-\frac{r}{2}}$.*
2. *Let f be a quadratic (n, m) function, and let $x^{\intercal}\mathfrak{F}_w x$ denote the matrix representation of a component $w^{\intercal} \cdot f$. Then the linearity of f is $\mathcal{L}(f) = q^{n-\frac{r}{2}}$, where $r = \min\{\mathrm{Rank}(\mathfrak{F}_w) | w \in \mathbb{F}_q^m\}$.*

It is well known that the linearity of an (n, m) function is bounded from below by the value $\mathcal{L}(f) \geqslant q^{\frac{n}{2}}$, known as the covering radius bound. It is tight for every even n, and functions that reach the bound are known as *bent* functions. It is also known, from [36] that bent functions exist only for $m \leqslant n/2$. A class of quadratic bent functions that has been extensively studied in the literature is the class of Maiorana-McFarland bent functions [37]. In general, an (n, m) function from the Maiorana-McFarland class has the form $f = (f_1, f_2, \ldots, f_m) : \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}} \to \mathbb{F}_2^m$ where each of the components f_i is

$$f_i(x, y) = L(\pi_i(x)y) + g_i(x), \tag{2}$$

where π_i are functions on $\mathbb{F}_{2^{n/2}}$, L is a linear function onto $\mathbb{F}_2^m$ and g_i are arbitrary $(n/2, m)$ functions. Nyberg [36] showed that f is an (n, m)-bent function if every nonzero linear combination of the functions $\pi_i, i \in \{1, \ldots, m\}$ is a permutation on $\mathbb{F}_{2^{n/2}}$.

Since the minimum linearity (maximum nonlinearity) is achieved only for $m \leqslant n/2$, permutations can not reach the covering radius bound. But, they can reach the Sidelnikov-Chabaud-Vaudenay (SCV) bound [38], valid for $m \geq n - 1$, which for $m = n$ odd, can be stated as: $\mathcal{L}(f) \geqslant q^{\frac{n+1}{2}}$. (n, n) functions, where n is odd, that reach the SCV bound with equality, are called Almost bent (AB) functions.

As a direct consequence of Theorem 1 and the aforementioned bounds we have that quadratic (n, m) functions are

i. bent if and only if $\mathrm{Rank}(\mathfrak{F}_w) = n$ for every $w^{\intercal} \cdot f$,
ii. almost bent if and only if $\mathrm{Rank}(\mathfrak{F}_w) = n - 1$ for every $w^{\intercal} \cdot f$.

3 Strong (s, t)–linearity and (s, t)–linearity

We will show in the next sections that linearity plays a significant role for the security of $\mathcal{MQ}$ cryptosystems. However, in order to better frame it for use in $\mathcal{MQ}$ cryptography, we introduce the following notion of strong (s, t)–linearity. The motivation for this more precise measure comes from the recently introduced notion of (s, t)–linearity [33], that will also be discussed here in the context of $\mathcal{MQ}$ cryptography.

Definition 5. *Let f be an (n, m) function. Then, f is said to be strongly (s, t)–linear if there exist two linear subspaces $V \subset \mathbb{F}_q^n$, $W \subset \mathbb{F}_q^m$ with $\mathrm{Dim}(V) = s$, $\mathrm{Dim}(W) = t$ such that for all $w \in W$, V is a subspace of the linear space of $w^\intercal \cdot f$.*

Compared to the standard measure for linearity given in Definition 3, that actually measures the size of the vector space V, strong (s, t)–linearity also measures the size of the vector space W. We will see that this is particularly important in the case of $\mathcal{MQ}$ cryptosystems. We next provide some basic properties about strong (s, t)–linearity.

Proposition 3. *If a function is strongly (s, t)–linear, then it is also strongly $(s-1, t)$–linear, and strongly $(s, t-1)$–linear.*

Proposition 4. *Let f be an quadratic (n, m) function and $V \subset \mathbb{F}_q^n$ and $W \subset \mathbb{F}_q^m$ with $\mathrm{Dim}(V) = s$, $\mathrm{Dim}(W) = t$ be two linear spaces. Then f is strongly (s, t)–linear with respect to V, W if and only if the function f_W corresponding to all components $w^\intercal \cdot f$, $w \in W$ can be written as*

$$f_W(x, y) = g_W(x) + L_W(y)$$

where $\mathbb{F}_q^n$ is the direct sum of U and V, g_W is a quadratic function from U to $\mathbb{F}_q^t$ and L_W is a linear function from V to $\mathbb{F}_q^t$.

Proof. From Definition 5, f is strongly (s, t)–linear with respect to V, W if and only if V is a subspace of the linear space of $w^\intercal \cdot f$, for all $w \in W$. Now, for w a basis vector of W, $w^\intercal \cdot f$ can be written as $w^\intercal \cdot f(x, y) = g_w(x) + L_w(y)$ where $y \in V$ belongs to the linear space of $w^\intercal \cdot f$. Combining all the components for a basis of W we obtain the desired form.

Proposition 5. *Let f be a quadratic (n, m) function. Then f is strongly (s, t)–linear with respect to V, W if and only if the function f_W corresponding to all components $w^\intercal \cdot f$, $w \in W$ is such that all its derivatives $D_a w^\intercal \cdot f$, with $a \in V$ are constant.*

Recently, Boura and Canteaut [33] introduced a new measure for the propagation of linear relations through S-boxes, called (s, t)-linearity.

Definition 6 ([33]). *Let f be an (n, m) function. Then, f is said to be (s, t)–linear if there exist two linear subspaces $V \subset \mathbb{F}_q^n$, $W \subset \mathbb{F}_q^m$ with $\mathrm{Dim}(V) = s$, $\mathrm{Dim}(W) = t$ such that for all $w \in W$, $w^\intercal \cdot f$ has degree at most 1 on all cosets of V.*

Similarly as for strong (s, t)–linearity, it is true that

Proposition 6 ([33]). *If a function is (s, t)–linear, then it is also $(s-1, t)$–linear, and $(s, t-1)$–linear.*

Boura and Canteaut [33] proved that any (s, t)–linear function "contains" a function of the Maiorana-McFarland class, in the following sense.

Proposition 7 ([33]). *Let f be an (n, m) function and $V \subseteq \mathbb{F}_q^n$ and $W \subseteq \mathbb{F}_q^m$ with $\mathrm{Dim}(V) = s$, $\mathrm{Dim}(W) = t$ be two linear spaces. Then f is (s, t)–linear with respect to*

V, W if and only if the function f_W corresponding to all components $w^\intercal \cdot f$, $w \in W$ can be written as

$$f_W = M(x) \cdot y + G(x)$$

where $\mathbb{F}_q^n$ is the direct sum of U and V, G is a function from U to $\mathbb{F}_q^t$ and $M(x)$ is a $t \times s$ matrix whose coefficients are functions defined on U.

A useful characterization of (s,t)–linearity, resulting from the properties of the Maiorana-McFarland class is through second order derivatives defined by $D_{a,b}f = D_aD_bf = D_bD_af$.

Proposition 8 ([33]). *Let f be an (n,m) function. Then f is (s,t)–linear with respect to V, W if and only if the function f_W corresponding to all components $w^\intercal \cdot f$, $w \in W$ is such that all its second order derivatives $D_{a,b}w^\intercal \cdot f$, with $a, b \in V$ vanish.*

The two measures of linearity, even though they measure different linear subspaces are also interconnected. The following two propositions illustrate this connection.

Proposition 9. *If a function is strongly (s,t)–linear, then it is also (s,t)–linear.*

Proposition 10. *If a quadratic (n,m) function f is $(\lceil \frac{n}{2} \rceil + s, 1)$–linear than it is strongly $(2s,1)$–linear.*

Proof. From Proposition3 [33] we have the fact that a $(s,1)$–linear function has linearity $\mathcal{L}(f) \geqslant q^s$ (This comes from the fact that the linearity of a function is lower bounded by the linearity of any of its components.) Thus, if a quadratic (n,m) function is $(\lceil \frac{n}{2} \rceil + s, 1)$–linear, then $\mathcal{L}(f) \geqslant q^{\lceil \frac{n}{2} \rceil + s}$. From Theorem1 $\mathcal{L}(f) = q^{n - \frac{r}{2}}$, where $r = \min\{\text{Rank}(\mathfrak{F}_w) | w \in \mathbb{F}_q^m\}$. From here $n - \frac{r}{2} \geqslant \lceil \frac{n}{2} \rceil + s$ and further $n - 2s \geqslant r$. Hence f is strongly $(2s,1)$–linear.

In the next two sections we will provide a general framework for the security of $\mathcal{MQ}$ schemes against linear cryptanalysis using the notions of strong (s,t)–linearity and (s,t)–linearity.

4 The strong (s,t)–linearity measure for $\mathcal{MQ}$ systems

In this section, we show that strong (s,t)–linearity is fundamentally connected to the susceptibility of an $\mathcal{MQ}$ scheme to MinRank attacks and good keys attacks.

From Proposition 2 we have the following theorem.

Theorem 2. *Let $f = (f_1, f_2, \ldots, f_m)$ be a quadratic (n,m) function, and let $\mathfrak{F}_1, \mathfrak{F}_2, \ldots, \mathfrak{F}_m$ be the matrix representations of the coordinates of f.*

Then the MinRank problem $MR(n, r, m, \mathfrak{F}_1, \mathfrak{F}_2, \ldots, \mathfrak{F}_m)$ has a solution if and only if f is strongly $(n-r, 1)$–linear.

Proof. We can see that $v = (v_1, \ldots, v_n) \in \mathbb{F}_q^n \setminus \{0\}$ is a solution to the MinRank problem $MR(n, r, m, \mathfrak{F}_1, \mathfrak{F}_2, \ldots, \mathfrak{F}_m)$ if and only if

$$\text{Rank}\left(\sum_{i=1}^{n} v_i \mathfrak{F}_i\right) \leqslant r,$$

that is, if and only if $\text{Dim}\left(\text{Ker}\left(\sum_{i=1}^{n} v_i \mathfrak{F}_i\right)\right) \geqslant n-r$, *i.e.,* from Proposition 2, if and only if $v^\intercal \cdot f$ has at least $n-r$ linearly independent linear structures. Taking W to be the space generated by the vector v and V to be the linear space of $v^\intercal \cdot f$, from Definition 5 the last is equivalent to f being strongly $(n-r,1)$–linear.

Example 2. From Theorem 2 it is clear that bent functions are resistant to MinRank attacks, since no linear combination of the components of the function has smaller rank than n. Thus, regarding MinRank attacks, bent functions are optimal for use as a secret map in $\mathcal{MQ}$ cryptosystems.

Example 3. Regarding encryption $\mathcal{MQ}$ schemes, a natural conclusion would be that AB permutations are the most suitable for use. One of the most scrutinized AB permutations are the Gold functions defined over $\mathbb{F}_{q^n}$ for odd n by:

$$f(x) = x^{q^\ell+1},\ \gcd(q^\ell+1, q^n-1) = 1,\ \gcd(\ell, n) = 1$$

where the first condition guarantees balancedness, and the second AB-ness. Notably, one of the most famous $\mathcal{MQ}$ schemes, the C^* scheme, uses an AB function, although there are variants that do not meet the second condition [21].

As mentioned before, AB functions have $\text{Rank}(\mathfrak{F}_v) = n-1$ for any component $v^\intercal \cdot f$. This means that each of the components have a linear space of dimension 1, and no two components share a linear space, *i.e.,* AB functions are only strongly $(1,1)$–linear. Hence, MinRank for $r = n-1$ is trivially satisfied and does not reveal anything more about the structure of the map.

The example of Gold functions from Example 3 implies that although MinRank on its own can be a good indicator of a weakness in a scheme, it does not provide a sufficient condition for mounting a successful attack. A better framework for the applicability of MinRank is provided by the concept of good keys (cf. Section2.2). It should be emphasized that the definition of good keys (Definition 2), does not explicitly state the structure that is being preserved, thus, providing a framework even for structures not yet discovered. On the other hand, the motivation for good keys comes from the Rainbow band separation attack [39], that exploits (among others) a particular weakness connected to the presence of linear structures in the secret map. Moreover, known attacks that use MinRank, as well as other applications of good keys, again take advantage of the same property. Hence, we give a new definition for the special type of keys that separate the space of linear structures. This definition comes as a direct consequence of strong (s,t)–linearity. Later, we will also take a look at another weakness that the Rainbow band separation attack and its generalizations take advantage of, and we will also define the corresponding keys. We will call both types of keys *separation keys*.

Let V be a subspace of $\mathbb{F}_q^n$ of dimension $k \leq n$, and let S_V be an invertible matrix such that k of its rows form a basis of V. We note that the rest of the columns of the matrix can be arbitrary, as long as the matrix is invertible.

Definition 7. *Let* $(\mathcal{F}, S, T), (\mathcal{F}', S', T') \in \mathbb{F}_q[x_1, \ldots, x_n]^m \times \mathrm{GL}_n(\mathbb{F}_q) \times \mathrm{GL}_m(\mathbb{F}_q)$ *and let* $\mathcal{P} = T \circ \mathcal{F} \circ S = T' \circ \mathcal{F}' \circ S'$. *We call* $(\mathcal{F}', S', T')$ *a* strong (s,t) separation key *for* $\mathcal{P}$ *if* $\mathcal{P}$ *is strongly* (s,t)*–linear with respect to two spaces* V *and* W, $\mathrm{Dim}(V) = s$, $\mathrm{Dim}(W) = t$ *and*

$$S' = S_V^{\intercal}, \quad T' = T_W.$$

A strong (s,t) separation key separates the components of the public key that have a non empty common linear space. As a direct consequence of Definition 7 we have that:

Proposition 11. *If* $(\mathcal{F}', S', T')$ *is a strong* (s,t) *separation key for* $\mathcal{P}$, *then it is also a good key for* $\mathcal{P}$.

Many $\mathcal{MQ}$ cryptosystems, proposed so far have strong separation keys. As mentioned before, Rainbow [2] is one of the examples, but also all STS cryptosystems ([3,4]), and all $\mathcal{MQ}$ cryptosystem that combine a layered structure with other types of design principles, including among others Branched C^* [40], MQQ-SIG [5], TTS [6], EnTTS [7], MFE [41]. Table 1 summarizes the different strong separation keys for some of these schemes.

Table 1. Examples of strong (s,t) separation keys for some $\mathcal{MQ}$ cryptosystems

scheme	parameters	strong (s,t) separation keys
Branch.C^*	$(n_1, \ldots, n_b)$	$(\sum_i n_i, n - \sum_i n_i)$
STS	$(r_1, \ldots, r_L)$	$(n - r_k, r_k)$, $k = 1, \ldots, L-1$
Rainbow	$(v_1, o_1, o_2) = (18, 12, 12)$	$(12, 12)$
MQQ-SIG	$(q, d, n, r) = (2, 8, 160, 80)$	$(k, 80-k)$, $k = 1, \ldots, 79$
MFE	$(q^k, n, m) =$	$(2k, 10k)$, $(4k, 4k)$,
	$((2^{256})^k, 12, 15)$	$(6k, 2k)$, $(8k, k)$
EnTTS	$(n, m) = (32, 24)$	$(10, 14)$,$(14, 10)$

The known attacks on these systems, can all be considered as separation key attacks involving different techniques and optimizations. The framework of strong (s,t) linearity provides a unified way of looking at these attacks, and a *single* measure that can be used as criteria for the parameters of schemes that have strong separation keys. The next two theorems explain in detail how to mount a generic strong separation key attack, what is the complexity of the attack, and what is the best strategy for attack when the existence of a strong separation key is known. We decided to present the attack by representing the conditions for strong (s,t) linearity as systems of equations. In this way we obtain completely equivalent systems to the ones that can be obtained using good keys, thus, offering another elegant point of view on why good keys exist. Note that this is not the only technique that can be used to recover strong (s,t) separation keys (for example we can use probabilistic approach). However, it provides a clear picture of the cases when the existence of a particular strong separation key is devastating for the security of $\mathcal{MQ}$ schemes.

Theorem 3. *Let it be known that a strong* (s,t) *separation key exists for a given* $\mathcal{MQ}$ *public key* $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ *with matrix representations* $\mathfrak{P}_w$ *of a component* $w^{\intercal} \cdot \mathcal{P}$.

i. The task of finding a strong (s,t) separation key $(S_V^\intercal, T_W)$ is equivalent to solving the system of bilinear equations

$$\mathfrak{P}_{w^{(i)}} \cdot a^{(j)} = 0,\ i \in \{1,\dots,t\},\ j \in \{1,\dots,s\}, \tag{3}$$

in the unknown basis vectors $w^{(i)}$ of the space W, and the unknown basis vectors $a^{(j)}$ of the space V.

ii. The complexity of recovering the strong (s,t) separation key through solving the system (3) is

$$\mathcal{O}\left(t \cdot s \cdot n \cdot \binom{(n-s)s + (m-t)t + d_{reg}}{d_{reg}}^{\omega}\right) \tag{4}$$

where $d_{reg} = \min\{(n-s)s+(m-t)t\}+1$, and $2 \leqslant \omega \leqslant 3$ is the linear algebra constant.

Proof. i. From Definition7 the existence of a strong (s,t) separation key $(S_V^\intercal, T_W)$ means that $\mathcal{P}$ is strongly (s,t)–linear with respect to two spaces V, W of dimension $\mathrm{Dim}(V) = s, \mathrm{Dim}(W) = t$. So the task is to recover these two spaces, *i.e.,* to recover some bases $\{a^{(1)},\dots,a^{(s)}\}$ and $\{w^{(1)},\dots,w^{(t)}\}$ of V and W respectively. From Definition 5 and Proposition 2, $w \in W$ and $a \in V$ if and only if a is in the kernel of $\mathfrak{P}_w$, *i.e.,* if and only if $\mathfrak{P}_w \cdot a = 0$. Let the coordinates of the basis vectors $\{a^{(1)},\dots,a^{(s)}\}$ and $\{w^{(1)},\dots,w^{(t)}\}$ be unknowns. In order to insure that they are linearly independent, we fix the last s coordinates of $a^{(j)}$ to 0 except the $(n-j+1)$-th coordinate that we fix to 1, and similarly we fix the first t coordinates of $w^{(i)}$ to 0 except the i-th coordinate that we fix to 1. In this way we can form the bilinear system (3). The solution of the system will yield the unknown bases of U and W. Note that if we get more than one solution, any of the obtained solutions will suffice. However, it can also happen that the system has no solutions. This is due to the fixed coordinates in the basis vectors, which can be done in the particular manner with probability of approximately $(1-\frac{1}{q-1})^2$. Still, if no solutions, we can randomize the function $\mathcal{P}$ by applying linear transformation to the input space and the coordinates of the function, since from Prop 1, this preserves the strong (s,t)–linearity of $\mathcal{P}$.

ii. From i., the system (3) consists of $t \cdot s \cdot n$ bilinear equations in two sets of variables of sizes $\nu_1 = (n-s)s$ and $\nu_2 = (m-t)t$, bilinear with respect to each other. The best known estimate of the complexity of solving a random system of bilinear equations is due to Faugere *et al.* [42], which says that for the grevlex ordering, the degree of regularity of a generic affine bilinear zero-dimensional system over a finite field is upper bounded by

$$d_{reg} \leq \min(\nu_1, \nu_2) + 1. \tag{5}$$

Now, we use the F_5 algorithm for computing a grevlex Gröbner basis of a polynomial system [43,44], that has a complexity of

$$\mathcal{O}\left(\mu \cdot \binom{\nu_1 + \nu_2 + d_{reg}}{d_{reg}}^{\omega}\right), \tag{6}$$

for solving a system of $\nu_1 + \nu_2$ variables and μ equations ($2 \leqslant \omega \leqslant 3$ is the linear algebra constant). Using (5) and (6), we obtain the complexity given in (4).

The complexity given in (4) is clearly not polynomial, since d_{reg} depends on n. However, it can be substantially improved using the properties of strong (s,t)–linearity from Proposition 3. This is shown in the next theorem.

Theorem 4. *Let it be known that a strong (s,t) separation key exists for a given $\mathcal{MQ}$ public key $\mathcal{P}: \mathbb{F}_q^n \to \mathbb{F}_q^m$ with matrix representations $\mathfrak{P}_w$ of a component $w^\intercal \cdot \mathcal{P}$.*

i. The task of finding a strong (s,t) separation key can be reduced to
1. Solving the system of bilinear equations

$$\mathfrak{P}_w^{(i)} \cdot a^{(j)} = 0,\ i \in \{1,\dots,c_1\},\ j \in \{1,\dots,c_2\}, \tag{7}$$

in the unknown basis vectors $w^{(i)}$ of the space W, and the unknown basis vectors $a^{(j)}$ of the space V, where $c_!, c_2$ are small integers chosen appropriately.
2. Solving the system of linear equations

$$\begin{aligned} &\mathfrak{P}_w^{(i)} \cdot a^{(j)} = 0,\ i \in \{c_1+1,...,t\},\ j \in \{1,...,c_2\}, \\ &\mathfrak{P}_w^{(i)} \cdot a^{(j)} = 0,\ i \in \{1,...,c_1\},\ j \in \{c_2+1,...,s\}, \end{aligned} \tag{8}$$

in the unknown basis vectors $w^{(i)}$, $i \in \{c_1+1,\dots,t\}$ of the space W, and the unknown basis vectors $a^{(j)}$, $j \in \{c_2+1,\dots,s\}$ of the space V.

ii. The complexity of recovering the strong (s,t) separation key using the procedure from i. is

$$\mathcal{O}\binom{(n-s)c_2 + (m-t)c_1 + d_{reg}}{d_{reg}}^{\omega} \tag{9}$$

where $d_{reg} = \min\{(n-s)c_2, (m-t)c_1\}$.

Proof. i. The crucial observation that enables us to prove this part, is a consequence of Proposition 3. Recall that it states that strong (s,t)–linearity implies strong $(s-1,t)$ and strong $(s,t-1)$–linearity. Even more, if $\mathcal{P}$ is strongly (s,t)–linear, with respect to $V = Span\{a^{(1)},\dots,a^{(s)}\}$, $W = Span\{w^{(1)},\dots,w^{(t)}\}$, then it is strongly $(s-1,t)$–linear with respect to V_1, W, where $V_1 \subset V$, and strongly $(s,t-1)$–linear with respect to V, W_1, where $W_1 \subset W$. Hence, there exist two arrays of subspaces $V \supset V_1 \supset \cdots \supset V_{s-1}$ and $W \supset W_1 \supset \cdots \supset W_{t-1}$, such that $\mathcal{P}$ is strongly $(s-i,t-j)$–linear with respect to $V_i = Span\{a^{(1)},\dots,a^{(s-i)}\}$, $W_j = Span\{w^{(1)},\dots,w^{(t-j)}\}$. Thus, we can first recover the bases of some spaces V_{s-c_2}, W_{t-c_1}, and then extend them to the bases of V, W. Again, similarly, as in the proof of Theorem 3, we take the coordinates of the basis vectors $\{a^{(1)},\dots,a^{(s)}\}$ and $\{w^{(1)},\dots,w^{(t)}\}$ of V and W to be the unknowns, and again fix the last s coordinates of $a^{(j)}$ to 0 except the $(n-j+1)$-th coordinate that we fix to 1, and fix the first t coordinates of $w^{(i)}$ to 0 except the i-th coordinate that we fix to 1. Next, we pick two small constants c_1 and c_2, and form the bilinear system (7). Once the solution of this system is known, we can recover the rest of the bases vectors, by solving the linear system 8.

ii. The main complexity for the recovery of the key is in solving the system (7). Thus, proof for the complexity (9) is the same as for ii. Theorem 3. What is left, is to explain how the constants c_1 and c_2 are chosen. First of all, the system (7) consists of $c_1 \cdot c_2 \cdot n$ equations in $(n-s)c_2 + (m-t)c_1$ variables. We choose the constants c_1 and c_2 such that $c_1 \cdot c_2 \cdot n > (n-s)c_2 + (m-t)c_1$. Second, since the complexity is mainly determined by the value $d_{reg} = \min\{(n-s)c_2, (m-t)c_1\}$, these constants have to be chosen such that this value is minimized. Note that in practice, for actual $\mathcal{MQ}$ schemes, we can usually pick $c_1, c_2 \in \{1,2\}$.

The most important implication of the last theorem is that when $n - s$ or $m - t$ is constant we have a polynomial time algorithm for recovering a strong (s, t) separation key. This immediately implies that for any $\mathcal{MQ}$ scheme with this property we can recover in polynomial time a subspace on which the public key is linear.

Another implication is that it provides the best strategy of attacking an $\mathcal{MQ}$ scheme that possesses some strong (s, t) separation key. Indeed, since we need to minimize d_{reg}, we simply look for the minimal $m - t$ or minimal $n - s$ s.t. there exists a strong (s, t) separation key.

Example 4. Consider a (n, n) public key function from the family of STS systems (cf. Example 1.iii). From Table 1, for the parameter set $(r_1, \ldots, r_L)$ we see that the scheme has a strong $(n - r_1, r_1)$ separation key and also a strong $(n - r_{L-1}, r_{L-1})$ separation key. For the first key, $n - s = r_1$ is small, so we can choose $c_2 = 1$ and c_1 such that $c_1 n > r_1 + (n - r_1)c_1$, *i.e.,* we can choose $c_1 = 2$. For the second key, $n - t = n - r_{L-1}$ is small so we can choose $c_1 = 1$ and c_2 such that $c_2 n > r_{L-1}c_2 + (n - r_{L-1})$, *i.e.,* we can choose $c_2 = 2$. Note that for small q it is perfectly fine to choose $c_1 = c_2 = 1$ in both cases, since then at most q solutions for the strong keys will need to be tried out.

The level of nonlinearity of a given function can be used as sufficient condition for the nonexistence of a strong (s, t) separation key.

Theorem 5. *An (n, m) function f of linearity $\mathcal{L}(f) \leqslant q^{n-\frac{r}{2}}$ does not posses a strong (s, t) separation key for $s > n - r$.*

Proof. From the linearity given, f does not have any component whose linear space has dimension bigger than $n - r$. Thus, f is not strongly (s, t)–linear for $s > n - r$, and does not have a corresponding strong (s, t) separation key.

As a direct consequence, we have the following:

Corollary 1.

1. *If $(\mathcal{F}', S', T')$ is a strong (s, t) separation key for C^*, then $s \leqslant 1$ and $t \leqslant 1$.*
2. *UOV using Maiorana-McFarland bent function does not posses a strong (s, t) separation key for any $s > 0$.*

5 The (s, t)-Linearity Measure for $\mathcal{MQ}$ schemes

The size of the linear space of the components of an (n, m) quadratic function clearly provides a measure for the applicability of the function in $\mathcal{MQ}$ systems. Still, the notion of strong (s, t)–linearity can not provide a measure for the existence of all the linear subspaces on which the restriction of an (n, m) function is linear.

For example, the secret map of UOV is linear on the oil space, regardless of its nonlinearity, and even when it is of maximum nonlinearity *i.e.,* when it is bent. The existence of this space enabled Kipnis and Shamir to recover it in cases when it is large enough, as in the

original Oil and Vinegar scheme. Furthermore, the existence of such spaces improves the attack against Rainbow, compared to an attack that only considers linear spaces of the components.

We will show next that (s,t)–linearity provides a characterization for such subspaces, and thus, provides an improved measure for the security of $\mathcal{MQ}$ schemes.

Example 5. Let $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a UOV public mapping. In Section 4 we saw that the secret map of an UOV scheme belongs to the Maiorana-McFarland class. Thus, immediately, from Proposition 7, we conclude that $\mathcal{P}$ is (m,m)–linear, *i.e.,* $\mathcal{P}$ is linear on the oil space.

Now, similarly as in the previous section, we can define a special type of separation key, that separates the spaces with respect to which a function is (s,t)–linear.

Definition 8. *Let* $(\mathcal{F},S,T),(\mathcal{F}',S',T') \in \mathbb{F}_q[x_1,\ldots,x_n]^m \times \mathrm{GL}_n(\mathbb{F}_q) \times \mathrm{GL}_m(\mathbb{F}_q)$ *and let* $\mathcal{P} = T \circ \mathcal{F} \circ S = T' \circ \mathcal{F}' \circ S'$. *We call* $(\mathcal{F}',S',T')$ *an* (s,t) separation key *for* $\mathcal{P}$ *if* $\mathcal{P}$ *is* (s,t)*–linear with respect to two spaces* V *and* W, $\mathrm{Dim}(V) = s$, $\mathrm{Dim}(W) = t$ *and*

$$S' = S_V^{\intercal}, \quad T' = T_W.$$

Conclusively, any public mapping that was created using an oil and vinegar mixing has a (s,t) separation key. Table 2 gives the (s,t) separation keys for some of the $\mathcal{MQ}$ schemes that combine a layered structure with oil and vinegar mixing.

Table 2. Examples of (s,t) separation keys for some $\mathcal{MQ}$ cryptosystems

scheme	parameters	(s,t) separation keys
UOV	(q,v,o)	(o,o)
Rainbow	$(q,v,o_1,o_2) = (2^8,18,12,12)$	$(12,24)$, $(24,12)$
MQQ-SIG	$(q,d,n,r) = (2,8,160,80)$	$(8+8i, 80-8i), i \in \{0,...,9\}$
MFE	$(q^k,n,m) = ((2^{256})^k,12,15)$	$(2k,2k)$,$(3k,2k)$,$(4k,4k)$
ℓIC	$(q^k,\ell) = (2^k,3)$	$(2k,2k)$,$(k,2k)$
EnTTS	$(n,m) = (32,24)$	$(10,24)$,$(14,14)$,$(24,10)$

An interesting case regarding (s,t)–linearity is the C^* scheme for which we have the following result.

Proposition 12. *Let* $\mathcal{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *be the secret map of* C^* *(cf. Example 1ii) and let* $\gcd(\ell,n) = d$. *Then, there exists a* (d,n) *separation key for these parameters of* C^*.

Proof. First, let us consider the equation $D_{a,x}(f) = 0$ for a nonzero a. A little computation shows that it is equivalent to

$$ax(a^{2^\ell-1} + x^{2^\ell-1}) = 0,$$

and since we are interested in nonzero solutions we can restrict our attention to

$$a^{2^\ell-1} + x^{2^\ell-1} = 0.$$

This equation has $\gcd(2^\ell - 1, 2^n - 1) = 2^d - 1$ independent roots (see for example [45]). Thus, there exists a space V of dimension $\mathrm{Dim}(V) = d$ s.t. $D_{a,b}(f) = 0$, for all $a, b \in V$. This implies that $D_{a,b}(w^\intercal \cdot f) = 0$, for any $w \in \mathbb{F}_2^n$. Further from Proposition 8 and Definition 8 it follows that there exists a (d, n) separation key for the given parameters.

Hence, the best choice for parameters of the C^* scheme is when $d = 1$, because in this case, the dimension of the space V is the smallest, and it is hardest to separate it. Note that this is analogous to the case of the UOV scheme, where also it is desirable to have smaller space V. The use of $d > 1$ was exactly the property that was exploited by Dubois *et al.* in [25] to break a modified version of the signature scheme SFLASH with $d > 1$ before the more secure version with $d = 1$ was broken due to the possibility to decompose the second order derivative into linear functions [24]. Even then the authors of [25] noted that the condition $d = 1$ should be included in the requirements of the scheme, a fact that was overseen by the NESSIE consortium.

Note further that Proposition 12 implies that the dimension of the space V is invariant under restrictions of the public map (minus modifier). Thus, the SFLASH signature scheme also possesses a (d, k) separation key, where $k \leqslant n$ is the number of coordinates of the public key of SFLASH, and can equivalently be used to attack the modified version.

Similarly as for the case of strong (s, t) separation keys, (cf. Theorem 3 and Theorem 4), we can construct a generic algorithm that finds (s, t) separation keys. This part will be covered in the extended version of the paper. Here we focus our interest on a special type of separation keys, namely, (s, m) separation keys where the space W is the entire image space of the function. Indeed, schemes including UOV, Rainbow, Enhanced TTS, all posses exactly such keys. We will also show how the properties of (s, m)–linearity provide the best strategy for attacking schemes that posses (s, m) separation keys. Unfortunately, in this case it is more difficult to estimate the complexity of the attacks, since the obtained equations are of mixed nature. Therefore, we leave the complexity estimate for future work. Still, it is notable that we again arrive to equivalent systems of equation as in the case of good keys.

Theorem 6. *Let it be known that an (s, m) separation key exists for a given $\mathcal{MQ}$ public key $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ with matrix representations $\mathfrak{P}_i := \widetilde{\mathfrak{P}}_i + \widetilde{\mathfrak{P}}_i^\intercal$ of the coordinate functions p_i.*

i. The task of finding an (s, m) separation key $(S_V^\intercal, T_{\mathbb{F}_q^m})$ is equivalent to solving the following system of equations

$$\begin{aligned} a^{(j)}\mathfrak{P}_i a^{(k)} &= 0,\ i \in \{1, ..., m\},\ j, k \in \{1, ..., s\}, j < k \\ a^{(k)}\widetilde{\mathfrak{P}}_i a^{(k)} &= 0,\ i \in \{1, ..., m\},\ k \in \{1, ..., s\}, \end{aligned} \tag{10}$$

in the unknown basis vectors $a^{(j)}$ of the space V.

ii. The key can equivalently be found by

1. *First solving the system of equations*

$$a^{(j)}\mathfrak{P}_i a^{(k)} = 0,\ i \in \{1,...,m\},\ j,k \in \{1,...,c\}, j < k$$
$$a^{(k)}\widetilde{\mathfrak{P}}_i a^{(k)} = 0,\ i \in \{1,...,m\},\ k \in \{1,...,c\}, \quad (11)$$

in the unknown basis vectors $a^{(k)}$, $k \in \{1,\ldots,c\}$ of the space V, for an appropriately chosen integer c.

2. *And then solving the system of linear equations*

$$a^{(j)}\mathfrak{P}_i a^{(k)} = 0, i \in \{1,...,m\}, j \in \{1,...,c\}, k \in \{c+1,...,s\}, j < k$$

in the unknown basis vectors $a^{(k)}$, $k \in \{c+1,...,s\}$ of the space V.

Proof. i. From Definition 8, $\mathcal{P}$ is (s,m)–linear with respect to $V, \mathbb{F}_q^m$ where $\mathrm{Dim}(V) = s$. So we need to recover only some basis $\{a^{(1)},\ldots,a^{(s)}\}$ of V. From Definition 6 and Proposition 8, the condition for (s,t)–linearity can be written as $D_{a^{(j)},a^{(k)}}f = 0$ for all $a^{(j)}, a^{(k)} \in V$, *i.e.,* as $a^{(j)}\mathfrak{P}_i a^{(k)} = 0$. Since $D_{a,a}f = 0$ for any a, we must write this condition as $a^{(k)}\widetilde{\mathfrak{P}}_i a^{(k)} = 0$. We ensure the linear independence of the unknown basis vectors $\{a^{(1)},\ldots,a^{(s)}\}$ by fixing the last s coordinates of $a^{(j)}$ to 0 except the $(n-j+1)$-th coordinate that we fix to 1. The probability that we can fix the coordinates of the basis vectors in this way is approximately $1 - \frac{1}{q-1}$. If the system does not yield a solution we randomize $\mathcal{P}$. In this way we form the system (10). It consists of $m\binom{s+1}{2}$ equations in $s(n-s)$ variables.

ii. From Proposition 6, we have that if $\mathcal{P}$ is (s,m)–linear, with respect to a vector space $V = Span\{a^{(1)},\ldots,a^{(s)}\}$, $\mathbb{F}_q^m$, then it is $(s-1,m)$–linear with respect to $V_1, \mathbb{F}_q^m$, where $V_1 \subset V$. Hence, there exists an array of subspaces $V \supset V_1 \supset \cdots \supset V_{s-1}$, such that $\mathcal{P}$ is $(s-i,m)$–linear with respect to $V_i = Span\{a^{(1)},\ldots,a^{(s-i)}\}$. Thus, we can first recover the basis of some space V_{s-c} and then extend it to the bases of V. That is, we first solve (11), and then we are left with the linear system (12). What is left is how we choose the constant c. The system (11) consists of $m\binom{c+1}{2}$ equations in $(n-s)c$ variables. It is enough to choose c such that $m\binom{c+1}{2} > (n-s)c$, in order to get a unique solution for the basis vectors.

Remark 1. Conditions for (s,t)–linearity have been used in other attacks not involving good keys or system solving. For example, the analysis of UOV in [1] uses exactly the conditions of Proposition 8 in order to test whether a subspace is contained in the oil space. An equivalent condition is also used in [46] again for analysis of UOV, and the authors' approach here is a purely heuristic one.

We conclude this part with an interesting result on the (s,m)–linearity of a random quadratic (n,m)-function.

Proposition 13. *Let f be a randomly generated (n,m)-function over $\mathbb{F}_q$. Then, we can expect that there exist $q^{\frac{2(n-s)}{m(s+1)}}$ different subspaces V, such that f is (s,m)–linear with respect to $V, \mathbb{F}_q^m$.*

Proof. Let the (n,m)-function f be given. Then f is (s,m) linear with respect to some space V if and only if there exist s linearly independent vectors $a^{(1)},\ldots,a^{(s)} \in \mathbb{F}_q^n$ such that $V = Span\{a^{(1)},\ldots,a^{(s)}\}$ and f is linear on every coset of V. Without loss of generality, we can fix s coordinates in each of the $a^{(k)}$ to ensure linear independence. In this manner, from the conditions of linearity from Theorem 6 we obtain a quadratic system of $m\binom{s+1}{2}$ equations in $s(n-s)$ variables. We can expect that such a system, on average has around $q^{\frac{s(n-s)}{m\binom{s+1}{2}}} = q^{\frac{2(n-s)}{m(s+1)}}$ solutions. For simplicity, we assume that the coordinates can be fixed in the particular manner. (In general, this is possible with a probability of $1-\frac{1}{q-1}$.) Note that all of these solutions span different subspaces. Indeed, suppose $(a_1^{(1)},\ldots,a_1^{(s)})$ and $(a_2^{(1)},\ldots,a_2^{(s)})$ are two different solutions. Then there exists i such that $a_1^{(i)} \neq a_2^{(i)}$. Then $a_2^{(i)}$ is not in the span of $a_1^{(1)},\ldots,a_1^{(s)}$ because the fixed coordinates ensure linear independence. Thus, all the solutions generate different subspaces.

Proposition 13 implies that random quadratic (n,m) functions most probably have an $(\lfloor\frac{2n-m}{m+2}\rfloor, m)$ separation key. For the case of $n=m$, this means that there are no nontrivial (s,m) separation keys, but for the case of $n=2m$, we can expect that there is a $(2,m)$ separation key, and for $n=2m+4$, even a $(3,m)$ separation key.

Note that Proposition 13 further implies, that for $n \approx m^2$, a random quadratic (n,m) function is likely to have a (m,m) separation key. This is exactly the case identified by Kipnis *et al.* [1] as an insecure parameter set. See [1] for an efficient algorithm for recovering this space.

5.1 On the Reconciliation Attack on UOV

Recall the shape of the internal map of UOV from Example 1i. From Proposition7 and Proposition6 it follows that $\mathcal{P}$ is (i,m)–linear for any $1 \leqslant i \leqslant m$. In order to break the scheme, it is necessary to find a vector space V, such that $\mathcal{P}$ is (m,m)–linear with respect to $(V,\mathbb{F}_q^m)$. We will call any such space V an oil space. Ding *et al.* in [39] propose an algorithm that sequentially performs a change of basis that reveals gradually the space V. They call the algorithm *Reconciliation Attack on UOV*. In Figure 1, we present an equivalent version of the attack interpreted in terms of (s,t)–linearity (cf. Algorithm 2 [39]).

It can be noticed that the Reconciliation attack is exactly an (s,m) separation key attack, where the constant c in Thm 6 is chosen to be $c=1$. However, we will show that the choice of $c=1$ is justified only for the (approximately) balanced version of UOV, and not for any parameter set.

For example, consider the UOV parameter set $m=28$ and $v=56$. The public key in this case has a $(28,28)$ separation key. Using the reconciliation attack (equivalently if we take $c=1$ in Thm 6) in order to find a solution for $a^{(1)}$ one needs to solve a system of 28 quadratic equations in 56 variables. On average we can expect $q^{v-m} = q^{28}$ solutions. From the description of the reconciliation attack it seems that any of the solutions is a "good one", *i.e.,* it leads eventually to the recovery of the space V. This means that we can simply fix $v-m=28$ variables and on average get a single solution by solving a system

Input: UOV public key $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$.
$V_0 \leftarrow$ the zero-dimensional vector space
for $k := 1$ to m **do**
Find $a^{(k)} = (a_1^{(k)}, ..., a_v^{(k)}, 0, ..., 0, 1_{n-k+1}, 0, ..., 0) \in \mathbb{F}_q^n$,
where 1_{n-k+1} denotes that the $(n-k+1)$-th coordinate is 1, by solving

$$a^{(j)}\mathfrak{P}_i a^{(k)} = 0,\ i \in \{1, \ldots, m\}, j < k$$
$$a^{(k)}\widetilde{\mathfrak{P}}_i a^{(k)} = 0,\ i \in \{1, \ldots, m\},$$

Construct a space $V_k \subset \mathbb{F}_q^n$ with $\mathrm{Dim}(V_k) = k$, s.t.

- $V_k = V_{k-1} \oplus Span\left\{a^{(k)}\right\}$, and
- $\mathcal{P}$ is (k, m)–linear with respect to $(V_k, \mathbb{F}_q^m)$.

end for
Output: An oil space $V = V_m$ of dimension m.

Fig. 1. Reconciliation Attack on UOV in terms of (s, t)–linearity

of 28 equations in 28 variables. In other words, this approach seems to work equally well for the balanced version of the scheme (when $m = v$) and for the unbalanced version.

Now, consider a UOV public key $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$. By definition it is (m, m)–linear, and also (s, m)–linear for every $s \leqslant m$. We can use Theorem 6 ii. to find the (m, m) separation key by choosing c such that $m\binom{c+1}{2} > (n-m)c$, *i.e.,* $c > 2(n/m-2)$. We suppose that we have fixed $n - m$ coordinates of the vectors $a^{(1)}, \ldots, a^{(m)} \in \mathbb{F}_q^n$ to ensure linear independence. Suppose instead that we have chosen $c < 2(n/m - 2)$. Then Step 1 of Theorem 6 ii. will give on average $q^{2(n-m)/m(c+1)}$ solutions for the basis vectors, and all the solutions span a different space of dimension c such that $\mathcal{P}$ is (c, m) linear with respect to it (cf. Proposition 13). From the choice of the basis vectors, only one of these spaces is a subspace of the oil space V we are trying to recover. Thus, if $q^{2(n-m)/m(c+1)}$ is relatively big, it is infeasible to find the correct subspace. If we choose a wrong space, after several steps (depending on n, m, c), we will not be able to find any new linearly independent vectors. The reason is that from Proposition 13 it is expected that even in the random case such subspaces exist, but their dimension is much smaller than that of the actual oil space. Hence, we must choose at least $c \approx 2(n/m - 2)$. For example, $c = 1$ is suitable only for balanced versions where $n \approx 2m$, $c = 2$ can be used for n upto $\approx 3m$, and for the practically used parameters of $3m < n < 4m$ c should be 4 or even 5.

Remark 2. In [47], Thomae analyses the efficiency of the Reconciliation attack on UOV, and concludes that solving the equations from the first step of the attack is quite inefficient. He proposes instead to recover several columns from the good key at once and introduces some optimal parameter k for the number of columns, that corresponds to our parameter c in Theorem 6. However, the author does not discuss why the parameter is necessary, how to choose it, and what does it mean with regards to different parameters of UOV. The discussion above answers these questions.

5.2 Combining strong (s,t)–linearity and (s,t)–linearity

A number of existing $\mathcal{MQ}$ schemes combine several paradigms in their design. For example, Rainbow [2] or EnTTS [7] have a secret map with both layered and UOV structure. In other words, these schemes posses both types of separation keys. (Note that we do not talk about the trivial implication of a (s,t) separation key when a strong (s,t) separation key exists.) For example, Rainbow, with parameters (v, o_1, o_2), where $n = v + o_1 + o_2$, $m = o_1 + o_2$, has a $(o_2, o_1 + o_2)$ separation key with respect to $V, \mathbb{F}_q^m$, but also a strong (o_2, o_1) separation key with respect to the same subspace V and some $W \subset \mathbb{F}_q^m$. We can certainly focus on only one of the keys, and for example use either Theorem 4 or Theorem 6 to recover it. But since they share the same V the best strategy would be to combine the conditions for both strong linearity and linearity, *i.e.,* combine both theorems. A little computation shows that in this way, we can take both $c_1 = c_2 = 1$ in Theorem 4 and $c = 1$ in Theorem 6, *i.e.,* indeed we arrive to the most efficient case for recovery of V, W.

A similar argument applies to any $\mathcal{MQ}$ cryptosystem that encompasses layered and UOV structure. Notably, the possibility to use the aforementioned combination is exactly why the Rainbow band separation attack is much more efficient than the reconciliation attack.

6 Prudent Design Practice for $\mathcal{MQ}$ schemes

In the previous sections we saw that strong (s,t)–linearity and (s,t)–linearity provide a reasonable measure for the security of $\mathcal{MQ}$ cryptosystems. Certainly, in some schemes, the internal structure is clear from the construction, and such characterization may seem redundant. However, many schemes contain a hidden structure, that is invariant under linear transformations, (and thus, present in the public map) and that became obvious only after the scheme was broken. Furthermore, sometimes the constructions of the internal map lack essential conditions as in the case of SFLASH, where the specification was missing a condition on the $\gcd(\ell, n)$. We give another example concerning the MQQ-SIG scheme.

Example 6. The designers of the MQQ-SIG signature scheme in the construction of the internal map use a special type of quadratic $(2d, d)$ function $f = (f_1, \ldots, f_d)$ that is balanced when the first d arguments are fixed. They classify such functions depending on how many of f_i are linear, and as a security measure require that all should be quadratic. They further impose the restrictions that the rank of the matrix of f_i, $i = 1, \ldots, d$ should be high. While these are completely reasonable requirements, they do not properly reflect the linearity of the function, and are, thus, not at all sufficient to avoid instances of high linearity. Instead, a better requirement would be to impose a restriction on the rank of any of the components $v^\intercal \cdot f$, or equivalently to bound from above the linearity $\mathcal{L}(f)$.

Thus, it seems that a good practice is to include conditions about the linearity of the used functions. A nice concise criteria is the behaviour of the derivatives $D_a(f)$ and $D_{a,b}(f)$ of a function f (cf. Proposition 5 and 8) and the nonlinearity measure. As already mentioned, bent functions have the highest possible nonlinearity. However, since all quadratic bent functions over characteristic 2, are from the Maiorana-McFarland class, [48], their relatively high (s,t)-linearity can be considered as a drawback. Conclusively, other functions that have low linearity in both senses (strong (s,t) and (s,t)) should be considered. AB

functions have such properties. Unfortunately, Gold functions (cf. C^*) can not be used because of the presence of symmetry invariants, but it seems as a good idea to investigate other AB functions (or close to AB) for applicability in $\mathcal{MQ}$ cryptosystems.

7 Conclusion

High nonlinearity of vectorial functions is nowadays widely accepted criterion in symmetric cryptography. As it turns out, it is also crucial for the security of $\mathcal{MQ}$ cryptosystems and thus can be used as a relevant security measure in their design. Indeed, in this paper, we provided a general framework based on linearity measures that encompasses *any* attack that takes advantage of the existence of linear spaces, and thus can be considered as a generalization of all such attacks. That is why, we believe that other notions from symmetric cryptography including resiliency and differential uniformity can successfully be adapted in the $\mathcal{MQ}$ context, and benefit further to the understanding of the security of $\mathcal{MQ}$ cryptosystems.

Acknowledgement

The first author of the paper is partially supported by FCSE, UKIM, R.Macedonia.

References

1. A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced oil and vinegar signature schemes," in Advances in Cryptology EUROCRYPT '99. Springer, 1999, pp. 206–222.
2. J. Ding and D. Schmidt, "Rainbow, a new multivar. polynomial signature scheme." in ACNS, ser. LNCS, vol. 3531, 2005, pp. 164–175.
3. T.-T. Moh, "A public key system with signature and master key functions," Comm. in Algebra, vol. 27, no. 5, 1999, pp. 2207–2222.
4. C. Wolf, A. Braeken, and B. Preneel, "On the security of stepwise triangular systems," Designs, Codes and Cryptography, vol. 40, no. 3, 2006, pp. 285–302.
5. D. Gligoroski, R. S. Ødegård, R. E. Jensen, L. Perret, J.-C. Faugère, S. J. Knapskog, and S. Markovski, "MQQ-SIG - An Ultra-Fast and Provably CMA Resistant Digital Signature Scheme," in INTRUST, ser. LNCS, vol. 7222. Springer, 2011, pp. 184–203.
6. B.-Y. Yang, J.-M. Chen, and Y.-H. Chen, "Tts: High-speed signatures on a low-cost smart card," in CHES, ser. LNCS, vol. 3156. Springer, 2004, pp. 371–385.
7. B.-Y. Yang and J.-M. Chen, "Building secure tame-like multivariate public-key cryptosystems: The new tts." in ACISP '05, ser. LNCS, vol. 3574. Springer, 2005, pp. 518–531.
8. H. Imai and T. Matsumoto, "Algebraic methods for constructing asymmetric cryptosystems." in AAECC, ser. LNCS, vol. 229. Springer, 1985, pp. 108–119.
9. N. Courtois, L. Goubin, and J. Patarin, "Sflash, a fast asymmetric signature scheme for low-cost smartcards - primitive specification and supporting documentation." [Online]. Available: www.minrank.org/sflash-b-v2.pdf [Retrieved: September 2014].
10. J. Patarin, "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms," in Advances in Cryptology – EUROCRYPT '96, ser. LNCS, vol. 1070. Springer, 1996, pp. 33–48.
11. O. Billet, J. Patarin, and Y. Seurin, "Analysis of intermediate field systems," Cryptology ePrint Archive, Report 2009/542, 2009.
12. C.-H. O. Chen, M.-S. Chen, J. Ding, F. Werner, and B.-Y. Yang, "Odd-char multivariate hidden field equations," Cryptology ePrint Archive, Report 2008/543, 2008.

13. J. Patarin, N. Courtois, and L. Goubin, "Quartz, 128-bit long digital signatures." in CT-RSA, ser. LNCS, vol. 2020. Springer, 2001, pp. 282–297.
14. N. Courtois and L. Goubin, "Cryptanalysis of the TTM cryptosystem," in Advances in Cryptology – ASIACRYPT '00, ser. LNCS, vol. 1976. Springer, 2000, pp. 44–57.
15. A. Kipnis and A. Shamir, "Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization," in CRYPTO, ser. LNCS, vol. 1666. Springer, 1999, pp. 19–30.
16. E. Thomae and C. Wolf, "Cryptanalysis of Enhanced TTS, STS and all its Variants, or: Why Cross-Terms are Important," in Progress in Cryptology – AFRICACRYPT 2012, ser. LNCS, vol. 7374. Springer, 2012, pp. 188–202.
17. L. Bettale, J.-C. Faugre, and L. Perret, "Cryptanalysis of hfe, multi-hfe and variants for odd and even characteristic," Designs, Codes and Cryptography, vol. 69, no. 1, 2013, pp. 1–52.
18. N. T. Courtois, "Efficient zero-knowledge authentication based on a linear algebra problem MinRank," in ASIACRYPT 2001, ser. LNCS, vol. 2248. Springer, 2001, pp. 402–421.
19. C. Wolf and B. Preneel, "Large Superfluous Keys in Multivariate Quadratic Asymmetric Systems," in Public Key Cryptography, ser. LNCS, vol. 3386. Springer, 2005, pp. 275–287.
20. P.-A. Fouque, L. Granboulan, and J. Stern, "Differential cryptanalysis for multivariate schemes," in Advances in Cryptology EUROCRYPT 2005, ser. LNCS, vol. 3494. Springer, 2005, pp. 341–353.
21. J. Ding, "A new variant of the Matsumoto-Imai cryptosystem through perturbation." in PKC, 2004, pp. 305–318.
22. V. Dubois, L. Granboulan, and J. Stern, "An efficient provable distinguisher for hfe," in ICALP (2), ser. LNCS, vol. 4052. Springer, 2006, pp. 156–167.
23. ——, "Cryptanalysis of hfe with internal perturbation," in Public Key Cryptography, ser. LNCS, vol. 4450. Springer, 2007, pp. 249–265.
24. V. Dubois, P.-A. Fouque, A. Shamir, and J. Stern, "Practical cryptanalysis of SFLASH," in Advances in cryptology, ser. CRYPTO'07. Springer, 2007, pp. 1–12.
25. V. Dubois, P.-A. Fouque, and J. Stern, "Cryptanalysis of sflash with slightly modified parameters." in EUROCRYPT '07, ser. LNCS, M. Naor, Ed., vol. 4515. Springer, 2007, pp. 264–275.
26. J. Patarin, "Cryptoanalysis of the Matsumoto and Imai public key scheme of EUROCRYPT '88," in CRYPTO '95, 1995, pp. 248–261.
27. "Nessie: New european schemes for signatures, integrity, and encryption," 2003. [Online]. Available: https://www.cosic.esat.kuleuven.be/nessie/ [Retrieved: September 2014].
28. S. Tsujii, M. Gotaishi, K. Tadaki, and R. Fujita, "Proposal of a signature scheme based on sts trapdoor," in Post-Quantum Cryptography, ser. LNCS. Springer, 2010, vol. 6061, pp. 201–217.
29. K. Sakumoto, T. Shirai, and H. Hiwatari, "On provable security of uov and hfe signature schemes against chosen-message attack," in Post-Quantum Cryptography, ser. LNCS, 2011, vol. 7071, pp. 68–82.
30. D. Smith-Tone, "On the differential security of multivariate public key cryptosystems," in Post-Quantum Cryptography, ser. LNCS. Springer, 2011, vol. 7071, pp. 130–142.
31. R. Perlner and D. Smith-Tone, "A classification of differential invariants for multivariate post-quantum cryptosystems," in Post-Quantum Cryptography, ser. LNCS. Springer, 2013, vol. 7932, pp. 165–173.
32. K. Nyberg, "On the construction of highly nonlinear permutations," in EUROCRYPT, ser. LNCS, vol. 658. Springer, 1992, pp. 92–98.
33. C. Boura and A. Canteaut, "A new criterion for avoiding the propagation of linear relations through an Sbox," in FSE 2013 - Fast Software Encryption, ser. LNCS. Singapore: Springer, 2014.
34. W. Buss, G. Frandsen, and J. Shallit, "The computational complexity of some problems of linear algebra." J. Comput. System Sci., 1999.
35. C. Wolf and B. Preneel, "Equivalent Keys in Multivariate Quadratic Public Key Systems," Journal of Mathematical Cryptology, vol. 4, April 2011, pp. 375–415.
36. K. Nyberg, "Perfect nonlinear s-boxes," in EUROCRYPT, ser. LNCS, D. W. Davies, Ed., vol. 547. Springer, 1991, pp. 378–386.
37. J. F. Dillon, "Elementary hadamard difference sets," Ph.D. dissertation, University of Maryland, 1974.
38. F. Chabaud and S. Vaudenay, "Links between differential and linear cryptoanalysis." in EUROCRYPT '94, ser. LNCS, vol. 950. Springer, 1994, pp. 356–365.
39. J. Ding, B.-Y. Yang, C.-H. O. Chen, M.-S. Chen, and C.-M. Cheng, "New differential-algebraic attacks and reparametrization of rainbow." in ACNS, ser. LNCS, vol. 5037, 2008, pp. 242–257.
40. J. Patarin and L. Goubin, "Asymmetric cryptography with s-boxes." in ICICS, ser. LNCS, vol. 1334. Springer, 1997, pp. 369–380.

41. J. Ding, L. Hu, X. Nie, J. Li, and J. Wagner, "High order linearization equation (hole) attack on multivariate public key cryptosystems." in Public Key Cryptography '07, ser. LNCS, vol. 4450, 2007, pp. 233–248.
42. J.-C. Faugère, M. S. E. Din, and P.-J. Spaenlehauer, "Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1, 1): Algorithms and complexity," J. Symb. Comput., vol. 46, no. 4, 2011, pp. 406–437.
43. M. Bardet, J.-C. Faugère, and B. Salvy, "On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations," in ICPSS, 2004, pp. 71–75.
44. M. Bardet, J.-C. Faugère, B. Salvy, and B.-Y. Yang, "Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems," in Proc. of MEGA'05,, 2005.
45. R. Lidl and H. Niederreiter, Finite Fields. Cambridge UP, 1997.
46. A. Braeken, C. Wolf, and B. Preneel, "A study of the security of unbalanced oil and vinegar signature schemes." in CT-RSA, ser. LNCS, A. Menezes, Ed., vol. 3376. Springer, 2005, pp. 29–43.
47. E. Thomae, "About the Security of Multivariate Quadratic Public Key Schemes," Ph.D. dissertation, Ruhr-University Bochum, 2013.
48. L. Budaghyan, C. Carlet, T. Helleseth, and A. Kholosha, "Generalized bent functions and their relation to maiorana-mcfarland class." in ISIT '12. IEEE, 2012, pp. 1212–1215.