Research Article

Bilal Alam, Ferruh Özbudak and Oğuz Yayla

Classes of weak Dembowski–Ostrom polynomials for multivariate quadratic cryptosystems

Abstract: T. Harayama and D. K. Friesen [12] proposed the linearized binomial attack for multivariate quadratic cryptosystems and introduced weak Dembowski–Ostrom (DO) polynomials in this framework over the finite field $\mathbb{F}_2$. We extend the linearized binomial attack to multivariate quadratic cryptosystems over $\mathbb{F}_p$ for any prime p and redefine the weak DO polynomials for general case. We identify infinite classes of weak DO polynomials for these systems by considering highly degenerate quadratic forms over algebraic function fields and Artin–Schreier type curves to achieve our results. This gives a general answer to the conjecture stated by Harayama and Friesen and also a partial enumeration of weak DO polynomials over finite fields.

Keywords: Linearized binomial attack, weak DO polynomials, multivariate quadratic cryptosystems

MSC 2010: 94A60, 14G50

Bilal Alam: Institute of Applied Mathematics, Middle East Technical University, Dumlupınar Blv. No:1, 06800 Ankara, Turkey, e-mail: alam54b@gmail.com
Ferruh Özbudak: Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Dumlupınar Blv. No:1, 06800 Ankara, Turkey, e-mail: ozbudak@metu.edu.tr
Oğuz Yayla: Johann Radon Institute for Computational and Applied Mathematics (RICAM), Austrian Academy of Sciences, Altenberger Str. 69, 4040 Linz, Austria, e-mail: oguz.yayla@gmail.com

Communicated by: Alfred Menezes

1 Introduction

Public key cryptography is mainly used in e-commerce systems for authentication (electronic signatures) and secure communication (encryption). The security of using public key cryptography centers on the difficulty of solving certain classes of hard mathematical problems. Multivariate cryptography is an asymmetric cryptographic primitive based on multivariate polynomials over a finite field. Multivariate public key cryptosystems (MPKC for short) have a set of multivariate polynomials as its public key. Its main security assumption is based on the NP-hardness of the problem to solve these nonlinear equations over a finite field [18].

Multivariate Quadratic Problem: Solve the system $P_1(x) = P_2(x) = \cdots = P_m(x) = 0$ such that each P_i is a quadratic polynomial in $x = (x_1, \ldots, x_n)$ over a finite field $\mathbb{F}_q$.

The multivariate quadratic (MQ) problem is an NP-hard problem in general [18]. In fact, a random set of quadratic equations would not have a trapdoor and hence not be usable in an MQ cryptosystem. Instead of dealing with random equations, we deal with special equations where the security of an MQ cryptosystem is not guaranteed by NP-hardness of the MQ problem and there could exist effective attacks for any chosen trapdoor. The history of MPKCs therefore evolves as we understand more and more about how to design secure multivariate trapdoors.

This family is considered as one of the major families of PKCs that could even resist the powerful quantum computers of the future [9]. The last few decades saw a fast and intensive development in MPKCs. Some constructions are not as secure as was claimed initially, but others are still viable. Recently, a new idea of reviving hidden field equations (HFE) based multivariate quadratic cryptography using a field of odd characteristic [3, 8] is a proof of this fact.

Kipnis and Shamir [14] attacked MQ cryptosystems over $\mathbb{F}_q$ based on the observation that corresponding to any public key polynomial map of MQ cryptosystem there is an equivalent single univariate polynomial

over $\mathbb{F}_{q^n}$. This univariate polynomial belongs to the class of *Dembowski–Ostrom (DO) polynomials* introduced in [5]. An MQ cryptosystem defined over $\mathbb{F}_q$ when used in digital signature scheme usually gives short signatures of size $\mathbb{F}_q^m$ for some integer m. Thus, the birthday attack is generally applicable to the underlying MQ system at complexity $O(q^{m/2})$; see [4].

Harayama and Friesen in a recent work [12] proposed the linearized binomial attack for MQ systems over $\mathbb{F}_2$ with $n = m$ which is a customization of the birthday attack. They showed that the linearized binomial attack can be asymptotically better by at most a factor of $2^{n/8}$ than the birthday attack for MQ signature schemes that have a univariate public key polynomial belonging to certain classes of DO polynomials over $\mathbb{F}_{2^n}$. They called these polynomials *weak DO polynomials* and proved that there exist infinitely many weak DO polynomials. They also made a conjecture about the existence of infinite series of these polynomials over $\mathbb{F}_{2^n}$ of the form

$$g(x) = x^{2^{n/4}+1} + x^{2^{3n/4}+1} \in \mathbb{F}_{2^n}[x]$$

and posed an open question to enumerate such classes of weak DO polynomials.

In this paper we address this conjecture. In Corollary 4.3, we prove the existence of the conjectured class of weak DO polynomials, and, in Theorem 4.1, identify the general class to which this class belongs. We first extend the linearized binomial attack in [12] for the finite fields with characteristic 2 to the odd characteristic finite fields using results in [17] and then redefine weak DO polynomials for the finite fields of characteristic any prime p in Definition 3.2. Later we identify a general class of weak DO polynomials of the form

$$f(x) = \sum_{i=1}^{k} A_i x^{p^{(2i-1)n/(2k)}+1} \in \mathbb{F}_{p^n}[x]$$

using the theory of algebraic function fields. From our general class statement in Theorem 4.4, many general subclass polynomials can be easily derived like the conjectured class in [12].

The paper is organized as follows. Multivariate quadratic cryptosystems are introduced in Section 2. Section 3 introduces the existential forgery of MQ signature schemes, the linearized binomial attack and the significance of computing the number of solutions of a specific bivariate equation in terms of the linearized binomial attack. Later we give a general definition of weak DO polynomials over $\mathbb{F}_{p^n}$. In Section 4, we present a general class of weak DO polynomials using highly degenerate quadratic forms and Artin–Schreier type algebraic curves over finite fields. We present a short comparison of the Gröbner basis method and the linearized binomial attack at the end of Section 4.

2 Background

Let $\mathbb{F}_q$ be the finite field of characteristic p. In multivariate quadratic cryptosystems over $\mathbb{F}_q$ the trapdoor one-way function takes the form of a multivariate quadratic polynomial map over $\mathbb{F}_q$. Namely the public key is given by a set of quadratic polynomials over $\mathbb{F}_q$. A trapdoor public one-way function $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is defined as a polynomial vector of m multivariate quadratic polynomials $F = (P_1, \ldots, P_m) \in (\mathbb{F}_q[x_1, \ldots, x_n])^m$ such that

$$P_k(x_1, \ldots, x_n) = \sum_{1 \le i \le n} \sum_{1 \le j \le n} \alpha_{i,j}^{(k)} x_i x_j + \sum_{1 \le i \le n} \beta_i^{(k)} x_i + \gamma_i^{(k)},$$

where $\alpha_{i,j}^{(k)}, \beta_i^{(k)}, \gamma_i^{(k)} \in \mathbb{F}_q$ for all $k = 1, 2, \ldots, m$. To be useful for public key cryptography, we do not only need an intractable problem, but also a way of embedding a trapdoor into it. For the public quadratic polynomial F, an equivalent invertible secret map serves as the trapdoor. This equivalent map is generally composed of a low degree central univariate polynomial $f(x)$ in $\mathbb{F}_{q^n}[x]$ and two affine bijections L_1 and L_2 over the vector space $\mathbb{F}_q^n$:

$$F = L_1 \circ \phi \circ f \circ \phi^{-1} \circ L_2.$$

The one-way mapping F is the public key and the invertible triple (L_1, L_2, f) is the private key (trapdoor information). The canonical bijection ϕ and its inverse ϕ^{-1} are used to transfer elements between the extension

field $\mathbb{F}_{q^n}$ and the vector space $\mathbb{F}_q^n$. Regarding the public system of polynomials in MQ cryptosystems, Kipnis and Shamir [14] in principle observed the following.

Theorem 2.1 ([20, Theorem 2.4.9]). *Let $F = (P_1, \ldots, P_m) \in (\mathbb{F}_q[x_1, \ldots, x_n])^m$ be a multivariate quadratic system of equations. Moreover, define $l := \max\{n, m\}$ and an extension field $\mathbb{E} = \mathbb{F}_{q^l}$. Then, there exists a unique univariate polynomial $f'(x)$ over $\mathbb{E}$:*

$$f'(x) = \sum_{1 \le i \le D} a_i x^{q^{\alpha_i} + q^{\beta_i}} + \sum_{1 \le j \le L} b_j x^{q^{\gamma_j}} + c,$$

where $D, L \in \mathbb{N}$, $a_i, b_j, c \in \mathbb{F}_{q^l}$, $\alpha_i \ge \beta_i$, $q^{\alpha_i} + q^{\beta_i} \le q^l - 1$, $q^{\gamma_j} \le q^l - 1$ for each $1 \le i \le D$, $1 \le j \le L$ which computes the same function as the polynomial vector F and vice versa.

From the adversary point of view, the action of L_1 and L_2 transforms the internal polynomial f into a very sparse univariate polynomial of very high degree, as shown for instance by Kipnis and Shamir in [14]. A possible decryption attack would consist in inverting or factorizing this polynomial. However, there are no efficient algorithms to perform these tasks and merely deciding the existence of roots is in fact NP-hard [14].

Several major methods have been developed to attack MQ cryptosystems. Structural attacks rely solely on the specific structure of the trapdoor involved. General attacks use various methods of solving the set of multivariate polynomial equations, e.g., the Gröbner basis method and its improvements. One similar general attack has been proposed by Harayama and Friesen [12] in which they exploit the equivalent univariate representation of the public key polynomial map. Broadly, they attack MQ signature schemes to find one valid forged message and signature pair.

Harayama and Friesen [12] used Weil sum computation of the univariate representation $f'(x)$ for MQ cryptosystems $m = n$ over $\mathbb{F}_p$ in their attack, i.e., $q = p$. They consider the following result from Mills [17] which we also refer later in this paper.

Theorem 2.2 ([11, Theorem 2.1.1], [17, Theorem 1.4]). *Let $S(a_1, \ldots, a_D, b_1, \ldots, b_L, c)$ be the Weil sum of the following univariate polynomial:*

$$f'(x) = \sum_{1 \le i \le D} a_i x^{p^{\alpha_i} + p^{\beta_i}} + \sum_{1 \le j \le L} b_j x^{p^{\gamma_j}} + c,$$

where $D, L \in \mathbb{N}$, $a_i, b_j, c \in \mathbb{F}_{p^n}$, $\alpha_i \ge \beta_i$, $p^{\alpha_i} + p^{\beta_i} \le p^n - 1$, $p^{\gamma_j} \le p^n - 1$ for each $1 \le i \le D$, $1 \le j \le L$. With the translation of coefficients involved such that

$$A_i^{p^{t_i}} = a_i \in \mathbb{F}_{p^n} \quad \text{for } 1 \le i \le D,$$

and parameters $t_i, s_i \in \mathbb{Z}$ and $b \in \mathbb{F}_{p^n}$ such that $t_i \equiv \beta_i - \beta_1 \bmod n$, $s_i = \alpha_i - \beta_i \ge 0$ for $1 \le i \le D$ and

$$b = \sum_{1 \le j \le L} b_j^{p^{n-\gamma_j}},$$

$S(a_1, \ldots, a_D, b_1, \ldots, b_L, c)$ can be equivalently expressed as

$$S = \sum_{x \in \mathbb{F}_{p^n}} \chi_1\Big(\sum_{i=1}^{D} A_i x^{p^{s_i}+1} + b^{p^{\beta_1}} x \Big),$$

where χ_1 denotes the canonical additive character of $\mathbb{F}_{p^n}$ and $\chi_1(c) = e^{2\pi \operatorname{Tr}(c)/p}$ for all $c \in \mathbb{F}_q$. The polynomial $\sum_{i=1}^{D} A_i x^{p^{s_i}+1} + b^{p^{\beta_1}} x$ is the simplified univariate representation *of $f'(x)$ with $S(a_1, \ldots, a_D, b_1, \ldots, b_L, c) = S(A_1, \ldots, A_D, b_1, \ldots, b_L, c)$.*

We note that Harayama and Friesen [12] only considered MQ cryptosystems over $\mathbb{F}_2$ in their attack. In the present study, however, we consider MQ cryptosystems over $\mathbb{F}_p$ for any prime p. We explain our motivation on the extension to odd characteristic in Remark 2.3. On the other hand, similar to [12], we consider homogeneous MQ cryptosystems, i.e., $m = n$. But, it is easy to extend the ideas to the heterogeneous case according to the existence of a univariate polynomial in this case as given in Theorem 2.1.

Remark 2.3. Multivariate cryptography is not limited to the finite fields of characteristic 2. However, major MQ signature schemes, such as Rainbow(28, 18, 12, 12) [7], PMI+(136, 6, 18, 8) Perturbed Matsumoto–Imai Plus [21], Quartz or HFEv-(2, 129, 103, 3, 4) [13], employ the finite fields with characteristic 2. This is due to the reduced computational complexity involved. Most of them have been subjected to algebraic attacks which involve mathematical tools like the Gröbner basis method, Min-Rank problem solving, relinearization etc. to solve a set of multivariate quadratic equations. These attacks are sub-exponential or polynomial time attacks mainly because they employ field equations dependent on field characteristic 2. If the ground field is chosen to be of any characteristic other than 2, then all these attacks become void or at least exponential in terms of time and memory required for solving new field equations [8] except some specific cases (see Section 4.3). This is our prime motivation in considering the linearized binomial attack for MQ cryptosystems not only over the binary finite fields but also over the finite fields of odd characteristic.

3 Existential forgery and linearized binomial attack

Multivariate quadratic cryptosystems are generally considered as a signature scheme. The classical way to compute a digital signature $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ with a multivariate public key polynomial map $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ is to first compute the hash $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_p^n$ of a message $m \in \mathbb{F}_p^n$. The respective signature $\sigma \in \mathbb{F}_p^n$ computed by using the inverse private key triple $(L_2^{-1}, f^{-1}, L_1^{-1})$ is given as

$$\sigma = F^{-1}(x) = L_2^{-1}(f^{-1}(L_1^{-1}(x))).$$

In order to verify the signature of a received message and signature pair (m, σ), the recipient checks the equality

$$(x_1, x_2, \ldots, x_n) = (P_1(\sigma_1, \sigma_2, \ldots, \sigma_n), \ldots, P_n(\sigma_1, \sigma_2, \ldots, \sigma_n)),$$

where $x = (x_1, x_2, \ldots, x_n)$ is the hash of message m and $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ is the signature. According to the birthday paradox, a valid signature can be forged in the square root of exhaustive search. Namely, an adversary produces a list of $p^{n/2}$ evaluations $F(\sigma)$ of arbitrary signatures σ using the public key polynomial map F and a list of $p^{n/2}$ hash values of arbitrary messages m in the hash image space. Then with the probability greater than 50%, one can expect to produce at least one valid message and signature pair (m, σ), which is called *existential forgery*.

3.1 Linearized binomial attack

Harayama and Friesen [12] considered the homogeneous MQ signature scheme over $\mathbb{F}_2$, i.e. $p = 2$, and proposed a linearized binomial attack which they regard as a customization of the birthday attack. It is also known as the meet-in-the-middle attack [16, Section 7.2.3]. In the linearized binomial attack, they assume under the framework of an adaptively chosen message attack that the adversary can obtain messages whose hash values are in the image space $\mathrm{Im}(L)$ of the linearized polynomial $L : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, where $L(y) = y^{p^\delta} - y$ for some $\delta \in \mathbb{Z}^+$.

Similar to the birthday attack, for the linearized binomial attack with hash space reduced to $p^{n-\delta}$, the adversary produces a list of $p^{(n-\delta)/2}$ evaluations $f'(x) \in \mathrm{Im}(L)$ at arbitrary signatures $x \in \mathbb{F}_{p^n}$ using the public key polynomial map f'. The adversary also produces a list of $p^{(n-\delta)/2}$ hashes $H(m) \in \mathrm{Im}(L)$ of arbitrary messages $m \in \mathbb{F}_{p^n}$ by making $p^{(n-\delta)/2}$ adaptively chosen message queries to the hashing oracle. Therefore, we are looking for $x_0 \in \mathbb{F}_{p^n}$ values such that $f'(x_0) = y_0^{p^\delta} - y_0$ for some $y_0 \in \mathbb{F}_{p^n}$. Let

$$h(x, y) = f'(x) - y^{p^\delta} + y,$$

where x is the randomly generated signature value, $f'(x)$ is the evaluation through the public polynomial map and $z = y^{p^\delta} - y$ defines the restricted hash space. In other words we are looking for solutions over $\mathbb{F}_{p^n}$ of

the bivariate equation

$$\begin{aligned} h(x,y) &= f'(x) - y^{p^\delta} + y = 0 \\ &= \sum_{1\le i\le D} a_i x^{p^{\alpha_i}+p^{\beta_i}} + \sum_{1\le j\le L} b_j x^{p^{\gamma_j}} - y^{p^\delta} + y = 0 \end{aligned}$$

for some $D, L, a_i, b_j, \alpha_i, \beta_i$ as in Theorem 2.2. Using Theorem 2.2, it can be verified that this is similar to looking for the solutions over $\mathbb{F}_{p^n}$ to the simplified bivariate equation

$$h(x,y) = \sum_{i=1}^{D} A_i x^{p^{s_i}+1} + b^{p^{\beta_1}} x - y^{p^\delta} + y = 0, \tag{3.1}$$

where A_i, b, s_i, β_1 are as defined in Theorem 2.2. Obtaining these solutions can also be termed as *collision* among the two lists produced. The complexity of obtaining such a collision is the main concern in the attack. Without having any assumption on f', it maps a randomly generated signature $x \in \mathbb{F}_p^n$ to the restricted hash message space of cardinality $p^{n-\delta}$ with a probability $p^{n-\delta}/p^n$. The complexity of obtaining $p^{(n-\delta)/2}$ signatures with corresponding evaluations in the reduced hash space $\mathrm{Im}(L)$ is $p^n/p^{n-\delta}p^{(n-\delta)/2}$. The overall complexity of the linearized binomial attack is, according to the birthday paradox,

$$\frac{p^n}{p^{(n-\delta)/2}}\sqrt{\frac{\pi}{2}p^{n-\delta}}.$$

This, however, is always greater than the complexity $\sqrt{\frac{\pi}{2}p^n}$ of the birthday attack.

Using results of Mills [17], Harayama and Friesen [12] imposed certain conditions on the exponents of the corresponding simplified univariate representation $f'(x)$ of the MQ public key polynomial $F(x)$, under which one can expect this complexity to be improved. These conditions are called *emulation conditions* and defined as follows for $\delta = \gcd(s_1, \dots, s_D, n)$:

$$n/\delta \text{ is even}, \quad \delta = \gcd(s_i, n) \text{ for each } i, \quad s_i/\delta \text{ is odd for each } i, \quad 2\delta \text{ divides } |s_i - s_j| \text{ for all } i \neq j.$$

With the emulation conditions, the nonzero solutions over $\mathbb{F}_{p^n}$ to the bivariate equation $h(x, y)$ in (3.1) are divided into T equivalence classes of size $p^\delta + 1$. It is clear that $T = (p^n - 1)/(p^\delta + 1)$ and that the number t of the classes consisting of solutions over $\mathbb{F}_{p^n}$ to h satisfies $t = (N - p^\delta)/((p^\delta + 1)p^\delta)$, where N denotes the number of rational solutions over $\mathbb{F}_{p^n}$ of $h(x, y)$ (see [17, Lemmas 3.4, 3.5, 3.6] and [12, Lemma 2.2.1]). In other words, one can pick arbitrary elements x in $\mathbb{F}_{p^n}$ so that they are mapped by f' to the reduced space of cardinality $p^{n-\delta}$ with a high probability t/T.

Harayama and Friesen [12] considered the simplified univariate representation for $f'(x)$ and respective bivariate equation $h(x, y)$ with $b = 0$ and $p = 2$ in (3.1). On the other hand, we consider the attack for MQ signature schemes over $\mathbb{F}_p$ for any prime p. For the involved mathematical premise of the attack, results from Mills [17] can be used. Thus using the results in [17] together with [12], the *linearized binomial attack* can be stated as follows:

(1) Let $\delta = \gcd(s_1, \dots, s_D, n)$. This δ allows the adversary to fix a linearized binomial $L(y) = y^{p^\delta} - y$ in $\mathbb{F}_{p^n}[y]$. We denote by $\mathrm{Im}(L)$ the image of the mapping L over $\mathbb{F}_{p^n}$.

(2) Generate $\frac{T}{t}p^{(n-\delta)/2}$ random signatures $x \in \mathbb{F}_{p^n}$ and obtain the list

$$\{f'(x_1), f'(x_2), \dots, f'(x_{\frac{T}{t}p^{(n-\delta)/2}})\}.$$

(3) Generate $p^{(n-\delta)/2}$ messages m with hash values $z \in \mathrm{Im}(L)$ to obtain the list

$$\{z_1, z_2, \dots, z_{p^{(n-\delta)/2}}\}.$$

(4) Search for a coincidence $f'(x_j) = z_i$ for some i, j in two lists.

Remark 3.1. Harayama and Friesen [12] assumed the scenario in step (3) under the framework of an adaptively chosen message attack. Also it is assumed not to incur any additional cost other than $O(p^{(n-\delta)/2})$. We note that it is valid under the framework of a fully programming random oracle model [10] where such reductions are allowed to the arbitrary chosen range values. Moreover, it is also fundamental to the security proof of a cryptographic construction under an adaptively chosen message attack in the random oracle model.

The linearized binomial attack forms a case of existential forgery [16, Section 11.2.4] when successful. A valid (*message, signature*) pair under a linearized binomial attack can thus be forged in the total time complexity

$$O\Big(\frac{T}{t}p^{(n-\delta)/2}\Big).$$

When this complexity is smaller than the birthday security parameter $p^{n/2}$, the linearized binomial attack is considered successful against the MQ signature scheme. The same can be equivalently stated in terms of the number N of solutions of the bivariate equation $h(x, y) = 0$ in (3.1). If

$$N > p^{\delta} + p^{\delta/2}(p^n - 1), \tag{3.2}$$

then the complexity of the linearized binomial attack is better than the complexity $p^{n/2}$ of the birthday attack.

We note that the complexity of the attack is asymptotically less than the complexity $O(p^{n/2})$ of the birthday attack by a factor of $p^{\delta/2}$. Hence the gain in the complexity increases as δ gets closer to n.

3.2 Weak Dembowski–Ostrom polynomials

Based on the linearized binomial attack, Harayama and Friesen [12] defined the weak Dembowski–Ostrom polynomials as follows:

Definition 3.2. Let $\mathbb{F}_q$ be the n-th degree extension of the finite field $\mathbb{F}_p$. Let $f'(x) = \sum_{i=1}^{D} A_i x^{p^{s_i}+1}$ be a DO polynomial over $\mathbb{F}_q$ satisfying the following emulation conditions for $\delta = \gcd(s_1, \ldots, s_D)$:

$$n/\delta \text{ is even}, \quad s_i/\delta \text{ is odd for each } i.$$

If the number N of solutions over F_q of the bivariate equation $f'(x) = y^{p^{\delta}} - y$ satisfies

$$N > p^{\delta} + p^{\delta/2}(p^n - 1),$$

then f' is called *weak DO polynomial*.

The MQ signature scheme having public polynomials with the univariate representation in weak DO polynomials is subjected to the linearized binomial attack in complexity less than $p^{n/2}$.

Our weak DO polynomial definition differs from the definition in [12]. The following remark explains the difference.

Remark 3.3. Harayama and Friesen [12] defined weak DO polynomials for the case $p = 2$, however we give a general definition for any prime p. The N-bound in (3.2) is also slightly different than the one observed in [12]. Since computing δ from the equivalent univariate representation of the public key is trivial, one does not need to search for δ in $\{1, 2, \ldots, n\}$. Moreover, in [12], Harayama and Friesen ignored the factor of $\pi/2$ in computing the complexity of the linearized binomial attack and later in the N-bound evaluation for weak DO polynomials. They also ignored the divisor $p^{\delta/2}$ in computing the number t of branches. We note that a branch may repeat at most p^{δ} times. We also remove the emulation condition "2δ divides $|s_i - s_j|$ for all $i \neq j$" which evolves directly from s_i/δ being odd. The emulation condition $\delta = \gcd(s_i, n)$ is also removed, which we will justify in Remark 3.4 below.

In [12], Harayama and Friesen proved the existence of weak DO polynomials and demonstrated weak DO polynomials for $D = 2$ with $n = 4i$, $s_1 = i$, $s_2 = 3i$ and $p = 2$ by taking $\delta = i = n/4$. Later, based on their simulation results they conjectured that

$$f'(x) = x^{2^{n/4}+1} + x^{2^{3n/4}+1} \in \mathbb{F}_{2^n}[x] \tag{3.3}$$

with $n = 4i$, $i \geq 2$, forms an infinite class of weak DO polynomials. They considered the linearized binomial attack for MQ signature schemes over $\mathbb{F}_2$ due to the fact that the exact value of Weil sum for f' in Theorem 2.2

(see also [12, Theorem 2.3.1]) can only be determined when defined over $\mathbb{F}_{2^n}$. The Weil sum value is used to compute the exact number N of solutions of the bivariate equation h in (3.1) using the equality

$$N = 2^n + (2^\delta - 1)S, \tag{3.4}$$

where S is the exact value of the Weil sum for the simplified univariate polynomial f' (see [12, Theorem 2.2.3]). However, based on our observation in Remark 3.4 below we use degenerate quadratic forms over finite fields to count the number of solutions of the bivariate equation in (3.1) and identify a general class of *weak DO* polynomials.

Remark 3.4. We note that if the bivariate equation happens to be equivalent to a certain type of algebraic curve, then the number of points can be easily determined using [15, Theorem 6.32] in terms of standard classification of quadratic forms, without resolving the sign of the Weil sum of f'. This also allows us to remove the emulation condition of $\delta = \gcd(s_i, n)$ which is required to obtain the number N of solutions over F_q in terms of the Weil sum S as in (3.4). The same should affect the choice of δ in the linearized binomial attack.

4 Classes of weak Dembowski–Ostrom polynomials

In order to classify the weak DO polynomials, we now mention a few results from the algebraic function fields. We consider certain highly degenerate quadratic forms over the finite field $\mathbb{F}_q$ of characteristic p.

4.1 Quadratic forms

Let Q_s be a quadratic form over $\mathbb{F}_q$ defined as

$$Q_s : \mathbb{F}_{q^{2k}} \to \mathbb{F}_q, \quad a \rightarrowtail \mathrm{Tr}(aS(a))$$

and

$$S(X) = \alpha_0 X + \alpha_1 X^q + \cdots + \alpha_h X^{q^h} \in \mathbb{F}_{q^{2k}}[X]$$

be an $\mathbb{F}_q$-linearized polynomial of degree q^h in $\mathbb{F}_{q^{2k}}[X]$ for $k \geq 1$, $h \geq 0$. Let F be the algebraic function field over $\mathbb{F}_{q^{2k}}$ given as

$$F = \mathbb{F}_{q^{2k}}(u, v) \quad \text{with} \quad v^q - v = uS(u). \tag{4.1}$$

Let $\mathrm{Tr}(\cdot)$ denote the trace map from $\mathbb{F}_{q^{2k}}$ to $\mathbb{F}_q$, i.e., $\mathrm{Tr}(a) = a + a^q + \cdots + a^{q^{2k-1}}$ for $a \in \mathbb{F}_{q^{2k}}$. Let V_s be the subset of $\mathbb{F}_{q^{2k}}$ defined as

$$V_s = \{a \in \mathbb{F}_{q^{2k}} : Q_s(a) = 0\}.$$

For an Artin–Schreier type algebraic function field given in (4.1), there is only one rational point of F over the point at infinity of the function field $\mathbb{F}_{q^{2k}}(u)$. The other rational points of F correspond to the elements $a \in \mathbb{F}_{q^{2k}}$ satisfying $\mathrm{Tr}(aS(a)) = 0$. Moreover for each $a \in \mathbb{F}_{q^{2k}}$ with $Q_s(a) = \mathrm{Tr}(aS(a)) = 0$, there are q rational points in F, so that the total number of rational points is given by

$$N(F) = 1 + q|V_s|; \tag{4.2}$$

see [19, Proposition 6.4.1].

4.2 Classification of weak Dembowski–Ostrom polynomials

Enumerating weak DO polynomials satisfying the emulation conditions in Definition 3.2 can be indirectly achieved by using the theory of quadratic forms and counting the number of rational points on the Artin–

Schreier type algebraic curves which we briefly mentioned in Section 4.1. Following the notations in Section 4.1, we define an Artin–Schreier type algebraic curve as follows:

$$F = \mathbb{F}_{p^n}(x, y) \quad \text{with} \quad y^q - y = xS(x), \tag{4.3}$$

where $q = p^{n/(2k)}$ and

$$S(X) = \alpha_0 X + \alpha_1 X^q + \cdots + \alpha_h X^{q^h} \in \mathbb{F}_{p^n}[X], \quad 0 \le h \le n-1.$$

It is easy to check that the number of $\mathbb{F}_{p^n}$ rational points (4.2) of the algebraic function field in (4.3) is greater than the N-bound defined in (3.2) if $|V_s| = p^n$ which corresponds to the cardinality of $\mathbb{F}_{p^n}$. This is also verified by using MAGMA [2].

Hence, we are looking for a class of polynomials S satisfying

$$|V_s| = \{a \in \mathbb{F}_{p^n} : Q_s(a) = \mathrm{Tr}(aS(a)) = 0\} = p^n. \tag{4.4}$$

We first prove a simple class of weak DO polynomials in Theorem 4.1. Then, Corollary 4.3 to Theorem 4.1 will directly show the correctness of the conjecture in [12] (see also equation (3.3)). Then we will prove a general class of weak DO polynomials in Theorem 4.4. We also verify our computations using MAGMA [2].

Theorem 4.1. *Let p be any prime and $n, k \in \mathbb{Z}^+$ such that $2k|n$. Let $s_1 = jn/(2k)$ and $s_2 = (2k-j)n/(2k)$ for some $j \in \{1, 2, \ldots, 2k-1\}$ such that $\gcd(j, 2k-j) = 1$. Let $A_1, A_2 \in \mathbb{F}_{p^n}$ such that $A_1^{p^{s_2}} + A_2 = 0$. Then*

$$f(x) = A_1 x^{p^{s_1}+1} + A_2 x^{p^{s_2}+1} \in \mathbb{F}_{p^n}[x]$$

forms an infinite class of weak DO polynomials.

Proof. First we examine $f(x)$ for the emulation conditions. By definition

$$f(x) = A_1 x^{p^{s_1}+1} + A_2 x^{p^{s_2}+1} = A_1 x^{p^{jn/(2k)}+1} + A_2 x^{p^{(2k-j)n/(2k)}+1} \in \mathbb{F}_{p^n}[x],$$

where $j \in \{1, 2, \ldots, 2k-1\}$ such that $\gcd(j, 2k-j) = 1$ and $\delta = \gcd(s_1, s_2) = n/(2k)$. If $\gcd(j, 2k-j) = 1$ then w.l.o.g. j can be considered odd and hence with $s_1 = jn/(2k)$ and $s_2 = (2k-j)n/(2k)$, we have the emulation conditions in Definition 3.2 satisfied with n/δ even and s_i/δ odd for $i \in \{1, 2\}$ and $k, n \in \mathbb{Z}^+$ such that $2k|n$.

Let the trace map Tr be from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^\delta}$. To verify the condition in (4.4), we need to prove the following:

$$\mathrm{Tr}(f(x)) = \mathrm{Tr}\big(A_1 x^{p^{jn/(2k)}+1} + A_2 x^{p^{(2k-j)n/(2k)}+1}\big) = 0 \quad \text{for all } x \in \mathbb{F}_{p^n}. \tag{4.5}$$

Each $x \in \mathbb{F}_{p^n}$ has $2k-1$ conjugates over $\mathbb{F}_{p^\delta}$. Each conjugate is of the form $x^{p^{in/(2k)}}$ for $1 \le i \le 2k-1$. Hence for $i = 2k-j$ we get

$$(A_1 x^{p^{jn/(2k)}+1})^{p^{n(2k-j)/(2k)}} = A_1^{p^{n(2k-j)/(2k)}} x^{p^n + p^{(2k-j)n/(2k)}} = A_1^{p^{s_2}} x^{p^{(2k-j)n/(2k)}+1} = -A_2 x^{p^{(2k-j)n/(2k)}+1}.$$

Hence the trace $\mathrm{Tr}(f(x))$ in (4.5) sums to 0 under the condition $A_1^{p^{s_2}} + A_2 = 0$ over $\mathbb{F}_{p^n}$ for all $x \in \mathbb{F}_{p^n}$.

Now, we consider the following Artin–Schreier type curve:

$$F = \mathbb{F}_{p^n}(x, y) \quad \text{with } y^q - y = xS(x), \tag{4.6}$$

where $q = p^{n/(2k)}$ with

$$S(X) = A_1 x^{q^j} + A_2 x^{q^{2k-j}} \in \mathbb{F}_{p^n}[X]$$

for $j \in \{1, 2, \ldots, 2k-1\}$ such that $\gcd(j, 2k-j) = 1$. Then, the number $N(F)$ of points on the Artin–Schreier type curve can be evaluated using (4.2). It is verified that $N(F)$ for the Artin–Schreier type curve in (4.6), such that $n, k \in \mathbb{Z}^+$ and $2k|n$, is greater than the bound for weak DO polynomials in (3.2). Hence for a particular choice of k we get an infinite class of weak DO polynomials, i.e., over various extensions $\mathbb{F}_{p^n}$ of $\mathbb{F}_p$ such that $2k|n$. Table 1 mentions such choices of n for each particular k. □

k	n	(s_1, s_2)	δ	N-bound			N-observed		
				$p = 2$	$p = 3$	$p = 5$	$p = 2$	$p = 3$	$p = 5$
Class polynomial: $A_1x^{p^{n/4}+1} + A_2x^{p^{3n/4}+1}$ such that $A_1^{p^{3n/4}} + A_2 = 0$ over $\mathbb{F}_{p^n}$									
2	4	(1, 3)	1	23	141	1400	33	244	3126
2	8	(2, 6)	2	514	19689	1953145	1025	59050	9765626
2	12	(3, 9)	3	11590	2761470	2729575281	32769	14348908	30517578126
Class polynomial: $A_1x^{p^{n/6}+1} + A_2x^{p^{5n/6}+1}$ such that $A_1^{p^{5n/6}} + A_2 = 0$ over $\mathbb{F}_{p^n}$									
3	6	(1, 5)	1	91	1263	34941	129	2188	78126
3	12	(2, 10)	2	8194	1594329	1220703145	16385	4782970	6103515626
3	18	(3, 15)	3	741460	2013095934	42649611997714	2097153	10460353204	476837158203126
Class polynomial: $A_1x^{p^{n/8}+1} + A_2x^{p^{7n/8}+1}$ such that $A_1^{p^{7n/8}} + A_2 = 0$ over $\mathbb{F}_{p^n}$									
4	8	(1, 7)	1	362	11365	873466	513	19684	1953126
4	16	(2, 14)	2	131074	129140169	762939453145	262145	387420490	3814697265626
4	24	(3, 21)	3	47453137	1467546920251	$666400187 \cdot 10^9$ + 462505721	134217729	$7625 \cdot 10^9$ + 597484988	$7450580596 \cdot 10^9$ + 923828126

Table 1. Weak DO polynomials (cf. Theorem 4.1 with $j = 1$, $k = 2, 3, 4$).

k	j	$s_1 = jn/(2k)$	$s_2 = (2k - j)n/(2k)$	$\delta = \gcd(s_1, s_2)$	Class polynomial
2	1	$n/4$	$3n/4$	$n/4$	$A_1x^{p^{n/4}+1} + A_2x^{p^{3n/4}+1}$
3	1	$n/6$	$5n/6$	$n/6$	$A_1x^{p^{n/6}+1} + A_2x^{p^{5n/6}+1}$
4	1	$n/8$	$7n/8$	$n/8$	$A_1x^{p^{n/8}+1} + A_2x^{p^{7n/8}+1}$
4	3	$3n/8$	$5n/8$	$n/8$	$A_1x^{p^{3n/8}+1} + A_2x^{p^{5n/8}+1}$
5	1	$n/10$	$9n/10$	$n/10$	$A_1x^{p^{n/10}+1} + A_2x^{p^{9n/10}+1}$
5	3	$3n/10$	$7n/10$	$n/10$	$A_1x^{p^{3n/10}+1} + A_2x^{p^{7n/10}+1}$
6	1	$n/12$	$11n/12$	$n/12$	$A_1x^{p^{n/12}+1} + A_2x^{p^{11n/12}+1}$
6	5	$5n/12$	$7n/12$	$n/12$	$A_1x^{p^{5n/12}+1} + A_2x^{p^{7n/12}+1}$
⋮	⋮	⋮	⋮	⋮	⋮

Table 2. Parameter list: $D = 2$ with $A_1^{p^{s_2}} + A_2 = 0$ over $\mathbb{F}_{p^n}$.

Remark 4.2. Moreover, the classes of weak DO polynomials for $j \in \{1, 2, \ldots, 2k-1\}$ with $\gcd(j, 2k - j) = d > 1$ can also be represented by Theorem 4.1 for $s_1 = j'n/(2k')$ and $s_2 = (2k' - j')n/(2k')$ where $j = j'd$ and $k = k'd$ such that $\gcd(j', 2k' - j') = 1$. Hence we do not mention those redundant classes.

We present examples of weak DO polynomials satisfying Theorem 4.1 in Table 2. In Table 1, for $k = 2, 3, 4$ and $p = 2, 3, 5$, we consider a few initial n values and define weak DO class polynomials satisfying Theorem 4.1 with $\delta = 1, 2, 3$. We also mention the corresponding N-bound and N-observed calculated by using (3.2) and (4.2), respectively.

Corollary 4.3. *Let $n, k \in \mathbb{Z}^+$ such that $2k|n$. Let $s_1 = jn/(2k)$ and $s_2 = (2k - j)n/(2k)$ for some $j \in \{1, 2, \ldots, 2k-1\}$ such that $\gcd(j, 2k - j) = 1$. Let $A_1, A_2 \in \mathbb{F}_{2^n}$ such that $A_1^{2^{s_2}} + A_2 = 0$. Then*

$$f(x) = A_1x^{2^{s_1}+1} + A_2x^{2^{s_2}+1} \in \mathbb{F}_{2^n}[x]$$

forms an infinite class of weak DO polynomials.

The conjecture in [12] (see our equation (3.3)) is a special case of the class given in Corollary 4.3 for $j = 1$ and $k = 2$ with $A_1, A_2 \in \mathbb{F}_2$.

Theorem 4.4. *Let p be any prime and $n, k \in \mathbb{Z}^+$ such that $2k|n$. Let $s_i = \alpha_i n/(2k)$ with $\alpha_i = 2i-1$ for $1 \le i \le k$ where $A_i \in \mathbb{F}_{p^n}$ such that $A_i + A_{k+1-i}^{p^{s_i}} = 0$. Then*

$$f(x) = \sum_{i=1}^{k} A_i x^{p^{s_i}+1} \in \mathbb{F}_{p^n}[X]$$

forms an infinite class of weak DO polynomials.

Proof. Similar to Theorem 4.1, we first examine $f(x)$ for the emulation conditions given in Definition 3.2. Let

$$f(x) = \sum_{i=1}^{k} A_i x^{p^{s_i}+1} \in \mathbb{F}_{p^n}[x],$$

where $s_i = \alpha_i n/(2k)$ with $\alpha_i = 2i-1$ for $1 \le i \le k$. For simplification of the proof we assume that $A_i \neq 0$ for $1 \le i \le k$ and $\delta := \gcd(s_1, \dots, s_k) = n/(2k)$. Emulation conditions are trivially satisfied with $n/\delta = 2k$ even and $s_i/\delta = \alpha_i$ odd for $1 \le i \le k$.

To evaluate equation (4.4), let the trace map be defined as $\mathrm{Tr} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^\delta}$. We need to prove

$$\mathrm{Tr}(f(x)) = \mathrm{Tr}\Big(\sum_{i=1}^{k} A_i x^{p^{s_i}+1}\Big) = 0 \quad \text{for all } x \in \mathbb{F}_{p^n}. \tag{4.7}$$

We show in two steps that equation (4.7) holds. First we will show that $\mathrm{Tr}(A_i x^{p^{\alpha_i n/(2k)}+1}) = 0$ for an odd integer k with $i = (k+1)/2$. In the second step, we will show that $\mathrm{Tr}(A_i x^{p^{\alpha_i n/(2k)}+1}) = -\mathrm{Tr}(A_{i'} x^{p^{\alpha_{i'} n/(2k)}+1})$ for $i' = k+1-i$ and $i = 1, 2, \dots, k$. We start with the first step. Let k be an odd integer and $i = (k+1)/2$. Then, the trace of the monomial $A_i x^{p^{\alpha_i n/(2k)}+1}$ with $\alpha_i = k$ and $A_i + A_i^{p^{n/2}} = 0$ is

$$\begin{aligned}
\mathrm{Tr}(A_i x^{p^{\alpha_i n/(2k)}+1}) &= \mathrm{Tr}(A_i x^{p^{kn/(2k)}+1}) \\
&= A_i x^{p^{kn/(2k)}+1} + A_i^{p^{n/(2k)}} x^{p^{(k+1)n/(2k)}+p^{n/(2k)}} + \cdots + A_i^{p^{(k-1)n/(2k)}} x^{p^{(2k-1)n/(2k)}+p^{(k-1)n/(2k)}} \\
&\quad + A_i^{p^{kn/(2k)}} x^{p^{(2k)n/(2k)}+p^{kn/(2k)}} + \cdots + A_i^{p^{(2k-1)n/(2k)}} x^{p^{(k-1)n/(2k)}+p^{(2k-1)n/(2k)}} \\
&= A_i x^{p^{n/2}+1} + A_i^{p^{n/(2k)}} x^{p^{(k+1)n/(2k)}+p^{n/(2k)}} + \cdots + A_i^{p^{(k-1)n/(2k)}} x^{p^{(2k-1)n/(2k)}+p^{(k-1)n/(2k)}} \\
&\quad + A_i^{p^{n/2}} x^{1+p^{n/2}} + \cdots + A_i^{p^{(2k-1)n/(2k)}} x^{p^{(k-1)n/(2k)}+p^{(2k-1)n/(2k)}} \\
&= A_i x^{p^{n/2}+1} + A_i^{p^{n/(2k)}} x^{p^{(k+1)n/(2k)}+p^{n/(2k)}} + \cdots + A_i^{p^{(k-1)n/(2k)}} x^{p^{(2k-1)n/(2k)}+p^{(k-1)n/(2k)}} \\
&\quad - A_i x^{1+p^{n/2}} - A_i^{p^{n/(2k)}} x^{p^{n/(2k)}+p^{(k+1)n/(2k)}} - \cdots - A_i^{p^{(k-1)n/(2k)}} x^{p^{(k-1)n/(2k)}+p^{(2k-1)n/(2k)}}.
\end{aligned}$$

Hence we have $\mathrm{Tr}(A_i x^{p^{\alpha_i n/(2k)}+1}) = 0$ for $i = (k+1)/2$. In the second step, let $i' = k+1-i$. We evaluate the $\alpha_{i'}$-th conjugate of the monomials of the form $A_i x^{p^{\alpha_i n/(2k)}+1}$ for $1 \le i \le k$ and $i \neq (k+1)/2$:

$$(A_i x^{p^{\alpha_i n/(2k)}+1})^{p^{\alpha_{i'} n/(2k)}} = A_i^{p^{\alpha_{i'} n/(2k)}} x^{p^{(\alpha_i+\alpha_{i'})n/(2k)}+p^{\alpha_{i'} n/(2k)}} = A_i^{p^{\alpha_{i'} n/(2k)}} x^{1+p^{\alpha_{i'} n/(2k)}} = -A_{i'} x^{1+p^{\alpha_{i'} n/(2k)}}.$$

Hence $\mathrm{Tr}(A_i x^{p^{\alpha_i n/(2k)}+1}) = -\mathrm{Tr}(A'_i x^{p^{\alpha'_i n/(2k)}+1})$ for $i' = k+1-i$ and $i = 1, 2, \dots, k$. Therefore, equation (4.7) holds.

Now, we consider the following Artin–Schreier type curve:

$$F = \mathbb{F}_{p^n}(x, y) \quad \text{with} \quad y^q - y = xS(x), \tag{4.8}$$

where $q = p^{n/(2k)}$ and

$$S(x) = \sum_{i=1}^{k} A_i x^{q^{\alpha_i}} \in \mathbb{F}_{p^n}[x].$$

The number $N(F)$ of $\mathbb{F}_{p^n}$ rational points on the Artin–Schreier type curve in (4.8) can be evaluated using (4.2). It is verified that $N(F)$ is greater than the bound for weak DO polynomials in (3.2) for $k, n \in \mathbb{Z}^+$ such that $2k|n$. Similar to Theorem 4.1, for a particular choice of k we get infinite classes of weak DO polynomials, i.e., over various extension $\mathbb{F}_{p^n}$ of $\mathbb{F}_p$ such that $2k|n$.

In the cases where $A_i = 0$ for some $1 \leq i < k$ we proceed in a similar way. Let $A_{i_1}, A_{i_2}, \ldots, A_{i_t}$ be the nonzero elements. Then, we have $\delta = \gcd(s_{i_1}, \ldots, s_{i_t}) = dn/(2k)$ for $\gcd(\alpha_{i_1}, \ldots, \alpha_{i_t}) = d > 1$. The corresponding DO polynomial $f(x)$ will satisfy the emulation conditions in Definition 3.2 with $n/\delta = 2k'$ even with $k = k'd$ and $s_{i_j}/\delta = \alpha_{i_j}/d$ odd for $1 \leq j \leq t$. The remaining steps of the proof similarly hold for $\delta = n/(2k')$. □

Similar to Table 2, classes of weak DO polynomial satisfying Theorem 4.4 can be constructed for different values of $k, n \in \mathbb{Z}^+$ such that $2k|n$.

Using the conditions in Theorem 4.4 on $A_i \in \mathbb{F}_{p^n}$ for $1 \leq i \leq k$ such that $A_i + A_{k+1-i}^{p^{s_i}} = 0$, we state a few examples of weak DO polynomial classes over $\mathbb{F}_{p^n}$ as follows:

- For $k = 2$, $A_1 x^{p^{n/4}+1} + A_2 x^{p^{3n/4}+1}$.
- For $k = 3$, $A_1 x^{p^{n/6}+1} + A_2 x^{p^{3n/6}+1} + A_3 x^{p^{5n/6}+1}$.
- For $k = 4$, $A_1 x^{p^{n/8}+1} + A_2 x^{p^{3n/8}+1} + A_3 x^{p^{5n/8}+1} + A_4 x^{p^{7n/8}+1}$.
- For $k = 5$, $A_1 x^{p^{n/10}+1} + A_2 x^{p^{3n/10}+1} + A_3 x^{p^{5n/10}+1} + A_4 x^{p^{7n/10}+1} + A_5 x^{p^{9n/10}+1}$.

Remark 4.5. It is clear that Theorem 4.1 is a subclass of Theorem 4.4. However, we present them as separate classes to prove the existence of conjectured class [12] of weak DO polynomials. Theorem 4.4 partially addresses the second open problem in [12] of enumerating weak DO polynomials.

We note that MQ signature schemes should eliminate weak DO polynomials as we present in Theorem 4.4 and their equivalent forms from their key generation algorithms.

4.3 Comparison to Gröbner basis method

In recent years, a significant effort has been made to invert HFE polynomials using the Gröbner basis method over finite fields of any characteristic (see [1, 6] and references therein). Ding and Hodges [6] present a bound for the *degree of regularity* (see [6, Definition 3.1]) of HFE system over an arbitrary finite field. Degree of regularity (D_{reg}) measures the time complexity of Gröbner basis method in inverting HFE polynomials. If D_{reg} is a constant, then the complexity is polynomial in the number n of variables. Moreover, the complexity is quasi-polynomial and exponential in n if D_{reg} is logarithmic and polynomial in n, respectively. Ding and Hodges prove in [6, Theorem 4.2] that the bound on D_{reg} is proportional with p and D where p is the order of finite field and D is the number of terms in the HFE polynomial. Thus it is very easy to invert HFE polynomials when both p and D are constant or logarithmic in n. On the other hand it is exponential when either p or D is of scale $O(n)$. Therefore, we deduce that the Gröbner basis method is better than the linearized binomial attack against weak DO polynomials we derived in Theorem 4.4 for small p and k. In other cases, the linearized binomial attack performs better in the existential forgery of MQ signature schemes.

5 Conclusion

In this paper we studied the linearized binomial attack [12] for MQ cryptosystems. Using results from Mills [17], we extended the attack in [12] to MQ signature schemes over the finite fields of any characteristic. Then we gave a general definition of weak DO polynomials [12] for the finite fields of any characteristic. Using Artin–Schreier type algebraic function fields, we constructed and proved classes of weak DO polynomials. In fact, we showed that the number of solutions of bivariate equation in the linearized binomial attack can be evaluated without the need to determine the sign of the Weil sum of the simplified univariate representation of the public key.

Acknowledgement: We thank the referees for providing detailed comments which helped to improve this paper.

Funding: Oğuz Yayla is supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under the National Postdoctoral Research Scholarship no. 2219.

References

[1] L. Bettale, J.-C. Faugère and L. Perret, Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic, *Des. Codes Cryptogr.* **69** (2013), 1–52.
[2] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.
[3] C.-H. O. Chen, M.-S. Chen, J. Ding, F. Werner and B.-Y. Yang, Odd-char multivariate hidden field equations, preprint (2008), http://eprint.iacr.org/2008/543.
[4] N. T. Courtois, Short signatures, provable security, generic attacks and computational security of multivariate polynomial schemes such as HFE, Quartz and Sflash, preprint (2004), http://eprint.iacr.org/2004/143.
[5] P. Dembowski and T. G. Ostrom, Planes of order n with collineation groups of order n^2, *Math. Z.* **103** (1968), 239–258.
[6] J. Ding and T. J. Hodges, Inverting HFE systems is quasi-polynomial for all fields, in: *Advances in Cryptology* (CRYPTO 2011), Lecture Notes in Comput. Sci. 6841, Springer, Berlin (2011), 724–742.
[7] J. Ding and D. Schmidt, Rainbow, a new multivariable polynomial signature scheme, in: *Applied Cryptography and Network Security*, Lecture Notes in Comput. Sci. 3531, Springer, Berlin (2005), 164–175.
[8] J. Ding, D. Schmidt and F. Werner, Algebraic attack on HFE revisited, in: *Information Security*, Lecture Notes in Comput. Sci. 5222, Springer, Berlin (2008), 215–227.
[9] J. Ding and B.-Y. Yang, Multivariate public key cryptography, in: *Post-Quantum Cryptography*, Springer, Berlin (2009), 193–241.
[10] M. Fischlin, A. Lehmann, T. Ristenpart, T. Shrimpton, M. Stam and S. Tessaro, Random oracles with(out) programmability, in: *Advances in Cryptology* (ASIACRYPT 2010), Lecture Notes in Comput. Sci. 6477, Springer (2010), 303–320.
[11] T. Harayama, On the Weil sum evaluation of central polynomial in multivariate quadratic cryptosystem, preprint (2006), http://eprint.iacr.org/2006/075.
[12] T. Harayama and D. K. Friesen, Weil sum for birthday attack in multivariate quadratic cryptosystem, *J. Math. Cryptol.* **1** (2007), 79–104.
[13] A. Kipnis, J. Patarin and L. Goubin, Unbalanced oil and vinegar signature schemes, in: *Advances in Cryptology* (EUROCRYPT '99), Lecture Notes in Comput. Sci. 1592, Springer, Berlin (1999), 206–222
[14] A. Kipnis and A. Shamir, Cryptanalysis of the HFE public key cryptosystem by relinearization, in: *Advances in Cryptology* (CRYPTO '99) Lecture Notes in Comput. Sci. 1666, Springer, Berlin (1999), 19–30.
[15] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia Math. Appl. 20, Cambridge University Press, Cambridge, 1997.
[16] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press Ser. Discrete Math. Appl., CRC Press, Boca Raton, 1997.
[17] D. Mills, On the evaluation of Weil sums of Dembowski–Ostrom polynomials, *J. Number Theory* **92** (2002), 87–98.
[18] J. Patarin and L. Goubin, Trapdoor one-way permutations and multivariate polynomials, in: *Information and Communications Security*, Lecture Notes in Comput. Sci. 1334, Springer, Berlin (1997), 356–368.
[19] H. Stichtenoth, *Algebraic Function Fields and Codes*, 2nd ed., Grad. Texts in Math. 254, Springer, Berlin, 2009.
[20] C. Wolf, *Multivariate quadratic polynomials in public key cryptography*, Ph.D. thesis, Katholieke Universiteit Leuven, 2005.
[21] C. Wolf and B. Preneel, Taxonomy of public key schemes based on the problem of multivariate quadratic equations, preprint (2005), http://eprint.iacr.org/2005/077.

Received May 15, 2013; revised March 10, 2014; accepted July 9, 2014.